THE RETURN OF DIGITAL AUTHORITY

THE RETURN OF DIGITAL AUTHORITARIANISM

Internet shutdowns in 2021

#KeepItOn
#KeepItOn

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 282 organizations 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 Marianne Díaz Hernández and Felicia Anthonio in collaboration with the Access Now team.

The authors would like to especially thank Sage Cheng, Donna Wentworth, Ángela Alarcón, Bridget Andere, Golda Benjamin, Raman Jit Singh Chima, Marwa Fatafta, Natalia Krapiva, Namrata Maheshwari, Peter Micek, Kassem Mnejja, Wai Phyo Myint, Melody Patry, Dhevy Sivaprasakam, Alexia Skok, Carolyn Tackett, and Anastasiya Zhyrmont for their contributions. They would like to thank Data4Change, Software Freedom Law Centre India (SFLC.in), Yodet, Miaan Group, Internet Outage Detection and Analysis (IODA), Athan, Kentik, Beam Reports, 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.

A note on our data

This #KeepItOn report looks at incidents of internet shutdowns documented by Access Now and the #KeepItOn coalition in 2021. 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.

April 2022

Table of contents

I. Internet shutdowns in 2021: A global overview 2
   1.1 Regional and country-specific snapshots of shutdowns 6
   Africa 6
   Asia Pacific 7
   Eastern Europe and Central Asia 8
   Latin America and the Caribbean 11
   Middle East and North Africa 12

II. Triggers of internet shutdowns in 2021 13
   2.1 Internet shutdowns during protests, political turmoil, and coups 15
       The Myanmar coup 15
       The Sudan coup 15
       Iran’s deadly crackdown on protests 16
       Other countries on the watch 16
   2.2 Internet shutdowns during elections 17
       How the #KeepItOn coalition is responding 19
   2.3 Internet shutdowns in active conflict zones 20
       Ethiopia: internet blackout in Tigray 20
       Israel’s attack on the Gaza Strip 22
       The Myanmar military’s ongoing digital coup 23
   2.4 Internet shutdowns during examinations 23

III. Notable trends and developments in 2021 25
   3.1 Prolonged shutdowns 25
   3.2 Increased use of mobile shutdowns during protests 25
   3.3 Targeted blocking of communications platforms 26
   3.4 Advancing technologies: combining throttling, blocking, and network shutdowns 28
   3.5 Shutdowns targeted to specific locations and populations 28

IV. Fighting back in 2021: challenges and opportunities 29
   4.1 Progress at the international level 29
   4.2 Progress in challenging internet shutdowns in court 30
   4.3 Progress on equipping civil society to circumvent and resist shutdowns 31
   4.4 Progress on collaborative monitoring and analysis of shutdowns 32

VI. Conclusion: our movement needs to keep growing 32
I. Internet shutdowns in 2021: A global overview

With a gradual return to normalcy following the outbreak of the global COVID-19 pandemic, we saw a dramatic resurgence of internet shutdowns in 2021. During this year, Access Now and the #KeepItOn coalition documented at least 182 internet shutdown incidents around the world in 34 countries, as compared to at least 159 shutdowns in 29 countries in 2020. We saw a global increase of 23 shutdowns from 2020 to 2021.

Following trends we’ve seen developing for years, in 2021 governments imposed both prolonged and increasingly targeted internet shutdowns, and relied on many of the same justifications for deploying these inherently disproportionate and drastic measures. Authorities in many countries imposed shutdowns in transparent efforts to silence critics and suppress dissent. Others wielded shutdowns to control the flow of information during elections and active conflict and war, including coups. In some cases, countries persisted in the harmful practice of disrupting internet access during school exams, a blunt method to discourage cheating.

India was responsible for 106 incidents of shutdowns documented in 2021, making it the world’s biggest offender for the fourth consecutive year. After India, Myanmar imposed the highest total number of shutdowns in 2021, with 15 disruptions, followed by Sudan and Iran with five shutdowns in each country. Over the past five years, our documentation shows that authorities have increasingly moved to disrupt the internet during events that affect the country’s political situation, such as elections, protests, coups, and violent conflicts. In particular, seven countries on our record that had never shut down the internet before joined the shame list in 2021: Burkina Faso, Niger, Palestine, Senegal, South Sudan, Eswatini (formerly Swaziland), and Zambia. On the other hand, in a positive development, countries including Benin, Iraq, and The Gambia, which had previously shut down the internet during key national events, kept access to the internet open during elections in 2021.

A close look at the 2021 data shows that what could have been a story about the global decline of internet shutdowns after the pandemic instead reveals a return to the rights-harming tactics of the pre-pandemic period. And these tactics are spreading. That’s especially troubling given our continued reliance on the internet to stay safe and healthy, connect to our loved ones, and fully participate in today’s digital world. It’s also yet another warning sign of the rise of digital authoritarianism across the globe.

In 2021, we saw shutdowns in conflict zones, and as a form of attack in conflicts, including before, during, and after two coups (Myanmar and Sudan). The shutdowns in Eastern Europe and Central Asia, including in Russia, point to the increased geopolitical tensions that we see exploding today. The continued trend of long shutdowns in Ethiopia, Myanmar, India, Pakistan, and elsewhere is an agonizing indicator of the willingness of government authorities to disconnect and deepen the suffering of their own people.

When we look at the resurgence of internet shutdowns in 2021, it is the human impact that matters most. Network disruptions can serve to cloak human rights abuses during crises.

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 people’s say or do. Access Now (n.d.) Retrieved March 30, 2021, from https://www.accessnow.org/keepit-on-faq/


including war crimes and acts of genocide.\(^5\) They obstruct humanitarian aid,\(^6\) and hinder journalism and the documentation of rights violations.\(^7\) They also leave people who have loved ones in these conflict zones in fear, unable to reach family and friends or get them to safety. In Myanmar, for example, shutdowns have blocked the capacity to report air strikes on civilians, the burning of houses, and extrajudicial killings and arrests, including of children.\(^8\)

Regardless of the context or rationale, internet shutdowns are an attack on human rights. The global COVID-19 pandemic has only highlighted the severity of disconnecting people from the internet when it is used for everything from access to education, work, and banking services, to access to information, culture, and entertainment, as well as basic communication in daily life.\(^9\)

It is our hope this report serves as a warning: ignore internet shutdowns at your peril. They are never a sign of respect for human rights, a healthy democracy, or effective governance.

