WEAPONS OF CONTROL, SHIELDS OF IMPUNITY
The #KeepItOn campaign unites and organizes global organizations and efforts to end internet shutdowns. The campaign was launched by a coalition of about 70 organizations in 2016 at RightsCon in Silicon Valley. Membership of the coalition has since increased rapidly to more than 300 members from 105 countries around the world ranging from civil society, rights, and advocacy groups to research centers, detection networks, foundations, and media organizations.

This report is a publication of Access Now for the #KeepItOn coalition and was written by Zach Rosson, Felicia Anthonio, and Carolyn Tackett in collaboration with the Access Now team.

The authors would like to especially thank Sage Cheng, Donna Wentworth, Marwa Fatafta, Raman Jit Singh Chima, Wai Phyo Myint, Golda Benjamin, Anastasiya Zhymont, Natalia Krapiva, Ángela Alarcón, Bridget Andre, Ji Yeon Kim, Jaimee Kokonya, Namrata Maheshwari, Peter Micek, Kassem Mnejja, Laura O’Brien, Gaspar Pisanu, Agneris Sampieri, Dhevy Sivaprakasam, Chetna Kumar, Alexia Skok, and Megan Kathure, for their contributions. They would like to thank Data4Change, Software Freedom Law Centre India (SFLC.in), Yodet, Digitally Right, Miaan Group, Cloudflare, Internet Outage Detection and Analysis (IODA), Myanmar Internet Project, Athan, Kentik, Open Observatory of Network Interference (OONI), and other members of the #KeepItOn coalition for providing valuable information and insights about case studies, reviewing data and sources, and contributing to the report. Any errors, misrepresentations, or inaccuracies are ours alone, and we welcome your feedback.

Design and data visualization by Sage Cheng.

A note on our data

This #KeepItOn report looks at incidents of internet shutdowns documented by Access Now and the #KeepItOn coalition in 2022. While we try to build a comprehensive database, our data relies on technical measurement as well as contextual information, such as news reports or personal accounts. The constraints of our methodology mean that there may be cases of internet shutdowns that have gone unreported, and numbers are likely to change if and when new information becomes available after publication. For further reading, please visit https://accessnow.org/keepiton-data-methodology.

February 2023
### Table of contents

I. Internet shutdowns in 2022: a global overview  
   Overview of 2022 data  

II. Triggers for internet shutdowns in 2022  
   Shutdowns during protests  
   Shutdowns during active conflict  
   Shutdowns during examinations  
   Shutdowns during elections  

III. New and continuing trends in 2022  
   Grave human rights abuses and violence shrouded by shutdowns on the rise  
   Countries entrenched in repeat offenses and prolonged shutdowns  
   Targeted shutdowns and their immeasurable harms  

IV. Internet shutdowns by region  
   Africa  
      Shutdowns during protest and unrest  
      Shutdowns during elections  
      Sustained platform blocks  
      Ethiopia  
   Asia Pacific  
      Myanmar  
      India  
      Shutdowns during protest and unrest  
   Eastern Europe and Central Asia  
      Central asia  
      Russia’s invasion of Ukraine  
      Armenia-Azerbaijan territorial dispute  
   Latin America and the Caribbean  
      Cuba  
      Brazil  
   Middle East and North Africa  
      Platform blocks  
      Exam-related shutdowns  
      Iran  
      Sudan  

V. Fighting back: the movement is growing  

VI. What’s next
I. Internet shutdowns in 2022: a global overview

Overview of 2022 data

Documented internet shutdowns by year *

<table>
<thead>
<tr>
<th>Year</th>
<th>Total number of shutdowns</th>
<th>Total number of shutdowns, not including India</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>75</td>
<td>45</td>
</tr>
<tr>
<td>2017</td>
<td>106</td>
<td>37</td>
</tr>
<tr>
<td>2018</td>
<td>196</td>
<td>62</td>
</tr>
<tr>
<td>2019</td>
<td>213</td>
<td>92</td>
</tr>
<tr>
<td>2020</td>
<td>159</td>
<td>50</td>
</tr>
<tr>
<td>2021</td>
<td>184</td>
<td>77</td>
</tr>
<tr>
<td>2022</td>
<td>187</td>
<td>103</td>
</tr>
</tbody>
</table>

* These numbers reflect the latest data available as of publication of this report and include updates to previously published totals for past years.

Number of countries where shutdowns occurred

<table>
<thead>
<tr>
<th>Year</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>25</td>
</tr>
<tr>
<td>2017</td>
<td>19</td>
</tr>
<tr>
<td>2018</td>
<td>26</td>
</tr>
<tr>
<td>2019</td>
<td>33</td>
</tr>
<tr>
<td>2020</td>
<td>29</td>
</tr>
<tr>
<td>2021</td>
<td>34</td>
</tr>
<tr>
<td>2022</td>
<td>35</td>
</tr>
</tbody>
</table>

India: 84
Ukraine: 22**
Iran: 18
Myanmar: 7
Bangladesh: 6
Jordan: 4
Libya: 4
Sudan: 4
Turkmenistan: 4

Afghanistan: 2
Burkina Faso: 2
Cuba: 2
Kazakhstan: 2
Russia: 2
Sierra Leone: 2
Tajikistan: 2
Uzbekistan: 2

Algeria: 1
Armenia: 1
Azerbaijan: 1
Brazil: 1
China: 1
Ethiopia: 1
Iraq: 1
Nigeria: 1
Oman: 1
Pakistan: 1
Somaliland: 1
Sri Lanka: 1
Syria: 1
Tunisia: 1
Turkey: 1
Uganda: 1
Yemen: 1**
Zimbabwe: 1

** Shutdowns were imposed by external forces during armed conflict in Ukraine and Yemen.
**INTERNET SHUTDOWNS IN 2022**

**Shutdown triggers in 2022**

<table>
<thead>
<tr>
<th><strong>Protests</strong></th>
<th>62 shutdowns in 16 countries during protests</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exams</strong></td>
<td>8 shutdowns in 6 countries “to prevent exam cheating”</td>
</tr>
<tr>
<td><strong>Active conflicts</strong></td>
<td>33 shutdowns during active conflicts</td>
</tr>
<tr>
<td><strong>Elections</strong></td>
<td>5 shutdowns in 5 countries tied to elections</td>
</tr>
</tbody>
</table>

**Shutdown trends in 2022**

1. **Grave human rights abuses*** and violence shrouded by shutdowns on the rise

   → 48 shutdowns in 14 countries coinciding with documented human rights abuses:

   Bangladesh, Ethiopia, Iran, Jordan, Kazakhstan, Myanmar, Russia, Sierra Leone, Somaliland, Sudan, Tajikistan, Uzbekistan, and active conflict zones in Ukraine and Yemen

   *** Human rights abuses include cases where there is evidence of violence, including murder, torture, rape, or apparent war crimes by governments, militaries, and police or security forces.

2. **Countries entrenched in repeat offenses and prolonged shutdowns**

   → 787+ days

   By the end of 2022, people in Tigray, Ethiopia had endured 2+ years of full communications blackout, and many remain disconnected

   → 33 of the 35 countries that imposed shutdowns are repeat offenders since 2016

   → 500+ days

   People in many regions across Myanmar had been in the dark for 500+ days by March 2023

   → 16 shutdowns worldwide lasted from 2021 to 2022 and 16 are now ongoing from 2022 to 2023, compared to 8 between 2020 and 2021

3. **Targeted shutdowns and their immeasurable harms**

   → 23 countries had 28 service-based shutdowns in 2022:

   Afghanistan, Algeria, Armenia, Azerbaijan, Bangladesh, Brazil, Burkina Faso, China, India, Iran, Jordan, Kazakhstan, Nigeria, Oman, Russia, Sri Lanka, Tunisia, Turkey, Turkmenistan, Uganda, Ukraine (imposed by Russian military), Uzbekistan, and Zimbabwe

   → Layered tactics of shutdown + censorship + surveillance:

   - Iran: Nationwide platform blocks + curfew-style mobile blocks in regional hotspots
   - Myanmar: Disrupting mobile networks, VPN access, encrypted messaging + forcing people onto heavily surveilled, military-operated ISP networks
   - Ukraine: Cyberattacks impacting Ukrainian ISPs + attempts to force occupied territories onto highly censored and surveilled Russian networks
Governments around the world are imposing internet shutdowns at alarming rates, reaching milestones that seemed unlikely in 2016 when the #KeepItOn campaign was launched.

In 2022, Access Now and the #KeepItOn coalition documented at least 187 shutdowns across 35 countries — breaking our record for the number of countries to hit the kill switch in a single year. If we set aside the figures from India, a unique case, 2022 was also the year with the highest total number of shutdowns in the rest of the world to date. While we observed a downturn in shutdown rates at the height of COVID-19 in 2020, with an increase in 2021, internet shutdowns spiked in 2022, exceeding even pre-pandemic levels. This resurgence also drove the total number of shutdowns recorded since 2016 well above 1,000.