---

**Number of internet shutdowns by country in 2021**

**India:** 106  
**Myanmar:** 15  
**Iran:** 5  
**Sudan:** 5  
**Cuba:** 4  
**Jordan:** 4  
**Ethiopia:** 3  
**Uganda:** 3  

**Bangladesh:** 2  
**Chad:** 2  
**Eswatini:** 2  
**Indonesia:** 2  
**Iraq:** 2  
**Kazakhstan:** 2  
**Nigeria:** 2  
**Pakistan:** 2  
**Syria:** 2  
**Turkmenistan:** 2  
**Yemen:** 2  

**Afghanistan:** 1  
**Algeria:** 1  
**Burkina Faso:** 1  
**China:** 1  
**The Republic of the Congo:** 1  
**Gabon:** 1  
**Niger:** 1  
**Oman:** 1  
**Palestine:** 1  
**Russia:** 1  
**Senegal:** 1  
**South Sudan:** 1  
**Tajikistan:** 1  
**Uzbekistan:** 1  

**Number of internet shutdowns by region in 2021**

- **Africa:** 19 shutdowns in 12 countries (2021) vs. 19 shutdowns in nine countries (2020)
- **Asia Pacific:** 129 shutdowns in seven countries (2021) vs. 114 shutdowns in five countries (2020)
- **Eastern Europe and Central Asia:** seven shutdowns in five countries (2021) vs. four shutdowns in three countries (2020)
- **Latin America and the Caribbean (LatAm and the Caribbean):** four shutdowns in one country (2021) vs. four shutdowns in three countries (2020)
- **Middle East and North Africa (MENA):** 23 shutdowns in nine countries (2021) vs. 18 shutdowns in nine countries (2020)
THE RETURN OF DIGITAL AUTHORITARIANISM

1.1 Regional and country-specific snapshots of shutdowns

Africa

In 2021, 12 countries cut internet access 19 times in Africa, three more countries than the previous year. What is behind the spread of network disruptions in Africa? The Republic of the Congo, Chad, Niger, Uganda, and Zambia held elections in 2021, and there were protests and significant civil unrest in Eswatini, Ethiopia, Gabon, Senegal, and South Sudan. Elections and protests are common spurs for shutdowns in Africa and around the world, as authorities use them to assert or maintain control of populations, to the detriment of citizens' fundamental rights and democratic freedoms. Despotic and authoritarian regimes also learn from one another, replicating rights-harming tactics for control.

One instance of a shutdown in Africa that departs from this pattern of manipulation for political control is a shutdown Nigeria ordered to deal with what is known locally as banditry, referring to gangs of criminals that carry out kidnapping, cattle rustling, and other crimes. According to a news report, officials temporarily cut off mobile telecommunications services in parts of the states of Zamfara and Kaduna because the gangs were using them to warn one another about the location of government troops.

Asia Pacific

In 2021, we recorded a total of 129 internet shutdowns in seven countries in Asia Pacific, compared to 114 shutdowns across five countries in 2020. India was responsible for at least 106 incidents, making it the country imposing the highest number of shutdowns globally for the fourth consecutive year. Of these, 85 were in Jammu and Kashmir, a region where authorities continue to impose intentional internet disruptions that last for long periods, disrupting and endangering people’s lives for months on end.

Unfortunately, it’s possible that we are also missing some network disruptions that took place due to the lack of government transparency. The Indian government has been reluctant to create and maintain a centralized repository of data on the shutdowns authorities order across the country. This represents a failure to meet the requirements of the 2017 Suspension Rules and the Supreme Court order backing them. The lack of a centralized repository continues to make it difficult for civil society and other actors to effectively monitor and document shutdowns, and some are likely to go unreported.

The shutdowns Indian authorities imposed in 2021 drew international attention and condemnation. The government cut internet access in a clear attempt to suppress the Farmers’ Protests, a movement opposing the Parliament of India’s passage of three farm acts the previous year. Authorities plainly sought to prevent protesters from communicating with one another, and to obstruct press reporting. Despite the disruptions, the government was not able to conceal its violent nature.

Geo-scopes of internet shutdowns in Africa in 2021

Level 1: It only affected one city, county, or village.
Level 2: It affected more than one city in the same state, province, or region.
Level 3: It affected locations in more than one state, province, or region.
Unknown: It is unclear which areas in the country were affected.

Geo-scopes of internet shutdowns in Asia Pacific in 2021

Level 1: It only affected one city, county, or village.
Level 2: It affected more than one city in the same state, province, or region.
Level 3: It affected locations in more than one state, province, or region.
Unknown: It is unclear which areas in the country were affected.


In December 2021, India’s Parliamentary Standing Committee on Communications and Information Technology released a report highlighting the growing trend of internet shutdowns, the impact on rights and freedoms, and the need for recommendations to the government to reform the framework governing suspension of telecom/internet services. While the report makes several positive recommendations aimed at enhancing transparency and accountability, and strengthening safeguards, it does not altogether condemn the use of internet shutdowns, and fails to state one of the most important facts of internet shutdowns: they can never be justified.

INTERNET SHUTDOWNS REPORT 2021


compliance with data protection laws.

A report from the Open Observatory of Network Interference (OONI) shows that access to Facebook, Signal, WhatsApp, Facebook Messenger, and Telegram has been restored, but as of March 2022 people still could not reach Twitter, Vkontakte, TikTok, or Skype without a VPN.

Finally, there is Russia, the only country to block access to communications platforms in Eastern Europe in 2021. The government’s actions show a clear escalation of censorship tactics, from censorship of particular websites or organizations, to takedown orders for major online communications platforms, to the throttling (slowing) of these platforms, to full platform blocks.

In March 2021, Roskomnadzor, the Russian agency responsible for ensuring compliance with media and telecommunication laws, responded to Twitter’s refusal to take down content it flagged by ordering telcos to throttle access to the widely used platform. The decision had unintended consequences, slowing down access to over 40,000 domains containing t.co (Twitter’s shortened domain name). That included the websites of key government institutions in Russia, as well as major platforms Google and Yandex.

Throttling is among many tactics the Russian government has pursued to force foreign tech companies to do its bidding. After Google and Meta refused to take down content the state deemed unlawful, Russian authorities filed lawsuits against them. They also threatened staff at Google and Apple, succeeding in convincing these companies to take down opposition leader Alexey Navalny’s Smart Voting app from their stores and platforms on election day. Authorities also blocked VPNs to stop the Russian people from circumventing this censorship.