Shutdowns continued to be triggered by protests, active conflict, examinations, elections, political instability, and other high-profile national events. Authorities ordered shutdowns for many of the same reasons they have for years, some using the same tired justifications. In the midst of unrest and conflict, or just during yearly school examinations, governments, militaries, and police forces kept people in the dark as a desperate means of control. For prolonged periods of time, those in power used shutdowns to silence people, often targeting specific communities through complete blackouts, mobile shutdowns, and platform blocking.

India implemented at least 84 shutdowns in 2022, the most of any country for the fifth consecutive year. Ukraine suffered through 22 shutdowns imposed by the Russian military during its full-scale invasion and occupation, the second highest total globally. Iran followed with 18 shutdowns, breaking its own annual shutdown record with layers of shutdowns during massive protests around the country. Nine countries imposed at least four shutdowns each, repeatedly reaching for this tool for control. Perpetrators continued 16 shutdowns from 2021 into 2022, and another 16 shutdowns from 2022 into 2023, with 12 spanning the length of the entire year or longer. Ongoing shutdowns in Tigray, Ethiopia since 2020, and in regions across Myanmar since 2021, highlight the cruelty of singular prolonged blackouts in exacerbating humanitarian crises. These shutdowns demonstrate a pattern of entrenchment in the use of shutdowns, where countries repeatedly use this tactic — both over time and within the annual reporting period — or persist in keeping people in the dark for extended periods.

Internet shutdowns, of any form, always violate fundamental human rights and cause incalculable and persistent damage to people’s lives. Although shutdowns vary significantly in their technical implementation and effect on people’s ability to use the global internet, we rely on total numbers of shutdowns to show the global scale of the problem. However, since we started documenting shutdowns in 2016, India has accounted for approximately 58% of all shutdowns documented in Access Now’s Shutdown Tracker Optimization Project (STOP) database. The responsibility of Indian states for the majority of shutdowns globally is impossible to ignore and a deep problem on its own. If we examine the number of shutdowns without India in 2022, we reach another grim milestone. Of the 187 shutdowns across the world, 103 occurred outside of India, across 34 countries, passing a record last set in 2019, when there were 92 shutdowns outside India across 32 countries. We recorded 50 shutdowns

---

1. An internet shutdown has been defined as “an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.” An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. See Access Now (2020). No more internet shutdowns! let’s #KeepItOn. Retrieved February 22, 2023, from https://www.accessnow.org/no-internet-shutdowns-lets-keepiton/.
INTERNET SHUTDOWNS IN 2022

across 28 countries outside of India in 2020, half the amount in 2022. The rise in shutdowns outside India represents a meteoric increase in the global spread of shutdowns over the past two years, but also reflects the increased capacity of civil society to verify and document shutdowns in repressive environments.

The human impacts of shutdowns remained visceral in 2022, as authorities hit the kill switch most often in times of existing chaos and violence. Perpetrators imposed 48 shutdowns across 14 countries to shroud violence and serious human rights abuses, such as murder, torture, rape, or apparent war crimes. Whether in conflict zones or during mass protests, authorities used shutdowns to try to hide serious rights violations and sever communications between individuals and communities, which also impacted human rights monitoring, including shutdown tracking and provision of humanitarian aid.

Mobile shutdowns continued to target marginalized groups, including ethnic and religious minorities and other vulnerable groups. Shutdowns deepen the gender digital divide, disrupting the ability of women to conduct business or access information on reproductive healthcare. Lack of access to resources, inability to communicate with loved ones, and difficulty sending or receiving news are just a few of the impacts that each shutdown has on countless people.

Despite these troubling findings, we have seen progress in the battle to end shutdowns and encouraging signs of solidarity in the international community. The #KeepItOn coalition has grown to over 300 members from 105 countries, taking the fight to new places and bigger stages. Together, we successfully mobilized against election-related shutdowns globally, including during Kenya’s general elections, while sustaining momentum in urging relevant authorities to push for an end to the over two-years-long blackout in Ethiopia’s Tigray region. Another milestone was the resounding message of the Office of the United Nations High Commissioner for Human Rights (OHCHR) in their landmark report, which described the “dramatic real-life effects of shutdowns on the lives and human rights of millions of people,” and echoed the refrains of civil society that shutdowns cause “incalculable damage” with costs exceeding “any hoped for benefit.”

As people around the world grapple with economic insecurity, humanitarian crises, and repression by authoritarian states, internet shutdowns are unwelcome intrusions, demonstrably harmful, and clear violations of human rights. Global attention on shutdowns is reaching a critical juncture, and civil society is meeting the challenge by shining a light on the darkness of internet shutdowns.

Geo-scopes of internet shutdowns in 2022

- 49.2% of shutdowns only affected one city, county, or village (92)
- 31.6% of shutdowns affected locations in more than one state, province, or region (59)
- 18.7% of shutdowns affected more than one city in the same state, province, or region (35)
- 0.5% Unknown (1)

II. Triggers for internet shutdowns in 2022

Using seven years of internet shutdown data compiled through our Shutdown Tracker Optimization Project (STOP) with the crucial support of the #KeepItOn coalition, we have tracked the myriad ways internet access is weaponized by those in power to assert control and silence voices. Authorities or aggressors in 35 countries imposed shutdowns during protests, active conflict, school examinations, elections, periods of political instability, or high-profile events like religious holidays or visits by government officials.

**Shutdowns during protests**

In 2022, protests erupted worldwide in the wake of resurging authoritarianism, worsening economic inequality, and deepening repression of marginalized groups. Authorities in Bangladesh, Cuba, India, Iran, Jordan, Kazakhstan, Libya, Myanmar, Pakistan, Sierra Leone, Somalia, Sri Lanka, Sudan, Tajikistan, Uzbekistan, and Zimbabwe imposed 62 shutdowns during protests in 2022, approaching the pre-pandemic watermark of 65 shutdowns recorded during protests in 2019. Of these protest-related shutdowns in 2022, 19 disproportionately impacted entire countries. However, the majority were imposed at either the regional (17) or local (25) levels, representing targeted, aggressive attempts to conceal human rights abuses and dismantle protest movements.

**Shutdowns during active conflicts**

Perpetrators imposed shutdowns in the context of conflict in 2022 using a variety of methods, such as leveraging prolonged blackouts in Myanmar and Ethiopia, repeated airstrikes targeting civilian infrastructure in Ukraine and Yemen, or platform blocks in Azerbaijan, Armenia, and Russia. Aggressors carried out 33 shutdowns during active conflicts, deepening the alarming pattern of recent years where internet shutdowns function as deliberate military strategy. Whether internet access is severed through the deliberate destruction of infrastructure by invading forces, or through the targeted suspension of service by a government in power, people are cut off from the world for weeks, to months, to years.

The human toll of conflict-related shutdowns is immense. International humanitarian efforts are hampered, life-saving information about troop movements and humanitarian corridors is difficult or impossible to obtain, and documentation of war crimes and atrocities is restricted.\textsuperscript{14} The insecurity and desperation for people experiencing a lack of reliable food, water, and electricity in humanitarian crises is only exacerbated during internet and telecommunications blackouts, as the lack of contact with loved ones or the outside world only amplifies the uncertainty and severs many avenues for seeking help. Lastly, even if attacks cease, recovering destroyed infrastructure can take months to years, adding on to the misery of extended shutdowns in places like Tigray\textsuperscript{15} and liberated cities across Ukraine.\textsuperscript{16}

**Shutdowns during examinations**

Governments continued to brazenly impose shutdowns during student and public exams throughout 2022. Authorities implemented eight shutdown orders for exams, in four cases disproportionately cutting internet access across entire countries (Algeria, Jordan, Sudan, Syria), and in four cases targeting shutdowns to the region with exam locations (Iraqi Kurdistan and India’s Assam and West Bengal). These orders often encompassed multiple planned disruptions across the exam season. With 11 exam-related shutdowns in 2021 and eight in 2020, it’s clear exam shutdowns are a persistent problem disrupting the lives of millions and violating the rights of everyone impacted, not just students.

\textsuperscript{14} See supra note 13.
\textsuperscript{15} See supra note 11.
INTERNET SHUTDOWNs IN 2022

Given these impacts and the failure of shutdowns to curb student cheating, authorities must make good on past promises to cease imposing them.