It appears the government’s successful efforts to control Russia’s digital spaces only emboldened authorities, encouraging them to go even further. After Russia invaded Ukraine in February 2022, we have seen an even more extreme crackdown on speech as the government seeks to suppress dissent and gain control of the narrative surrounding the conflict. Authorities have passed new laws restricting speech about the war, and banned digital and media platforms, as well as circumvention tools such as VPNs. After Facebook decided to temporarily allow people in Ukraine to call for violence against the Russian heads of state and military invading their country, a Russian court declared parent company Meta “extremist,” effectively banning use of the Facebook and Instagram platforms in Russia.

It’s notable that the Belarus government, which cut access to the internet surrounding disputed elections in 2020 and is now helping Russia wage war in Ukraine, took steps in 2021 to institutionalize its power to hit the “kill switch” and block internet access at its discretion.

Latin America and the Caribbean

According to our documentation, Cuba was the only country in the region to cut internet access in 2021. Authorities responded to growing protests and demands for government reform by shutting down the internet and blocking platforms. In July, as Cubans flooded the streets to demand access to food, water, medicine, and COVID-19 vaccines, the government imposed a complete blanket shutdown. Even after restoring internet access, authorities blocked WhatsApp, Telegram, and Signal. While VPNs were being used by citizens to access blocked services, the state-owned telco ETECSA also blocked the words “VPN” and “libertad” (freedom) from being sent across SMS.

VPN services have been working only intermittently in the island since October 2020. In addition, the Cuban government has reportedly been revoking specific people’s SIM cards. This leaves those affected — mainly activists and journalists — completely disconnected, as ETECSA is Cuba’s only internet provider.

There may also have been shutdowns in Paraguay in 2021, although we do not have enough evidence to include the disruptions in our STOP database. According to research by technology and community organization TEDIC, these reported shutdowns may have been due to militarization of the area, and in the days leading up to a Joint Task Force intervention, all users in one area were left without any service coverage.

---

Geo-scopes of Internet shutdowns in Latin America & the Caribbean in 2021

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cuba</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cuba</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cuba</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Middle East and North Africa

In 2021, we documented at least 23 shutdowns in nine countries in the Middle East and North Africa, five times more than 2020. Sudan and Iran each shut down the internet five times, the highest number of shutdowns in the region. The majority of disruptions in both countries were clearly aimed at silencing dissent.48

Historically, authorities in both countries have imposed shutdowns to quell protests, and to shroud deadly crackdowns and other human rights abuses.49 People in Palestine and Yemen were impacted by shutdowns resulting from attacks on telecommunications infrastructure and disruptions coordinated with escalations in military activity, while the governments of Oman and Jordan took aim at emerging communications platforms that people were using to more freely express themselves. In some cases, authorities ordered deliberate network disruptions in an attempt to stop students from cheating on exams, a harmful and disproportionate practice that according to our records has only expanded across the Middle East and North Africa since 2016. Those maintaining this practice in 2021: Algeria, Iraq, Jordan, Sudan, and Syria.

Geo-scopes of Internet shutdowns in Latin America & the Caribbean in 2021

Level 1: It only affected one city, county, or village.
Level 2: It affected more than one city in the same state, province, or region.
Level 3: It affected locations in more than one state, province, or region.
Unknown: It is unclear which areas in the country were affected.

II. Triggers of internet shutdowns in 2021

As five years of data in our STOP database show, governments around the world turn to internet shutdowns in attempts to assert control over populations. We often see network disruptions during periods of high tension, often as a means of asserting or maintaining power. That included imposing internet blackouts during military coups.

Official justifications vs. actual causes of internet shutdowns worldwide in 2021

The largest portion of claims of “national security” during observed “political instability” came from India’s shutdowns.


On the first day of the year, Indian authorities cut internet access in the district of Jammu and Kashmir, the place that would see more shutdowns than anywhere else on Earth in 2021. Later in the month, India would impose additional shutdowns to quell protests surrounding India’s Republic Day. But on January 1, there were already ongoing shutdowns taking place, not just in India but also in Ethiopia and Myanmar — each of which would see more shutdowns in the following months, in a context of fear, violence, and conflict.

When government authorities plunge citizens into the dark during a crisis, lives are at stake. There is a direct link between internet shutdowns and human rights violations across the globe. Internet shutdowns nurture a culture of impunity for crimes committed against people and keep the rest of the world in the dark with regard to the scale and intensity of the situation. They make it difficult for journalists and human rights defenders to gain access to the affected areas in order to report on happenings and hold governments accountable for atrocities.

As we highlight below, shutdowns are always dangerous and counterproductive, but they are especially so during protests, political turmoil, communal violence, and war. In addition, they can facilitate further aggression.

### The 2021 ranking of the actual causes of internet shutdowns

<table>
<thead>
<tr>
<th>Country</th>
<th>Protests</th>
<th>Communal violence</th>
<th>School exam cheating</th>
<th>Information control</th>
<th>Public holiday</th>
<th>Visits by officials</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>80</td>
<td>9</td>
<td>7</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>The rest of the world</td>
<td>30</td>
<td>11</td>
<td>9</td>
<td>8</td>
<td>7</td>
<td>6</td>
</tr>
</tbody>
</table>

#### 2.1 Internet shutdowns during protests, political turmoil, and coups

Authorities in Bangladesh, Burkina Faso, Chad, Cuba, Ethiopia, India, Indonesia, Iran, Iraq, Jordan, Kazakhstan, Myanmar, Pakistan, Senegal, South Sudan, Sudan, Turkmenistan, and Uganda disrupted or entirely cut connectivity during protests in 2021. As we have noted in previous reports, governments use network disruptions as a tool not only to thwart and disarticulate the protest itself, but also to hide the human rights violations that are commonly linked to security forces’ crackdown on protesters, particularly in countries that have authoritarian regimes or weak democracies.

### The Myanmar coup

On February 1, 2021, as the military seized control of the government, there were multiple reports of internet shutdowns across Myanmar. The shutdowns affected both internet and voice connectivity across several states, and evolved into a curfew-style disruption, with authorities cutting internet access on a daily basis between February 15 and April 28 when internet access was partially restored. Under the cover of the shutdowns, the military escalated violence against people protesting the coup — including using live ammunition, rubber bullets, and tear gas against the protesters. On March 3, during a nationwide blackout, at least 38 protesters were killed in what the U.N. envoy to Myanmar denounced as “the bloodiest day since the coup.”