Shutdowsn during elections

Elections also continue to be a trigger for authorities to shut down the internet or block platforms, with five shutdowns in 2022 tied to elections in Brazil, India, Kazakhstan, Turkmenistan, and Uganda. Authorities try to control information or quell dissent throughout election cycles, sometimes in the months leading up to elections, as we saw in Brazil, during inaugurations or protests surrounding contested elections, as we saw in Kazakhstan, or even months or years after an election, as we saw in Uganda, where authorities persisted in blocking social media once the election was over.

In 2022 we saw a slight decrease in the number of election-related shutdowns from previous years (12 in 2019, 10 in 2020, seven in 2021). In 2023 Access Now and the #KeepItOn coalition are once again monitoring elections through our #KeepItOn Election Watch campaign, with the aim of preventing further election shutdowns. We are watching 17 elections in 2023, focusing in particular on countries that have previously cut internet access or blocked communications platforms. There are some encouraging signs that civil society mobilization is an effective tool for preventing shutdowns surrounding elections. In 2022, two countries that were on our watchlist, Kenya and The Gambia, each maintained internet access throughout their elections. That said, we also saw elections postponed or effectively canceled. Given the rise of anti-democratic norms around the world, this instability suggests the risk of election shutdowns will remain high. The year ahead will therefore prove to be a significant test of government commitments to #KeepItOn during elections, as well as the capacity of civil society to prepare for, prevent, circumvent, document, or otherwise mitigate the impact of any such shutdowns.

III. New and continuing trends in 2022

Grave human rights abuses and violence shrouded by shutdowns on the rise

All internet shutdowns violate human rights. The impacts are especially profound in contexts where people are most at risk of violence. In 2022, we saw a spike in the use of shutdowns to shroud violence and serious human rights abuses, with 48 shutdowns linked to this kind of abuse in diverse contexts.

For example, in some contexts, authorities responded to protests with brutal crackdowns and internet shutdowns, even though research shows network disruptions can exacerbate polarization and contribute to moving protests toward violent confrontations. In other contexts, such as during conflicts and war, governments, warring parties, or military regimes deployed shutdowns in apparent attempts to hide human rights and humanitarian law violations such as murder, torture, rape, and other war crimes. Finally, perpetrators used internet shutdowns

as a tool of warfare, not only to cover apparent war crimes, but to inflict further harm on the civilian population. Missile strikes, specifically, led to 15 shutdowns in 2022 — 14 launched by the Russian military on cities across Ukraine and one launched by Saudi-led coalition forces on a telecommunications facility in Hudaydah, Yemen.22

Over the span of a year, there was evidence of violence and serious human rights violations cloaked by shutdowns in 14 countries. This cloaking exacerbates the harm to people and communities, exacting a severe human toll. Humanitarian and human rights organizations project that in areas impacted by shutdowns, it delays or prevents casualty counts, affects the capacity of communities to identify victims, and interferes with the ability of news media to report accurately on the scale of the attacks. All of this impedes humanitarian assistance.24

The association of violence with internet shutdowns merits further investigation. Across a variety of contexts, it appears that violence directly associated with shutdowns is on the rise. In 2022, 133 of the 187 total shutdowns occurred alongside some form of violence, compared to 110 in 2021, 99 in 2020, and 75 in 2019. In some of these cases, authorities have cited violence as part of the rationale for shutting down the internet. However, there is no evidence to show internet shutdowns reduce violence — quite the opposite.25 And when authorities order shutdowns during conflicts, or use them as a form of attack, they serve to exacerbate, not relieve, human suffering.

It is notable that authorities often cite concerns about the spread of misinformation and incitement to violence as a rationale to order shutdowns and platform blocks. In 2022, authorities in five countries (Azerbaijan, Brazil, India, Jordan, and Uganda) cited the need to restrict misinformation, incitement to violence, or other forms of harmful content online as a primary justification for rights-harming disruptions or blocking. The proliferation of hateful content and dangerous misinformation does require active policy and legal interventions. However, the spread of misinformation and hate speech is not an excuse for internet shutdowns, which are often used in politicized and arbitrary ways that are “incompatible with international human rights law,” especially as their impact on human rights extends beyond the areas or periods of their implementation.26 Rather, it highlights the vital role that responsible government interventions and rights-respecting tech companies play in moderating content on their platforms, especially in times of crisis.27

Countries entrenched in repeat offenses and prolonged shutdowns

As the COVID-19 pandemic continued to recede in many parts of the world in 2022, shutdowns outstripped pre-pandemic levels and reached grim milestones. The number of shutdowns in countries other than India topped 100 for the first time, and nine countries — Bangladesh, India, Iran, Jordan, Libya, Myanmar, Sudan, Turkmenistan, Ukraine (imposed by Russia) — had at least four shutdowns in 2022, compared with seven countries with at least four shutdowns in 2019. In the context of political upheaval, protest movements, violence, and active conflict, millions of people across these nine countries experienced frequent and severe shutdowns with disturbing regularity. These recurring shutdowns, whether implemented as a knee-jerk reaction to protests, through internet curfews, or through deliberate attacks on infrastructure during conflict,28 exacerbate the well-documented harms of internet shutdowns and amount to thousands of total hours without connectivity.
We also saw prolonged shutdowns continue in full force, affecting entire regions and countries. In 2022, a record 16 shutdowns carried over from 2021, including a protracted shutdown in Tigray, Ethiopia, a blanket shutdown in regions across Myanmar, and nine continuous platform blocks. As 2022 rolls into 2023, another set of 16 shutdowns are still in place in many of the same countries, with 12 of these having lasted at least one year. The justifications authorities offer are flimsy and insufficient as time passes and we continue to see the violation of a broad spectrum of human rights. By the end of 2022, the people of Tigray had endured 787 days of a full communications blackout, and today it is the longest shutdown currently in effect. Also by the end of 2022, many regions across Myanmar had been in the dark for more than 460 days, and disruptions continue to escalate.

Targeted shutdowns and their immeasurable harms

As we’ve documented in recent years, some governments are becoming more sophisticated and intentional about how they implement shutdowns, evidently to more directly target certain groups, as well as to minimize economic repercussions. In 2022, 23 countries implemented or maintained 28 communications platform blocks, similar to the 22 countries with 29 platform shutdowns in 2021. Authorities and other actors, such as military aggressors, continued to impose targeted mobile network shutdowns. This was a popular tactic during protests (26 times), as a means of silencing people while allowing wealthy elites, government officials, and certain businesses to operate on broadband, fixed-cable internet.

---

29 See supra note 7.
30 See supra note 3.
Given the increasing technical expertise of state actors in censoring, surveilling, and shutting down access to the global internet, authorities or other actors began to institute multi-layered shutdowns in places like Iran, Jordan, Turkmenistan, Ukraine, and Uzbekistan. While Iranian authorities imposed broad app blocking, they also targeted regional hotspots with curfew-style mobile shutdowns. The Russian military used missile strikes to attack communications infrastructure in multiple cities in Ukraine, while also reportedly launching cyber attacks against Ukrainian internet providers.  

Perpetrators also used shutdowns in evident attempts to force people onto alternative platforms and infrastructure where surveillance and censorship is easier to implement. After imposing two shutdowns weeks apart in occupied Kherson, Russia reportedly re-routed connections from Ukrainian ISP KhersonTelecom to Russian-controlled internet providers and infrastructure, using a fiber optic cable connected via Crimea. Similarly, in May 2022 in Iran, it appears authorities blocked access to the global internet, but maintained access to the National Information Network (NIN). Turkmenistan, which implemented four shutdowns in 2022, is reportedly developing a centralized, national intranet suggesting that internet shutdowns may serve as a warning sign that a government will take additional technical measures to assert more control over digital spaces.

<Communications platform blocking in 2022>  

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1 city, county, or village]</td>
<td>[more than one city in the same state, province, or region]</td>
<td>[locations in more than one state, province, or region]</td>
<td>[areas in the country unclear]</td>
</tr>
</tbody>
</table>

35 See supra note 28.
IV. Internet shutdowns by region
Although 2022 marked a record low for the annual number of shutdowns in the region since we started tracking in 2016, Africa is still home to the world’s longest currently active shutdown globally in Tigray, Ethiopia. At least four of the region’s nine shutdowns took place alongside reported human rights abuses, both in the context of violent crackdowns on protests and active conflict. Elections have historically been a significant trigger for shutdowns across Africa, but there were relatively fewer elections in the region in 2022, and we documented one ongoing election-related platform shutdown in Uganda that had been in place since 2021. Since there will be more elections in 2023, Access Now and #KeepItOn coalition will continue to closely monitor the situation.