### The Sudan coup

Sudanese authorities shut down the internet on five different occasions in 2021. On October 25, the military imposed internet shutdowns as they seized power from a transitional government in a military coup. They arbitrarily detained several government officials, including the prime minister. When the people of Sudan took to the streets to protest, the military used violent tactics towend down a peaceful demonstration.

Critical incidents around the world in 2021.


The return of digital authoritarianism

denounce the military’s actions, they were met with additional network disruptions and violence by military forces, which resulted in the killing of seven people and injury of about 140 others.98 Authorities also cut internet access during school examinations.

Like Myanmar, Sudan has a dark history of perpetrating shutdowns that enable human rights violations. After the ousting of Omar Al-Bashir’s administration in April 2019, the military junta committed atrocities against the Sudanese people, including the killing of 100 civilians and injury of many others,99 and the rape of 70 women,100 in the shadow of a complete internet shutdown in June 2019.

Iran’s deadly crackdown on protests

In Iran, authorities responded to protests by cutting mobile internet access from February 24-28 in Sistan and Baluchestan, where over 95.7% of people rely on mobile networks to stay connected.101 They reportedly shut down internet access to hide gross human rights violations and possible international crimes, such as extrajudicial killings. According to media reports, the Islamic Revolutionary Guard Corps, a branch of Iran’s armed forces, opened fire at unarmed civilian fuel vendors, killing 10 individuals, including a child.102

These are not new tactics for Iranian authorities. In 2019, Amnesty International verified the deaths of 304 people killed by the Iranian security services during a week-long internet shutdown aimed at discouraging protests. More than 220 of these deaths took place within 48 hours of the internet shutting down.103

Other countries on the watch

Several other countries that responded to protests by imposing internet shutdowns in 2021 include:

Jordan: In March 2021, protests erupted after seven COVID-19 patients died due to lack of oxygen supply at the Al-Salt hospital. So authorities in Jordan throttled Facebook’s live streaming services to stop people from sharing videos, including those documenting police cracking down on protesters105 — a censorship tactic the government has periodically employed since 2018.

Pakistan: On April 16, after weeks of violent anti-France protests over cartoons published by the French satirical magazine Charlie Hebdo, the Interior Ministry ordered the Pakistan Telecommunication Authority to block Twitter, Facebook, WhatsApp, YouTube, and Telegram.106 In order for the government to further tighten its grip on the country’s digital space, Pakistan’s Information Technology and Telecommunication Ministry introduced a set of draconian regulations107 in October 2021. These regulations enable authorities to control and censor content published on social media platforms as they deem fit, a dangerous precedent restricting people’s enjoyment of fundamental rights.108

Eswatini: Authorities responded to pro-democracy protests by cutting internet access for the first time in 2021, on June 29 and October 15. They cited the need to control “unrest and anarchy.”109

Cuba: As we note above, Cuban authorities responded to protests and widespread calls for government reform in July 2021 by blocking internet access and communications platforms.110 This included rendering mobile networks nearly unworkable.

Burkina Faso: On November 20, 2021, authorities in Burkina Faso shut down mobile internet for at least nine days in response to protests, citing vague “public safety” and “national defense” reasons.111 This was the first time it had cut internet access, according to our STOP database, but by January 23, 2022, the Kabaré government had shut down the internet on three separate occasions.

2.2 Internet shutdowns during elections

Internet shutdowns during an election is a disaster for democracy. Yet over the past five years, government authorities have continued to impose them, before, during, or immediately after an election. In 2021, the #KeepItOn coalition documented seven election-related internet shutdowns in six countries: Chad, the Republic of the Congo, Iran, Niger, Uganda, and Zambia.112 This is lower than our 2020 record with 10 election-related shutdowns in seven countries, our 2019 record with 12 shutdowns in seven countries, and our 2018 record with 12 shutdowns in seven countries. Four of these shutdowns took place in African countries, where election shutdowns remain common despite increasing resistance and legal pushback. Following are details on the disruptions, in chronological order.


democratic discourse. Since then, the Ugandan authorities have refused to unblock Facebook in evident retaliation for the company’s removal of accounts belonging to government officials accused of seeking to manipulate public debate ahead of the January 2021 elections. The disruption was even more extensive and comprehensive than previous shutdowns in 2016, when Ugandan authorities blocked mobile money and social media platforms on two occasions—during the election period and the swearing-in ceremony of President Yoweri Museveni, who has clung to power since 1986. In Niger, the government responded to protests that erupted in the aftermath of the February 21 election by shutting down mobile internet access all across the nation, starting on February 24. Authorities did not restore full access for 10 days, and government officials provided no explanation for the egregious disruption.

The Republic of the Congo followed suit on March 21, as the government implemented a complete internet blackout a few hours before voting commenced. The shutdown cut broadband and mobile internet connections, as well as blocking SMS messaging, and lasted until March 23. Old habits die hard. In 2016, Interior Minister Raymond Mbooulou had ordered telecommunication companies to shut off telephone, internet, and SMS services for 48 hours during presidential elections for “reasons of security and national safety.” On June 20, authorities in Iran only blocked access to social media and mobile phone services, as the government responded to protests that erupted in the aftermath of the February 21 election by shutting down mobile internet access all across the nation, starting on February 24. Authorities did not restore full access for 10 days, and government officials provided no explanation for the egregious disruption.

The Republic of the Congo followed suit on March 21, as the government implemented a complete internet blackout a few hours before voting commenced. The shutdown cut broadband and mobile internet connections, as well as blocking SMS messaging, and lasted until March 23. Old habits die hard. In 2016, Interior Minister Raymond Mbooulou had ordered telecommunication companies to shut off telephone, internet, and SMS services for 48 hours during presidential elections for “reasons of security and national safety.”

On June 20, authorities in Iran responded to clashes between two local tribes following local city council elections by cutting off mobile connections for the entire day in Yasuj, the provincial capital of Kohgiluyeh and Boyer-Ahmad Province. Fortunately, there were no shutdowns during the general elections, which took place a few days earlier, on June 18.

Access Now, our regional partners, and other members of the international #KeepItOn coalition braced for a shutdown in Zambia during the August 12 elections, calling on the government to maintain an open and accessible internet. Despite Zambian authorities issuing a public statement vehemently denying rumors it was planning to hit the kill switch on election day, it did exactly that. Authorities blocked access to social media platforms including WhatsApp, Facebook, Twitter, and Instagram. Chapter One Foundation (Ltd) swiftly filed a lawsuit challenging the disruption, and two days later, the High Court of Zambia ordered the government to restore internet access immediately. While the shutdown should not have been ordered to begin with, as all such shutdowns taint elections, the ruling is an important victory against this kind of rights-harming attack on democracy. In fact, as we cover in section 4.2 below, civil society in a number of African countries fought internet shutdowns in courts of law in 2021, an enormously valuable contribution to the battle against shutdowns globally.

Finally, as we previously noted, the Russian government made a strenuous effort to deny voters access to opposition leader Alexey Navalny’s Smart Voting app, which let voters closely monitor and receive updates on the

---

2.3 Internet shutdowns in active conflict zones

Across the globe, warring parties have intensified attacks on essential civilian services during conflict and war, including attacks specifically targeting telecommunications infrastructure. Internet shutdowns during conflict put lives in danger and deprive people of access to life-saving information, both within and outside conflict zones. External parties are unable to understand what is happening on the ground, hampering international humanitarian efforts and preventing the documentation of war crimes and atrocities perpetrated against civilians. Worse, internet shutdowns carried out through deliberate damage to the internet and telecommunications systems and infrastructure can leave the affected population cut off from the world for months, and keep people struggling with repairs vulnerable to future shutdowns.

In 2021, we saw a continuation of the shutdown in Ethiopia’s Tigray region, which began in November 2020 and continues to this day, in a context of ongoing civil war, crimes against humanity, and ethnic cleansing.44 The shutdown impacted the neighboring Amhara and Afar regions following a spillover of the conflict to those areas. We also documented internet shutdowns in active conflict zones in the Gaza Strip, as the Israeli military engaged in bombing attacks in the ongoing conflict with Palestinians over the occupation of Palestine, and Myanmar, where the military seized and fought to maintain control. In Afghanistan, as the Taliban advanced toward solidifying control over the country following the U.S. military withdrawal, they imposed a communications blackout in Panjshir province, where resistance leaders were based and where people were experiencing dire shortages of food, water, medicine, and other basic supplies.45 Data collected through our STOP project on shutdowns in Azerbaijan, Syria, and Yemen46 over the past five years reveal a pattern: internet infrastructure is becoming a military target during active conflicts.

Ethiopia: internet blackout in Tigray deepens the impact of a brutal civil war

After conflict broke out between the Ethiopian Defense Forces and regional forces in Tigray, we saw a series of internet blackouts impacting people in the region, extending from November 2020 through 2021 to the present day. Internet access has been restored in the neighboring Afar and Amhara regions, which were impacted by the conflict and saw shutdowns in 2021.97

It is hard to overstate the devastating impact of the prolonged conflict and ongoing communications blackouts on Ethiopians in Tigray, where warring parties have leveraged the blackout to perpetrate heinous crimes against humanity.98 "Humanitarian aid workers don’t have access to conflict areas and can’t communicate among themselves to provide essential services such as food, water, clothing, and medication, leaving people vulnerable to sickness and famine."99 The U.N. estimated that about 350,000 people were on the verge of famine between May and June 2021.100 Human rights defenders, journalists, and the international community struggle to report on the ongoing conflict and humanitarian crisis. The information vacuum the internet shutdown created has also allowed the disinformation to thrive, putting people in even greater danger.101

The internet interruption is creating several negative influences on the people of Tigray by limiting the information [about] what is happening around them. Not only this, it also increases the economic crisis that is happening in Tigray.

How the shutdown blocks aid

In 2021, Adele Khod, UNICEF’s representative in Ethiopia, stressed the urgent need for aid supplies to reach parts of Tigray that had not been accessible for months.

“If we do not have telecommunication equipment, we cannot send people into the field and ensure their safety. It’s very simple,” she said.102

We know that we have 33,000 children at high risk of morbidity and mortality, of being very severely sick and eventually dying. We need to reach those children as fast as possible,” she said. “A lack of phone or internet, however, would hamper any aid effort.”

“[We] do not believe that such an attack is either legal or ethical,” she said.103

INTERNET SHUTDOWNS REPORT 2021

In 2021, we documented internet shutdowns in 106 countries affecting 147 million people. We found that 95% of shutdowns are deliberate and 52% are in conflict zones.

The report includes an overview of the shutdown landscape, trends in different regions, and case studies from around the world.

102 See supra note 99.
The weaponization of Facebook

As people in Tigray remained in the dark in late 2021, the conflict intensified, including online, where social media platforms were leveraged to incite ethnic violence and hatred against groups involved in the conflict. Ethiopia’s Prime Minister, Abiy Ahmed, used hate speech on Facebook in an effort to incite violence against the Tigray rebels.103 Ahmed’s message gained traction among government officials, who replicated his language when referring to attacks against Tigrayans.104 These escalations came alongside a troubled history of hate speech online by both high-level figures within the Ethiopian government, armed rebel groups, and their supporters across the diaspora.105

These dangerous and powerful calls for violence on Facebook spurred a public outcry and calls from activists for Facebook parent company Meta to improve its approach to content moderation in contexts of tension and conflict in Ethiopia. Meta’s failure to tamp down on or respond effectively to speech described as genocidal looks even more damning after whistleblower Frances Haugen’s leak of documents showing that Meta knew its platform was being used to incite violence but did very little to stop it.106 In 2021, Meta took belated action to delete some of the violence-inciting content.107 However, it’s clear Meta and other online platforms have yet to deal effectively with the challenge of preventing weaponization of their services.

Israel’s attack on the Gaza Strip

In May 2021, Israeli military forces bombed and destroyed or damaged telecommunications infrastructure, causing full and partial shutdowns in the Gaza Strip. The bombing also led to electricity outages that further compromised connectivity. The bombings struck Al-Jawhara tower on May 12, impacting telecommunications infrastructure housed in the building. On May 15, the strikes toppled the Al-Jalaa tower,108 which houses the offices of some telecommunications providers and media organizations including the Associated Press and Al Jazeera. Fusion, a local telecommunications company, reported disruption of its services due to bombings on May 12, 14, and 18.109 This destruction silenced Palestinian voices. When Palestinians were able to connect, major platforms like Facebook and Instagram removed their posts and suspended their accounts under biased policies and algorithms that effectively, if not intentionally, censored them.110