### Ethiopia
- Ongoing Tigray shutdown reached 787 days at end of 2022

### Uganda
- Ongoing Facebook block reached 719 days at end of 2022

### Burkina Faso: 2
- Sierra Leone: 2
- Somaliland: 1
- Zimbabwe: 1

### Shutoffs targeting platforms
- Burkin Faso: 1
- Nigeria: 1
- Uganda: 1

### Regional overview in 2022

<table>
<thead>
<tr>
<th>Country</th>
<th>2021 Shutdowns</th>
<th>2022 Shutdowns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethiopia</td>
<td>19</td>
<td>9</td>
</tr>
<tr>
<td>Uganda</td>
<td>12</td>
<td>7</td>
</tr>
</tbody>
</table>

- 44.5% of shutdowns related to protests
  - Sierra Leone: 2
  - Somaliland: 1
  - Zimbabwe: 1

- 33.3% of shutdowns targeted platforms
  - Burkin Faso: 1
  - Nigeria: 1
  - Uganda: 1

---


40 See supra note 19.

“national security” as a justification. A few weeks later on January 23, following reports of a coup attempt, the government once again cut off mobile connections across the country, restoring access two days later.

When anti-government protests escalated in Sierra Leone over the rising cost of living, authorities flipped the kill switch to quell the protests. The last time the government of Sierra Leone imposed internet shutdowns was in 2018, during elections.

Similarly, authorities in Somaliland, a self-declared state within the internationally recognized boundaries of Somalia, shut down internet access in a knee-jerk reaction to protests which erupted in August 2022 following the postponement of presidential elections. The shutdowns, which affected the Woqooyi Galbeed region as well as parts of Southern and Central Somalia, lasted about 10 hours. In 2017, Somaliland authorities shut down access to social media during elections.

Finally, Zimbabwean authorities intermittently disrupted internet service in an attempt to interfere with the “Yellow Sunday” rally held by the opposition party Citizens’ Coalition for Change. As supporters gathered for the rally, people began to report difficulty accessing social media platforms. Zimbabwe has previously imposed internet shutdowns to quash protests.

Shutdowns during elections

Elections, often linked with protests and unrest, have long been a consistent trigger for internet shutdowns in Africa. As we have noted, the record-low number of election-related shutdowns in 2022 (one ongoing shutdown in Uganda from 2021) is likely due to the relatively small number of elections that took place. It’s also possible that civil society advocacy played a role in dissuading authorities from interference.

The Gambia was on our elections watchlist, and in April 2022, the country maintained access to the internet throughout its legislative elections, despite a history of imposing elections-related shutdowns dating back to 2016.

Kenya, meanwhile, made and kept its commitment to #KeepItOn during the August 2022 general election, standing out as a leader among its neighbors in East Africa. That includes Uganda, which had blocked Facebook ahead of the January 2021 general elections and to date has not lifted the block.

Kenya’s government does not have a history of shutdowns, but it was on our elections watchlist due to increasing political tensions and the rampant spread of misinformation online. To prevent an election shutdown, Access Now and our coalition partners hosted trainings for journalists, human rights activists, and politicians to improve understanding of the risks of internet shutdowns.

48 Ibid.
52 See supra note 9.
defenders, and election observers, and maintained steady pressure on the Kenyan government and telecom executives to #KeepItOn throughout the 2022 general election period.65

Ahead of the Kenya election, then Interior Cabinet Secretary, Fred Matiang’i, indicated the government had no intention of shutting down the internet.66 He did, however, make it clear the government intended to take the spread of misinformation and hate speech seriously.67 After research by the human rights organization Global Witness revealed that Meta’s Facebook approved ads with hate speech,68 the National Cohesion and Integration Commission (NCIC) threatened to block the platform in Kenya unless Meta took measures to curtail the spread of hateful content. The agency gave Meta seven days to meet its demands.69 Several civil society organizations and a number of government officials condemned this threat out of concern for free expression surrounding the elections. Ultimately the government confirmed that neither the internet nor social media platforms would be blocked.60

Since election shutdowns remain a threat, Access Now and the #KeepItOn coalition will track elections in 11 countries in Africa in 2023, all of which have previously imposed shutdowns.70 This is an important opportunity for the democracies of Africa to chart a new course, with strong commitments to #KeepItOn throughout their election periods.

**Sustained platform blocks**

In 2021, the governments of Nigeria62 and Uganda63 each took action in evident retaliation against social media platforms that removed posts by government leaders or their followers. After the platforms removed these posts because they failed to meet the terms of service, government authorities blocked the platforms entirely.

Nigeria’s government blocked access to Twitter for a full seven months, sparking widespread public outcry.64 Authorities only lifted the block in January 2022 following extensive negotiations with the company.65 Civil society groups sued over the legality of this Twitter ban, and in 2022, they secured an important victory with the Community Court of Justice of the Economic Community of West African States (ECOWAS Court) declaring the blocking unlawful.66

The Ugandan government, meanwhile, has persisted in blocking Facebook for more than two years, and as of February 2023, Ugandans can only access it by using VPNS.67

---


61 See supra note 19.


63 See supra note 54.


67 See supra note 39.
INTERNET SHUTDOWNS IN 2022

// Ethiopia

Ethiopia’s Tigray region has been shut off from telecommunications services since the beginning of the civil war on November 4, 2020.68 A peace agreement between Ethiopia’s federal government and the Tigray People’s Liberation Front (TPLF) — which includes government commitments to restore access to essential services across the region — began to take hold in November 2022.69 But we have only started to see limited connectivity since December 2022, when Ethio Telecom began infrastructure repairs. As of February 2023 the majority of people in the region remain disconnected, and those who have regained some access are largely struggling with slow speeds and limited 2G services.70

The years-long internet shutdown in Tigray and affected neighboring communities paints a vivid picture of how devastating and dangerous these acts of disconnection can be. Aside from the immediate impact of cutting off the region’s six million people from the rest of the world, the ongoing communication blackout has resulted in multifaceted threats to Tigrayans’ fundamental rights.71 Since it is one of the longest uninterrupted internet shutdowns to have taken place during active conflict, it has also had a harrowing impact on people’s lives.72 The shutdown provided a cover for warring parties to commit heinous crimes, including systematic and widespread murder, rape, and sexual violence against vulnerable groups.73 It also prevented delivery of humanitarian aid to affected communities suffering from famine and other privations. No one could rely on basic services such as healthcare, banking, employment, and education.

Despite the horrors of the civil conflict and Tigray shutdown, digital rights activists and human rights defenders demonstrated enormous resilience, persisting in drawing the world’s attention to the rights violations happening in their communities.74 In solidarity, Access Now and the #KeepItOn coalition worked with local partners and members of the Ethiopian diaspora to amplify Tigrayan voices and demand accountability for the shutdown. We brought together more than 100 civil society organizations and individuals from more than 102 countries to urge the African Union to take action to end the shutdown.75 When Ethiopia hosted the annual Internet Governance Forum in November 2022, our coalition worked to move the situation in Tigray to the top of the global agenda.76

See the Middle East & North Africa (MENA) chapter for information on shutdowns in Algeria, Tunisia, Libya, and Sudan.

68 See supra note 11.
70 See supra note 11.
75 See supra note 12.

Shutdown impact story: Tigray

“I remember the days I woke up and tried calling different numbers every single day hoping that one of my family members would be able to pick up. It is the worst situation that a human being can be in, [not knowing] if your family members are alive or not. Hearing [reports of] all the drone strikes on civilians used to make me lose my mind. I was not able to focus on my school & work. I used to see my siblings in my dreams and eagerly wanted to talk to them but I was not able to for 2+ years. Even now I am still not able to reach out to a few family members because internet access is not restored in all cities of Tigray region.”

A young Tigrayan woman based in the U.S.
Asia Pacific Regional overview in 2022

**Myanmar:** 7
Longest ongoing shutdown exceeded 540 days as of March 2023

**India:** 84
Most shutdowns recorded in the world for five consecutive years

Bangladesh: 6  Afghanistan: 2  China: 1  Pakistan: 1  Sri Lanka: 1

Mobile vs. broadband shutdowns in the region

<table>
<thead>
<tr>
<th>Mobile</th>
<th>Broadband</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>82</td>
<td>16</td>
<td>4</td>
</tr>
</tbody>
</table>

1.2 billion mobile internet users in the region (source: Global System for Mobile Communications Association)

---

**Myanmar**

In Myanmar, the military crackdown on those resisting the regime after the coup d'état two years ago has included the use of internet shutdowns to facilitate and shroud serious human rights violations and sever communications between individuals and communities. At present, we can verify at least seven shutdowns in 2022; however, this number underplays the full range and nature of connection disruptions across the country. In reality, through 2022, the military consolidated control of all telecommunications providers in Myanmar, expanded surveillance infrastructure across the country, and shut down mobile and internet connections both consecutively and erratically across regions. This has posed a severe challenge for local partners as they work to verify the frequency and duration of shutdowns. Nevertheless,

---


our coalition continues to document additional discrete instances of shutdowns, particularly those targeted at specific communities, and we will continue to update Access Now’s STOP database\(^{80}\) as new information becomes available.