The Myanmar military’s ongoing digital coup

On February 1, 2021, as the military launched a coup in Myanmar, the junta shut down multiple communications channels for a half day across the nation, in an apparent attempt to control spread of news about the coup and facilitate arrests of key members of the political opposition and civil society.111 This included cutting internet access, mobile phone networks, radio channels, and television channels — except for the military-owned Myawaddy television channel.112 On February 3, the military restored 4G mobile access in some townships of Rakhine state, where the internet had long been suspended to conceal human rights abuses – presumably to distract attention from the coup. The blackouts resumed on February 6 and 7, when the junta cut access to the internet nationwide for the second time, for about 30 hours, blocking citizens’ attempts to access the information about the unfolding events. Military authorities imposed yet another nationwide shutdown on February 15, impacting fiber internet, wireless, and mobile networks. After that, the junta imposed nightly curfew-style shutdowns between 01:00 and 09:00 local time. These nightly disruptions lasted until April 28. In addition, on March 15, the junta shut down mobile internet services, an action that had a deep impact because the majority of internet users in Myanmar rely on their mobile phones for that access. By April 1, the Ministry of Transport and Communications had ordered internet service providers to suspend

INTERNET SHUTDOWNS REPORT 2021

wireless broadband services113 as well, increasing the military’s control of the internet. It would be two and a half months before the junta restored fiber optic and fixed cable connectivity, and even then, it did so by “allow-listing” organizations, corporations, and individuals for whom internet connectivity would remain specifically uninterrupted.114 Allow-listing effectively flips the concept of a free and open internet on its head, making blocking the norm and access the exception, in a discriminatory manner that exacerbates inequality, especially in the context of a coup and humanitarian crisis.

While the military gradually restored internet access across the country in 2021, it is still imposing regional internet shutdowns to this day, particularly in places where the military is meeting resistance.115 These shutdowns are blatant attempts to shroud serious human rights violations, including those potentially amounting to international crimes.116 In addition, the junta has proceeded to ban websites, including widely used social media and messaging platforms, forcing people in Myanmar to use VPNs to gain access. If the junta pushes through a recently resurrected cybersecurity bill, use of VPNs will be criminalized.117

2.4 Internet shutdowns during examinations

Over the past five years we have seen countries around the world shut down the internet to prevent cheating during school examinations, including

---

105 Ibid.
106 Ibid.
112 See supra note 20.
Algeria has been a lead perpetrator of exam-related shutdowns since 2016, and 2021 was no exception to the rule. In June, Algerian authorities shut down the internet between 8:00 and 12:00 local time as 731,000 students were sitting their first national exam. These disruptions continued throughout the day, alternating between complete blackouts during exam sessions, and heavy throttling — slowing down — of services in between sessions, during lunch breaks, and overnight. Millions of people in Algeria have suffered as a result, especially those whose work and livelihoods rely on social media and the internet. In 2020 alone, Algeria lost around 388 million USD due to exam-related internet shutdowns, and Algerian experts estimate economic losses at 500 million Algerian Dinars for every hour of internet shutdown in the country. The shutdowns continue despite Algerian President Abdelmadjid Tebboune’s public statement on TV that he will “no longer tolerate” this practice.

Syria continues its tradition of shutting down the internet during national exams in 2021, a practice that has been as regular as clockwork since 2016. In 2020, Sudan disrupted internet services for three hours while scheduled national exams were taking place. In 2021, Sudan’s public prosecutor once again ordered internet service providers to shut down mobile internet connections for these exams.

Governments that impose these disruptions have justified their use as a preemptive measure to prevent students from cheating or leaking exam questions. However, even if the practice did stop cheating, shutdowns are not a proportionate measure to meet that aim. Preventing cheating should not require undermining human rights.

III. Notable trends and developments in 2021

3.1 Prolonged shutdowns

Four longest internet shutdowns recorded in 2021

<table>
<thead>
<tr>
<th>Shutdown Duration</th>
<th>Country</th>
<th>Description</th>
</tr>
</thead>
</table>
| 626 days          | Bangladesh | Recent international exams in Bangladesh were
|                   |          | accompanied by internet access restrictions.
| 527 days          | Sudan     | Sudanesehome.net (2021). Directive from the
|                   |          | Attorney General to stop internet service starting
|                   |          | tomorrow. Retrieved February 23, 2022, from
|                   |          | https://sudanesehome.net/ |
| 501 days          | Jammu and Kashmir | The shutdown started June 11, 2021, and
|                   |          | continued for 501 days. The state of Jammu and
|                   |          | Kashmir region has been subjected to internet
|                   |          | disruptions intermittently since the military coup
|                   |          | in February 2020. The shutdown is
|                   |          | estimated to have affected more than
|                   |          | 500,000 people. Retrieved February 23, 2022, from
|                   |          | https://sudanesehome.net/ |
| 500 days          | Tigray, Ethiopia | At the halfway mark in 2021, we had already
|                   |          | documented the continuation of a deeply damaging
|                   |          | trend: some governments are prolonging their
|                   |          | interference, further exacerbating the devastating
|                   |          | harm they have on people’s lives. In Pakistan’s
|                   |          | Federally Administered Tribal Areas (FATA), the
|                   |          | Pakistan Telecommunication Authority restricted
|                   |          | full mobile networks following the conflict at its
|                   |          | border with Afghanistan in June 2016. The internet
didn’t get fully restored until December 2021, setting the
|                   |          | economic and educational development decades back for
|                   |          | the people living in the already isolated area. In India’s
|                   |          | Jammu and Kashmir region, people have suffered through
|                   |          | the longest shutdown on record, according to our
|                   |          | documentation. But authorities did not stop there.
|                   |          | They continued to impose shutdowns intermittently,
|                   |          | with 85 documented disruptions in total in 2021 —
|                   |          | leaving the population in a near-constant state of
|                   |          | compromised connectivity. Likewise, in Ethiopia, the
|                   |          | Tigray region has been cut off since November
|                   |          | 2020: that’s 18 months and counting. In Myanmar,
|                   |          | people in townships across Rakhine state — largely
|                   |          | populated by marginalized ethnic groups — have
|                   |          | experienced years-long shutdowns since 2019, as
|                   |          | we reported in our 2020 report. Just as the internet
|                   |          | was restored for local people, the whole country went
|                   |          | offline due to the military coup.
|                   |          | 

3.2 Increased use of mobile shutdowns during protests

In 2021, 18 governments, including Bangladesh, Burkina Faso, Chad, Cuba, Eswatini, India, Indonesia, Iran, Iraq, Jordan, Kazakhstan, Myanmar, Pakistan, Senegal, South Sudan, Sudan, Turkmenistan, and Uganda, imposed mobile internet shutdowns during protests. Cutting mobile access to crack down on protests is an increasing trend globally, and at least 37 shutdowns in 2021 affected mobile internet services during protests, compared to 15 instances in the previous year. With more and more people turning to their mobile phones to access the internet and digital communication services-and-blocks-social-media-platforms/ |


platforms globally, and particularly in developing and emerging countries.133 State actors have identified mobile internet shutdowns as an effective way to silence people without necessarily having to take the entire country off the grid. This tactic is especially discriminatory and harmful. While people who can afford or access more expensive options to get on the internet, such as fixed cable services, can remain connected, people and communities without such privilege are excluded and disconnected. It widens the digital divide between the privileged, such as government officials, banking companies, and elites, and everyone else. Authorities may also target mobile services in an attempt to silence their critics, who might otherwise find and share information privately, and connect with one another to organize, using certain mobile platforms or applications, such as social media apps, secure messaging apps, or VPNs.