Regardless of the final total, emerging information coming from trusted #KeepItOn coalition partners and people on the ground highlight the breadth and severity of shutdowns in the country. According to our partners, as of March 2023, the longest ongoing shutdown in Myanmar had been in place in Hpakant township in Kachin state for more than 18\(^{81}\) months, and approximately 50\(^{82}\) townships had been cut off for more than one\(^{83}\) year. Of these, more than 20\(^{84}\) townships faced shutdowns for the entirety of 2022 and for more than 500\(^{85}\) days, and at least 25\(^{86}\) townships faced shutdowns for 10\(^{87}\) months of 2022. Partners also reported shutdowns across the Sagaing, Magway, and Mandalay regions, and Shan, Chin, Kachin, and Kayah states, with the most affected areas being Sagaing, Magway, and Chin, where resistance to the military is strongest. Meanwhile, across the country, all 330\(^{88}\) townships have been subjected to shutdowns at least once in 2022, with many experiencing daily mobile and broadband shutdowns on top of other communications blackouts. Since there is ongoing armed conflict, some of these shutdowns were likely the result of damage to network infrastructure. People in remote areas have also been suffering from temporary outages due to lack of electricity or petrol, particularly in Kayah state.

These shutdowns are strategic. The Myanmar junta continues to actively and regularly impose disruptions prior to and during military attacks on villages, to shroud its “scorched earth” strategy\(^{89}\) of killings, torture, ill-treatment, and arrests,\(^{90}\) as well as widespread arson of property.\(^{91}\) Even when there are no military attacks, people in these villages have suffered from ongoing connectivity challenges, as significant price hikes for internet access\(^{92}\) and expanded regulations for IMEI and SIM card registration\(^{93}\) supplement shutdowns to make connectivity an exception rather than the norm. In regions where mobile connectivity continues, individuals are forced to use networks run by military-owned telecommunications providers, such as Myanmar Posts and Telecommunications (MPT) and

---

**Shutdown impact story: Myanmar**

“We have been facing significant challenges trying to confirm where there is connectivity and where it has been cut off in Myanmar. After the coup, with every passing month, more activists are forced to leave Myanmar for security reasons, while still trying to connect with and support people within. We know what the ‘right’ or ‘secure’ ways to communicate are, but we simply cannot use them. VPNs do not work in some regions, nor do calls on encrypted apps like Signal. In some places, we can only communicate over military-owned telecom operators’ networks, even when we know it is very risky. Many times, we have to communicate with intermediaries for people’s safety, so we struggle to get direct information. Everything we do is being monitored — the military is conducting house raids, freezing our bank accounts and mobile banking apps, monitoring financial transactions, tracking SIM cards and phone IMEIs, stopping the issuance of passports to control people flying in and out... All while burning villages, looting homes, and our family and friends have to keep moving to avoid capture. Their aim is to kill the resistance, and they will stop at nothing.”

A human rights defender

---

\(^{80}\) See supra note 7.


\(^{82}\) See supra note 33.


Weapons of Control, Shields of Impunity

Mytel, as those networks are the only remaining means of communication. While some telcos have recorded occasional temporary restoration of connectivity or 2G access in affected areas, there have also been increasing reports of highly targeted restrictions on mobile and phone lines.

While some telcos have recorded occasional temporary restoration of connectivity or 2G access in affected areas, there have also been increasing reports of highly targeted restrictions on mobile and phone lines.

India, which was responsible for 84 shutdowns in 2022, remains the country with the highest number of recorded shutdowns in the world — for the fifth consecutive year. Authorities disrupted internet access at least 49 times in Jammu and Kashmir due to political instability and violence, including a string of 16 back-to-back orders for three-day-long curfew-style shutdowns in January and February 2022. Though brief, rare spells of uninterrupted internet access in the region delivered clear benefits for women and small-business owners, further proof that internet access is vital for realizing economic security and closing the gender digital divide.

In 2021, around 80% of all shutdowns in India were in Jammu and Kashmir, compared to 58% in 2022. Authorities in regions across the country are increasingly resorting to this repressive measure, inflicting shutdowns on more people in more places. Setting aside Jammu and Kashmir, authorities in West Bengal (7) and Rajasthan (12) imposed more shutdowns than authorities in other regions in India, responding to protests, communal violence, and exams with disruptions that impacted the daily lives of millions of people for hundreds of hours in 2022. Although we counted fewer than 100 shutdowns in India for the first time since 2017, we’re not convinced Indian authorities have embarked on the path toward positive, sustained change with regard to digital rights. Legal challenges against shutdowns, fewer mass protests in the aftermath of the COVID-19 pandemic, and the sustained and increasing crackdown on dissent may have increased administrative friction or reduced the incentives for authorities to impose shutdowns. At the same time, the government’s persistent failure to publicly release shutdown orders in violation of the Supreme Court’s judgment, and the technical challenges in monitoring, tracking, and recording shutdowns — in particular in communities where shutdowns are an emerging issue — likely mean we have not yet recorded all disruptions. In addition, the proposed Draft Indian Telecommunication Bill, which would empower central and state governments with unrestricted powers to impose shutdowns when “necessary and expedient,” signals the government’s intention to continue down this troublesome path,

Shutdowns documented in Myanmar, August 2021 to March 2023 (verified as of February 2023)

- **540+ days**
  - Hpakan township in Kachin
- **500+ days**
  - 20+ townships across Sagaing, Magway, Mandalay, Chin, and Kachin
- **365+ days**
  - Approx. 50 townships across Sagaing, Magway, Mandalay, Chin, Kachin, and Kayah

// India

India, which was responsible for 84 shutdowns in 2022, remains the country with the highest number of recorded shutdowns in the world — for the fifth consecutive year. Authorities disrupted internet access at least 49 times in Jammu and Kashmir due to political instability and violence, including a string of 16 back-to-back orders for three-day-long curfew-style shutdowns in January and February 2022. Though brief, rare spells of uninterrupted internet access in the region delivered clear benefits for women and small-business owners, further proof that internet access is vital for realizing economic security and closing the gender digital divide.

In 2021, around 80% of all shutdowns in India were in Jammu and Kashmir, compared to 58% in 2022. Authorities in regions across the country are increasingly resorting to this repressive measure, inflicting shutdowns on more people in more places. Setting aside Jammu and Kashmir, authorities in West Bengal (7) and Rajasthan (12) imposed more shutdowns than authorities in other regions in India, responding to protests, communal violence, and exams with disruptions that impacted the daily lives of millions of people for hundreds of hours in 2022. Although we counted fewer than 100 shutdowns in India for the first time since 2017, we’re not convinced Indian authorities have embarked on the path toward positive, sustained change with regard to digital rights. Legal challenges against shutdowns, fewer mass protests in the aftermath of the COVID-19 pandemic, and the sustained and increasing crackdown on dissent may have increased administrative friction or reduced the incentives for authorities to impose shutdowns. At the same time, the government’s persistent failure to publicly release shutdown orders in violation of the Supreme Court’s judgment, and the technical challenges in monitoring, tracking, and recording shutdowns — in particular in communities where shutdowns are an emerging issue — likely mean we have not yet recorded all disruptions. In addition, the proposed Draft Indian Telecommunication Bill, which would empower central and state governments with unrestricted powers to impose shutdowns when “necessary and expedient,” signals the government’s intention to continue down this troublesome path.


INTERNET SHUTDOWNS IN 2022

Shutdown impact story: Meghalaya, India

“I saved myself enough money to buy a smartphone and then wanted to use it to my advantage. Therefore I got engaged with [a food ordering app] and started delivering. The money I earn is on a daily basis. It depends on the number of deliveries I make in a day, but with mobile internet not working, I have nothing to do and have not made a penny for the last five days.”

———

A food delivery worker

“Our primary mode of transaction is Google Pay. Customers are not able to pay us neither are we able to pay for the stuff we buy for the shop. It is a problem.”

———

A small business owner

These two stories were reported by Abha Anindita in the article Pain of living without mobile internet on The Meghalayan. For the full story, visit https://themeghalayan.com/pain-of-living-without-mobile-internet/.

violating fundamental rights of expression and assembly and providing opportunities to cover up human rights abuses. In addition to shutdowns, Indian authorities have honed their playbook by increasing censorship, blocking websites, and issuing takedown orders to social media platforms.

India’s expanding censorship toolkit

From 2015 to 2022, Indian authorities blocked at least 55,607 websites, URLs, applications, social media posts, and accounts.92 These censorship acts have been steadily on the rise, with the government blocking 2.4 times, or 142%, more social media posts in 2022 than 2018.93

<table>
<thead>
<tr>
<th></th>
<th>Shutdowns</th>
<th>Takedown orders (social media posts and accounts)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022</td>
<td>84 (21% ↓)</td>
<td>6775 (11% ↑)</td>
</tr>
<tr>
<td>2021</td>
<td>107</td>
<td>6096</td>
</tr>
</tbody>
</table>

Shutdowns during protest and unrest

Elsewhere in the Asia Pacific region, Pakistan95 and Bangladesh96 ordered shutdowns during protests, and China,97 Afghanistan,98 and Sri Lanka99 blocked social media services. On April 3, 2022, in an attempt to quell widespread protests against the president’s declaration of a state of emergency, the Sri Lankan Telecommunications Regulatory Commission banned all social media services across Sri Lanka.100 The shutdown accompanied a recent spike in censorship, information regulation, and isolation from the outside world — all markers of a government’s descent into digital authoritarianism.

94 Ibid.
As countries in Eastern Europe and Central Asia (EECA) sink deeper into authoritarianism, internet shutdowns and censorship have become increasingly prevalent during protests and elections. In the context of conflict and crisis across the region, from Russia’s attacks on Ukraine to governments’ violent crackdowns on protests across Central Asia, authorities have weaponized internet shutdowns to keep people in the dark and to carry out human rights abuses with impunity.

**Central Asia**

Across Central Asia, authorities imposed shutdowns with regularity during protests, denying people’s rights to freedom of expression and access to information in attempts to silence dissent and cover up abuses of power. The impacts have been devastating, disrupting people’s access to food, healthcare, education, and life-saving information.

In January 2022, the Kazakhstani people were subjected to a week of nearly constant shutdowns as protests escalated over the price of gas. The violent and disproportionate crackdown on protesters by police and security services resulted in the deaths of hundreds of people and detention of thousands. Shutdowns implemented by the Kazakhstan government left millions in the dark, causing cash and food shortages as mobile payment services were disrupted and debit card machines malfunctioned.

---

101 See supra note 32.
102 Ibid.
INTERNET SHUTDOWNs IN 2022

Shutdown impact story: Tajikistan

“I owned two pharmacies in Khorog, where I come from. We provided medications and medical supplies to hospitals and individuals. The internet played a key role in this business, since all transfers, settlements with suppliers, filing taxes, basically, all business control was carried out remotely via the internet.

But everything changed for me and my business when authorities in Tajikistan imposed a four months-long internet shutdown to quell protests in Khorog. My business was undoubtedly hit hard as we couldn’t operate efficiently anymore. I was forced to let go of my staff and eventually closed down the business. I lost over [USD] $15,000.”

A businessman in Khorog

Uzbek and Tajik authorities also met protests with violent crackdowns and internet blackouts in the autonomous region of Karakalpakstan, and the Gorno-Badakhshan Autonomous Region (GBAO), respectively — highlighting the disproportionate impact shutdowns often have on marginalized communities like the Karakalpak and Pamiri ethnic groups.

Authorities in Turkmenistan and Uzbekistan both implemented communications platform shutdowns, a tactic they have increasingly deployed in the past few years alongside censorship of websites and blocking of VPNs in an effort to control information and squash dissent.

// Russia’s invasion of Ukraine

In 2022, during the course of Russia’s full-scale invasion of Ukraine beginning in February, the Russian military imposed 22 shutdowns on Ukrainian cities and oblasts through a combination of cyber attacks, targeted air strikes, and deliberate dismantling of telecommunications infrastructure. Russia has systematically targeted civilian infrastructure across Ukraine, attempting to break down popular resistance to the invasion, restrict the flow of information, and inflict damage to communities in retaliation when Ukraine has successfully forced Russian troops out of occupied cities. These tactics have inflicted devastating harms, and at least 12 of the 22 shutdowns that occurred in Ukraine took place in parallel to documented human rights abuses. Lack of electricity, water, and food, combined with indiscriminate and brutal killings of civilians have been common throughout the invasion, often alongside disrupted communications and internet blackouts. In response, Ukraine has set up 4,000 “invincibility centers” where people can get warm, eat, charge devices, and connect to the

---

109 See supra note 28.
The government is also requiring ISPs to stock enough batteries, generators, and solar panels to stay online for at least three days in the case of blackouts. In formerly occupied Kherson, one of the areas Russia attempted to use as a foothold to serve as a base for its incursions deeper into Ukrainian territory, Russian forces systematically worked to displace Ukrainian telecommunications services with Russian ones, going so far as to reroute traffic and even lay new fiber optic cables from Crimea. These efforts resulted in significant lapses in connectivity for Ukrainians, and where Russia restored connection, it forced people onto the heavily censored and surveilled Russian internet.

Ukraine fought back against Russia’s efforts, with Ukrainian service providers implementing blocks where Russia had gained access to their equipment, and Ukrainian intelligence services destabilizing the newly run fiber optic cable. While important acts of resistance, the battle for control over telecommunications infrastructure further exacerbated disruptions in service for the people of Ukraine.

The Russian government also implemented two shutdowns at home — blocking access to Twitter, Facebook, and Instagram — as part of its crackdown on dissent and persistent efforts to enforce its own propaganda as the prevailing narrative surrounding the invasion. As a response to Russia’s pressure on platforms, TikTok took its own measures to severely limit access to its services in the country. At the same time, countries around the world rallying in support of Ukraine imposed a series of heightening sanctions against Russia, some explicitly targeting tech services, and other more general restrictions that created uncertainty about how they applied to services supporting access to the global internet inside Russia. Both U.S. and U.K. authorities took swift action responding to civil society’s calls for exemptions, to ensure that human rights defenders, journalists, and millions of others inside Russia could stay connected with the international community, access reliable information, and continue their resistance.

// Armenia-Azerbaijan territorial dispute

As the military conflict between Armenia and Azerbaijan over disputed territory has heightened since 2021, so too has both countries’ use of internet shutdowns and other tactics for information control. In the days following Azerbaijan’s military offensive in the disputed territory on September 14, 2022, authorities in both countries blocked TikTok, marking the first time on record Armenia deliberately blocked platform access.

---


112 Ibid.


114 See supra note 28.


Latin America and the Caribbean Regional overview in 2022

Cuba: 2
3 consecutive years of shutdowns

Brazil: 1
Return to court-ordered platform shutdowns

Brazilian courts have ordered blocks of Facebook (2016) and Telegram (2022) in a disproportionate response to content governance issues

Shutdown impact story: Cuba

"Internet shutdowns affect communication with sources, and the ability to know or verify what is happening at that moment, since the Cuban regime cuts the service mostly when there are protests and mass arrests. As a result there is a state of total isolation that prevents me not only from reporting on social networks, but also from communicating with my family, and given the harassment of independent journalists in Cuba, it is normal that my family is worried about these situations."

Cynthia de la Cantera Toranzo, Cuban independent journalist

Photo: Tim Stahmer
Though the Latin America and Caribbean region has seen fewer instances of internet shutdowns in 2022 relative to other regions, a number of repeat offenders have relied on shutdowns to quell dissent, restrict the flow of information, and apply pressure on social media companies to comply with government orders. Shutdowns undermine people’s ability to make their voices heard, participate in democratic processes, and to stay safe and connected during periods of unrest, and are a fundamental threat to human rights.

/// Cuba

Since mobile internet first became available in Cuba in December 2018, it has become a vital resource for activists and journalists. But Cuba has also quickly risen to the top of the list of the region’s most persistent perpetrators of internet shutdowns. In July 2022, Cubans protested in Los Palacios and Pinar del Rio, and in September, engaged in nationwide protests. Each time, they were subjected to complete blanket shutdowns for hours. The motivation for both protests was anger over persistent power outages, including in the aftermath of Hurricane Ian, when electricity was slow to return to many regions of the country. The island is particularly vulnerable to complete shutdowns, since there is just one telco run by the government, ETECSA, and only one fiber optic submarine cable connection to the global internet. In late 2022, the U.S. moved to reject an application to build a second submarine cable to Cuba, citing ill-founded national security concerns. With the government’s mounting track record of resorting to internet shutdowns in the face of public dissent, we are closely monitoring Cuba as its parliamentary election approaches in March 2023.

/// Brazil

In Brazil, the Supreme Court ordered a block of Telegram in March 2022 after the company failed to comply with previous orders by police and judicial authorities to remove misinformation in the lead-up to the presidential election. The block lasted two days, and was lifted once the court was satisfied with Telegram’s content moderation changes. Blocking entire platforms is always a disproportionate response and cannot be justified as a mechanism for dealing with content governance issues. Yet Brazil’s courts have a history of blocking popular social media platforms across the country, including an order to block Facebook in 2016 when it failed to take down a parody account, and a series of orders to block WhatsApp as punishment for failing to comply with requests for user data.