3.3 Targeted blocking of communications platforms

Authorities are increasingly responding to public criticism and dissent by blocking specific communications platforms. Some governments went even further, cutting access to VPNs that enable people to bypass the censorship.134 Our data indicates that service-based disruptions happened in 22 countries throughout 2021. This includes Bangladesh, China, Cuba, Eswatini, Ethiopia, India, Iran, Jordan, Kazakhstan, Myanmar, Nigeria, Oman, Pakistan, Russia, Senegal, South Sudan, Sudan, Tajikistan, Turkmenistan, Uganda, Uzbekistan, and Zambia.

In Myanmar, for example, the military pushed internet providers to block Twitter as part of its ongoing digital coup. The block was executed in such a manner that it resulted in what’s called “domain poisoning,” meaning that it impacted unrelated sites and services as far away as Western India.135

Russia throttled Twitter as part of its ever-ratcheting restrictions of free expression, after the platform failed to remove content authorities flagged as illegal. As we note above, this throttling ended up slowing down access to more than 40,000 domains containing t.co (Twitter’s shortened domain name). That included the websites of government agencies in Russia, and platforms like Google and Yandex.136

In Pakistan, authorities cut access to several major social media platforms, including Facebook, Twitter, and TikTok, ahead of planned anti-government protests.137

When people in Iran migrated from WhatsApp to the secure messaging app Signal for better privacy and freedom from surveillance, authorities blocked it. Authorities also ordered its removal from Cafe Bazaar, Iran’s version of Google Play, and Myket, another local app store.138 Signal is only one of the most recent platforms Iran has blocked. The government already blocks Facebook, Twitter, YouTube, and Telegram, and had previously blocked Signal intermittently in 2016 and 2017.

Similarly, in China, Signal became part of the long list of digital platforms blocked indefinitely by authorities in March 2021 after seeing an increase in the number of app downloads.139

Another target for blocking was Clubhouse, a social media audio chat application people use for online debates. In March 2021, authorities in Jordan blocked the app,140 and journalists, activists, and others fled to alternative platforms to condemn the blocking as a flagrant abuse of freedom of expression and access to information rights. Jordanian journalist Basil Alrafaih spoke out on Facebook, arguing, “An authority that is afraid to speak, and oppresses its people on the ground and in space, cannot confront a pandemic.”141 In Oman, the Internal Security Service ordered the Telecommunications Regulatory Authority to block

---

INTERNET SHUTDOWNS REPORT 2021

IV. Fighting back in 2021: challenges and opportunities

Internet shutdowns happen because governments want to control the flow of information online, regardless of the consequences for their own people, economies, and reputation around the world. That desire for control has translated to increased use of network disruptions, even as we see momentum grow in the global fight to stop shutdowns. Following is an overview of some of the progress we saw in 2021 despite the increase and spread of disruptions.

4.1 Progress at the international level

G7 declarations condemn internet shutdowns: In May 2021, participants at the G7 Foreign and Development Ministers’ Meeting issued a communiqué to condemn “actions by states to intentionally disrupt their own populations’ access to, or dissemination of, information, knowledge, and data online.” Heads of state echoed this sentiment in their own Carbis Bay G7 Summit Communique, stating, “We also affirm our opposition to measures which may undermine these democratic values, such as government-imposed internet shutdowns and network restrictions.” Notably, this communiqué adopted the definition of an internet shutdown Access Now and many members of the #KeepItOn coalition use, reflecting familiarity with our campaign and goals, and our presence in events leading to the 2021 G7 Summit.

A U.N. resolution condemns internet shutdowns and calls for a report on disruptions: When the U.N. Human Rights Council adopted a new version of the resolution on “the promotion, protection and enjoyment of human rights on the Internet” (A/HRC/47/16) in July 2021, it specifically called for shutdowns and mandated a report on “the trend in internet shutdowns, analyzing their causes, their legal implications and their impact on a range of human rights, including economic, social and cultural rights.” Access Now and our partners lobbied for this resolution and contributed evidence and analysis for the report.

A global multistakeholder forum sets up a global internet shutdown taskforce: In December 2021, the U.N. expert on the rights to peaceful assembly and association outlines pathway for ending internet shutdowns: Special Rapporteur Clément Voule submitted Ending Internet shutdowns: a path forward to the 47th Session of the Human Rights Council in June 2021, as a follow up to a 2019 report on the rights to freedom of peaceful assembly and of association in the digital age. The Special Rapporteur cites Access Now and the #KeepItOn coalition’s work, unpacking the “magnitude and severity of internet shutdowns as a means to suppress the right to peaceful assembly.” He also offers a series of recommendations for state actors, companies, investors, and international organizations to reverse this deadly trend.

INTERNET SHUTDOWNS REPORT 2021

IV. Fighting back in 2021: challenges and opportunities

Internet shutdowns happen because governments want to control the flow of information online, regardless of the consequences for their own people, economies, and reputation around the world. That desire for control has translated to increased use of network disruptions, even as we see momentum grow in the global fight to stop shutdowns. Following is an overview of some of the progress we saw in 2021 despite the increase and spread of disruptions.

4.1 Progress at the international level

G7 declarations condemn internet shutdowns: In May 2021, participants at the G7 Foreign and Development Ministers’ Meeting issued a communiqué to condemn “actions by states to intentionally disrupt their own populations’ access to, or dissemination of, information, knowledge, and data online.” Heads of state echoed this sentiment in their own Carbis Bay G7 Summit Communique, stating, “We also affirm our opposition to measures which may undermine these democratic values, such as government-imposed internet shutdowns and network restrictions.” Notably, this communiqué adopted the definition of an internet shutdown Access Now and many members of the #KeepItOn coalition use, reflecting familiarity with our campaign and goals, and our presence in events leading to the 2021 G7 Summit.