As Telegram’s services have become both more vital for human rights defenders and communities at risk and a more dangerous forum for the spread of harmful content, civil society has repeatedly called on the company to increase its engagement and to adopt stronger policies in defense of human rights. Telegram and similar platforms have a responsibility to ensure their services do not perpetuate human rights harms, and to make the investments and design choices necessary for them to be able to respond in real time as threats emerge. Their failure to do so has increasingly incentivized governments to take extreme measures in responding to misinformation, hate speech, and incitement to violence online, and likewise provided an easy excuse for governments seeking to disrupt access to information.

124 See supra note 19.
INTERNET SHUTDOWNS IN 2022

Middle East and North Africa Regional overview in 2022

**Iran:** 18
15 of 18 shutdowns in Iran happened during the nationwide protests for women’s rights and regime change in Iran

**Sudan:** 4
Repeated shutdowns by the military regime during protests across the country

Jordan: 4  Libya: 4  Algeria: 1  Iraq: 1  Oman: 1  Syria: 1  Tunisia: 1  Turkey: 1  Yemen: 1

24.3% of shutdowns in the region were service-based, usually blocking access to messaging and social media platforms

Jordan: 3  Iran: 2  Algeria: 1  Oman: 1  Tunisia: 1  Turkey: 1

Across the MENA region, authorities have increasingly relied on internet shutdowns to suppress dissent, undermine political participation, and shield perpetrators of human rights abuses from accountability. The region saw both an emergence of new shutdowns and the continuation of disruptions communities have endured for years — including ongoing airstrikes in Yemen impacting telecommunications infrastructure and social media platform blocking in Oman continuing from 2021. Authorities took aim at both social media platforms and mobile data services, targeting specific communities in moments of heightened risk.

**For example, in Libya — where people have grown increasingly frustrated with the feuds of political elites, neglect of public services, and government failure to schedule elections amid political deadlock — protesters stormed the parliament building on July 1, and authorities responded by shutting down internet and telecommunication services across the city of Tobruk.**

Authorities also imposed disruptions in the cities of Darna, Tobruk, and Benghazi coinciding with visits from Khalifa Haftar, the Commander-in-Chief of the Tobruk-based Libyan National Army. While shutdowns are becoming more entrenched, affected communities

---

WEAPONS OF CONTROL, SHIELDS OF IMPUNITY

are also becoming more resilient, continuously devising new tactics for staying connected, raising their voices, and holding the powerful to account.

Platform blocks

In Jordan, authorities returned to a familiar tactic of blocking social media platforms in the face of protests and unrest. While truck drivers led protests against rising fuel prices in mid-December 2022, and authorities were already imposing daily mobile shutdowns in the southern cities of Maan and Karak, the government also separately ordered a ban of TikTok, which was being used to livestream the ongoing protests. Jordan's Public Security Directorate stated that the ban was a result of TikTok's misuse and its failure to deal with content that "incites to violence and chaos." While the Jordanian Minister of Telecommunications stated in a media interview that TikTok would be blocked until it agrees to their conditions to "control content," there are reports that TikTok has been in negotiations with the government to lift the ban. Jordanian authorities previously blocked Facebook Live during 2021 protests regarding COVID-19 restrictions. They also blocked Clubhouse, the social media audio chat platform, the same year, and it remains blocked to this day. Jordanian authorities have also intensified VPN blocking in the last few years, and many popular VPN services and servers remain inaccessible. Turkish authorities responded to deadly explosions in Istanbul in November 2022 by restricting broadcast media and throttling social media platforms, restricting the flow of information in a moment of danger and uncertainty.

Tunisia implemented a shutdown for the first time since the 2011 revolution, blocking access to Zoom and Microsoft Teams in an attempt to prevent the Assembly of People’s Representatives (ARP) from convening virtually, after the president dissolved the legislative body. President Kais Saied had already moved to suspend the parliament on July 25, 2021, and the political crisis escalated further on March 30, 2022, when 123 Tunisian MPs attempted to take part in an online plenary session. After the two platforms were blocked, MPs moved to another online platform, GoToMeeting. President Saied responded by announcing a state of emergency in accordance with the provisions of Article 80 of the Tunisian Constitution, dismissing the Prime Minister, dissolving the ARP entirely, and lifting the immunity of its members.

Video platforms like these are necessary communication tools used by Tunisian citizens on a daily basis for professional purposes and to defend human rights, and cutting or disrupting access, even if temporary, is incompatible with international human rights law and Article 38 of the 2022 Tunisian constitution.


146 Ibid.
Exam-related shutdowns

School exams continued to be a primary driver of shutdowns in Sudan, Algeria, Syria, Jordan, and Iraqi Kurdistan, as authorities try — and fail — to curb cheating and the leaking of exam questions. This disproportionate practice violates the human rights of millions of people in addition to students, disrupts daily life, and impedes the population from exercising social, economic, and cultural rights. Despite the demonstrated failure of this practice as a cautionary measure, governments continue to implement internet shutdowns during national exams. For instance, and for the first time in its long history of shutdowns during exams, Iraq has already blocked social media and messaging platforms at an early stage in the year, during the midterm exam session that took place in February 2023. We will continue to watch closely in 2023 to see if authorities in these countries will follow the same script during yearly exams or make good on their promises to address cheating without draconian shutdowns.

Iran

Iran has a long history of brutal repression, and the government is known for imposing increasingly sophisticated internet shutdowns to crack down on protests. In 2022, Iranian authorities imposed an unprecedented 18 shutdowns across the country, part of an escalating wave of digital repression responding to protests sparked by the death of 22-year-old Mahsa (Jina) Amini on September 16, 2022, while she was in the custody of Iran’s “morality police.”

After the news broke, dozens of people gathered in the streets of Amini’s hometown, Saqqez, in the Kurdistan Province, to mourn her death. Authorities quickly shut down the internet in Kurdistan and disrupted access to Instagram and WhatsApp nationwide. Protests spread rapidly across the country, with women and girls at the forefront chanting “woman, life, freedom,” and denouncing the morality police, or Guidance Patrol, a special unit tasked with enforcing Islamic dress code, including mandatory hijab for women. Women protesters cut their hair, burned hijabs, and defaced pictures of Ali Hosseini Khamenei, Iran’s Supreme Leader. As support grew, the movement evolved into a broader indictment of the government and an uprising for regime change. Authorities responded with excessive force, bringing their full toolkit of oppression to bear.

As protests persisted and grew, authorities proceeded to block access to the global internet and repeatedly shut down mobile networks, both nationally and in targeted areas, while also continuing to block Instagram and WhatsApp — cutting off access to two of the only social media platforms that have remained accessible in Iran in recent years. This layering of shutdown tactics was a clear attempt to hide atrocities and human rights violations. The government relied heavily on persistent social media blocks to prevent protesters from organizing and to keep news of atrocities and human rights violations from spreading. While they typically kept mobile networks online during work hours, an effort to minimize the economic impact of the disruptions,
The Iranian authorities imposed curfew-style mobile shutdowns in the evenings to prevent coordination and documentation of protests. The Iranian regime clamped down particularly hard on dissent in regions with marginalized groups, with 50% of all shutdowns in 2022 targeting ethnic minorities from the Kurdistan, Baluchestan, and Ahvaz regions through blanket, regional shutdowns.

Iran’s internet blocking tactics

The people of Iran have been developing strategies for resilience in the face of shutdowns for years, and likewise the government has continuously worked to counter their tactics. In 2022, to make it extremely difficult, if not impossible, for Iran’s tech-savvy youth to bypass social media blocks, the government began blocking access to VPNs and took steps to criminalize their sale. Recent reports have also revealed Iran’s use of a suite of tools known as “SIAM,” which, among other concerns, can target an individual’s mobile device to only allow access to 2G networks rather than 3G or 4G, both limiting data speeds to near-usable levels and making communication on the device much more vulnerable to surveillance. In addition, authorities cracked down on technologists and network administrators who either expressed public solidarity with the protests or criticized the authorities’ digital repression, preventing them from acting as a resource for people trying to get back online or secure their communications.

For months, internet shutdowns provided a cover for the Iranian authorities to brutally repress protesters with full impunity. As of December 2022, this had resulted in the death of more than 500 protesters and the arrest of more than 19,000 others. Despite international outcry, reports indicate 100 or more detained individuals are currently facing the death penalty, as the government uses public execution as a form of intimidation and control.

The crackdown and censorship in Iran drew international condemnation, with the U.S. lifting sanctions to increase internet freedom and access to information in Iran. For instance, the U.S. Department of the Treasury issued the Iranian regime targets VPNs to limit internet access by bringing U.S. sanctions guidance in line with the changes in modern technology since the issuance of the 2014 license, Iran GL D-1. Ultimately, this means U.S.-based companies can offer tools and services like video conferencing, e-gaming, and the arrest of more than 19,000 others.

157 See supra note 34.
e-learning platforms, automated translation, web maps, user authentication services, and cloud services to people in Iran with confidence they are not breaking U.S. law. Still, work remains to combat corporate overcompliance with sanctions, and to ensure that tech companies and financial intermediaries allow the free flow of all data, hardware, software, services, and transactions possible under the newly expanded license.\textsuperscript{166} Other actors like the European Union and the Freedom Online Coalition (FOC) — a network of 36 governments advancing internet freedom globally — issued statements to denounce the internet blackout and crackdown on protesters in Iran.\textsuperscript{167}

\textbf{Sudan}

For years, the people of Sudan have been fighting for democracy and respect for human rights in their country, but their movement has been repeatedly met with weaponized internet shutdowns and social media blocks designed to suppress dissent.\textsuperscript{168} Since forcibly taking power in October 2021, the military government has increasingly taken action against those who raise their voices to resist their military rule, including \textbf{four} internet shutdowns in 2022.

Mass protests and intermittent shutdowns gripped Sudan in the months following the October 2021 military coup.\textsuperscript{169} Authorities disrupted the internet for 12 hours on January 2, 2022,\textsuperscript{170} as thousands of people resumed their protests to demand the return of civilian rule, prompting Prime Minister Abdalla Hamdok to resign on January 3.\textsuperscript{171}

When people took to the streets across the country once again on June 30 in the “March of the Millions,” marking the third anniversary of the 2019 uprising and ousting of former Sudanese President Omar Al-Bashir, eight protesters\textsuperscript{172} were reportedly shot dead by the military amidst an internet blackout.\textsuperscript{173} Authorities similarly took mobile networks offline nationwide amid protests on the one-year anniversary of the military coup on October 25.\textsuperscript{174}

The military government has also taken aim at civil society organizations challenging the use of shutdowns in the country, including by revoking accreditation from the Sudanese Consumers Protection Society (SCPS), which has been a leader in challenging internet shutdowns through litigation.\textsuperscript{175} In 2021, SCPS helped get millions back online after a court ruled in its favor and ordered telecommunications companies to fully restore internet connectivity across the country.\textsuperscript{176}


The complexity and severity of internet shutdowns have continued to intensify in recent years, becoming a go-to weapon for perpetrators to crush dissent and exert control world over. The disastrous impact of these acts of digital authoritarianism motivates Access Now and the #KeepItOn coalition to keep going, and the network of partners working to end internet shutdowns has, in turn, grown stronger and more diverse.

The coalition

The coalition has grown to over 300 organizations in 105 countries committed to fight against internet shutdowns globally. Our community is rooted in collaboration and solidarity, with experts from across fields coming together to learn from each other and advance shared advocacy goals. In particular, coalition members and other grassroots partners on the ground work tirelessly to identify, report, and verify internet shutdowns, and to guide strategies for resistance and resilience. These efforts are aimed at safeguarding fundamental rights guaranteed under international human rights law.

The measurement community is also growing and building up its capabilities to track and monitor internet shutdowns effectively as shutdowns become more sophisticated, continuing to align on standards and best practices that make us all more effective and keep each other safe. New partners, including DT Institute, Haki Na Sheria, West African ICT Action Network, Core23Lab, and Libya Crimes Watch have joined our movement in 2022, and we look forward to collaborating with them further. Technologists and activists have also continued coming together to devise new strategies for circumventing, navigating, or mitigating the impact of unlawful censorship and disproportionate restrictions on free expression and other human rights, as well as to map the evolving face of shutdowns.

And communities that have been most directly impacted by shutdowns have shown incredible resourcefulness and resolve in advancing efforts to document shutdowns, as well as human rights violations taking place alongside them.

Together, the #KeepItOn coalition is investing in building up our collective capacity and delivering those resources to others who are willing to join us in our cause. In particular, we are strengthening our playbook around elections that are vulnerable to internet shutdowns, organizing trainings for journalists, civil society, and election observers, and pressing governments to make strong commitments to #KeepItOn throughout election periods.

The international community

Additionally, we continue to galvanize overwhelming support from the international community in the fight to #KeepItOn. Last year, Access Now and the #KeepItOn community felt solidarity from the national, regional, and international community in the fight against internet shutdowns. The UN Office of the High Commissioner for Human Rights (OHCHR) issued its first dedicated report on internet shutdowns, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, shining a spotlight on the devastating impact they have on human lives.

This high-level report builds on years of civil society action elevating the human rights impacts of internet shutdowns globally. The report underscored that shutdowns run directly counter to efforts to close digital divides, and the promise of the accelerated economic and social development that universal connectivity would bring, threatening the realization of the Sustainable Development Goals. The High Commissioner further highlighted a number of recommendations directed to key stakeholders including states, companies, and development agencies to take urgent measures and commitments to bring an end to internet shutdowns. Access Now and other members of the #KeepItOn coalition made written submissions informed by, and with data from,

---

177 See supra note 6.
180 See supra note 13.
the campaign, to educate and provide relevant information to the OHCHR.181

Following the release of the report, the European Union joined the OHCHR to launch a global campaign to raise awareness182 about the findings of the report as well as provide a spotlight on the challenges and threats183 activists face in the fight to #KeepItOn. They also organized virtual public events on internet shutdowns and continue to engage with the #KeepItOn community. In 2021, the Freedom Online Coalition (FOC) launched the Task Force on Internet Shutdowns (TFIS), which has strengthened its collaborations with civil society and other actors on internet shutdowns through periodic briefings on urgent country situations, coordinating joint actions, and compiling best practices and trend monitoring for dissemination through submissions, webinars, and meetings.

Moreover, the #KeepItOn coalition saw an increased number of public statements issued or actions taken by governments and global bodies to condemn internet shutdowns. For instance, as Iranian authorities brutally descended on anti-government protests in 2022, several actions were undertaken by the U.S.,184 FOC,185 the OHCHR,186 and the E.U.187 among others, to provide support or denounce the weaponization of shutdowns in the country. In another encouraging development, the E.U. imposed sanctions on various Myanmar authorities who restricted freedom of assembly and of expression by blocking internet access,” among other violations of human rights.188 Also, as the impact of internet shutdowns has become widespread, more and more people are speaking up against them, including the director of the World Health Organization (WHO).189

In addition, the impact of internet shutdowns is a key focus of the Technology for Democracy Cohort of the U.S. Summit for Democracy.190 The Tech for Democracy Cohort is co-led by Access Now, the U.K., and Estonia, bringing together stakeholders across civil society, the private sector, and governments to develop resources that advance shared goals in the fight against shutdowns and elevate the voices of people sharing how shutdowns have impacted their lives.191

The courts

The #KeepItOn coalition and its partners have relied on strategic litigation in various countries to bring an end to ongoing shutdowns or condemnation and accountability for past disruptions. In July 2022, the Community Court of Justice of the Economic Community of West African States (ECOWAS Court) passed a landmark ruling denouncing the Twitter blocking the Nigerian government had imposed for over seven months. The court ruled that the shutdown was unlawful and an affront to the rights of the people of Nigeria.192 This is the second time the ECOWAS Court has ruled against internet shutdowns

187 Council of the EU (2022).
192 See supra note 66.

**VI. What’s next**

While we made important strides in 2022, it is clear that the fight against internet shutdowns will continue, and waging that fight will require continued investments in the strength, diversity, and solidarity of our movement. We call on all stakeholders to do their part in advancing our cause to uphold free expression and keep people connected.

---

**To governments:**

Commit in law, policy, and practice to #KeepItOn at all times, and encourage other states to do the same.

---

**To tech companies:**

Collaborate with civil society to share details about how and when shutdowns impacting your services occur, and take the steps necessary to make your platforms and services resistant to shutdowns wherever possible. In particular, for social media platforms, make the appropriate investments in high-quality, human-led content moderation, reducing incentives and excuses for internet shutdowns, particularly in moments of crisis.

---

**To civil society:**

Join us! The #KeepItOn coalition is growing, and we welcome you among our ranks.

---

**To journalists, technologists, lawyers, and others:**

We welcome the opportunity to partner with you in documenting, circumventing, and pushing back against internet shutdowns wherever they occur.

---
INTERNET SHUTDOWNS IN 2022

CONTACT
For questions and more information, please visit: https://www.accessnow.org/keepiton/

Or reach out to:

Felicia Anthonio
#KeepItOn Campaign Manager, Access Now
felicia@accessnow.org
WEAPONS OF CONTROL, SHIELDS OF IMPUNITY
Internet shutdowns in 2022

#KeepItOn