A U.N. resolution condemns internet shutdowns and calls for a report on disruptions: When the U.N. Human Rights Council adopted a new version of the resolution on “the promotion, protection and enjoyment of human rights on the Internet” (A/HRC/47/16) in July 2021, it specifically called for shutdowns and mandated a report on “the trend in internet shutdowns, analyzing their causes, their legal implications and their impact on a range of human rights, including economic, social and cultural rights.” Access Now and our partners lobbied for this resolution and contributed evidence and analysis for the report.

A global multistakeholder forum sets up a global internet shutdown taskforce: In December 2021, the U.N. expert on the rights to peaceful assembly and association outlines pathway for ending internet shutdowns: Special Rapporteur Clément Voule submitted Ending Internet shutdowns: a path forward to the 47th Session of the Human Rights Council in June 2021, as a follow up to a 2019 report on the rights to freedom of peaceful assembly and of association in the digital age. The Special Rapporteur cites Access Now and the #KeepItOn coalition’s work, unpacking the “magnitude and severity of internet shutdowns as a means to suppress the right to peaceful assembly.” He also offers a series of recommendations for state actors, companies, investors, and international organizations to reverse this deadly trend.
INTERNET SHUTDOWNS REPORT 2021

use of internet shutdowns since 2019 by holding regulators, the government, and internet providers accountable. As a result, we have seen four court decisions against shutdowns in Sudan.165

Zambia: After Chapter One Foundation filed a lawsuit challenging the election-day blocking of social media platforms, the Zambia High Court issued a landmark decision ordering authorities to restore full access immediately.166 In a court settlement and consent judgment on March 21, 2022, the Zambia Information and Communication Authority (ZICTA) agreed not to act outside of its legal authority and ordered to interrupt the flow or access to the internet going forward. ZICTA also agreed to provide notice to the public within 36 hours of any internet shutdowns.167

These court cases are effective: the Zambia and Sudan lawsuits brought an end to the shutdowns in those countries when authorities would not stop despite public outcry. We and our partners eagerly await a judgment in the Nigeria case.

4.3 Progress on equipping civil society to circumvent and resist shutdowns

Access Now and other members of the #KeepitOn coalition created a number of important resources in 2021, all designed to help people anticipate, navigate, and document the internet shutdowns that undermine our democracies and damage human rights.

The 2021 Election Watch: At Access Now, we launched an initiative to flag upcoming elections potentially ripe for shutdowns, provide real-time updates on disruptions, and encourage action to help #KeepitOn.168 Preventing election shutdowns is a global imperative, as they stop people from staying informed, auditing their own elections, and ensuring the integrity of democratic processes. People must have the power to document irregularities and share the evidence with the rest of the world.

#KeepitOn Internet Shutdowns and Elections Handbook: In addition, we launched a handbook aimed at election observers, embassies, activists, and journalists.169 It explains why internet shutdowns are a barrier to democratic elections, and offers recommendations for navigating a shutdown, including information on how to recognize the early warning signs, how to prepare for and circumvent a disruption, and how to monitor and document any shutdown that takes place.

Eyes on Internet Shutdowns: Documenting for Human Rights: This global campaign by WITNESS helps activists, human rights defenders, citizen eye witnesses, journalists, and documentarians prepare in advance to document human rights violations during internet shutdowns.170

Prepare, Prevent, Resist: Shutdowns Advocacy Workflow: Created by Internews in collaboration with the #KeepitOn community and researchers across the globe, this microsite is an extraordinary repository of resources on how to effectively advocate against internet shutdowns.171

INTERNET SHUTDOWNS REPORT 2021

at the Freedom Online Coalition (FOC) conference, Access Now, the U.S. State Department, and the Global Network Initiative launched the new FOC Task Force on Internet Shutdowns.154 At the launch, the groups underscored the FOC’s responsibility to advance internet freedom and emphasized the importance of “sharing and developing resources, issuing targeted statements, and creating and leveraging trusted channels of communication among all stakeholders to facilitate collaboration.”155

4.2 Progress in challenging internet shutdowns in court

With the challenge of growing shutdowns in Africa in 2021 came the opportunity to fight the disruptions in court, establish legal precedents, and build the case law against them — a gift to civil society activists, human right defenders, and other stakeholders around the world.

We saw important legal challenges in Nigeria, Sudan, and Zambia.

Nigeria: After Twitter took down a tweet by Nigerian President Muhammadu Buhari, the government blocked the platform.156 Civil society organizations including SERAP (Socio-Economic Rights and Accountability Project) filed lawsuits before the ECOWAS Court of Justice. International organizations Access Now, the Electronic Frontier Foundation, and Open Net Association supported the SERAP suit157 through a joint amicus brief.158 The government tried and failed to have the case dismissed, and the plaintiffs are still awaiting judgment. Notably, the ECOWAS Court of Justice previously issued a ruling against a shutdown in Togo in 2020 confirming the fundamental rights of the people impacted.

Sudan: When Sudanese authorities cut internet access in October 2021, the Sudanese Consumer Protection Organization sued the Telecommunication and Post Regulatory Authority (TPRA).159 After a judge ordered access restored on November 11, 2021,160 the TPRA argued against restoration on the grounds of “national security” and a “state of emergency.”161 arguments the court dismissed. When telecommunications companies in Sudan still failed to restore access, the judge took the unprecedented step of issuing an arrest warrant for the chief executive officers.162 That is when access was finally restored.163 It is notable and highly commendable that Sudanese civil society has responded to the up tick in the

168 See supra note 10.
169 See supra note 92.
THE RETURN OF DIGITAL AUTHORITARIANISM

These are just a few of the resources developed in 2021 that demonstrate the growing sophistication and strength of civil society resistance to shutdowns around the world.

4.4 Progress on collaborative monitoring and analysis of shutdowns

Fighting internet shutdowns requires collective efforts from diverse actors globally. Monitoring and documenting shutdowns remains crucial for alerting the public and holding perpetrators accountable. With governments becoming more sophisticated in imposing shutdowns, making it more difficult to detect certain outages, we are excited about the growth of the #KeepItOn measurement community in 2021. Companies and organizations like Cloudflare, Censored Planet, Mozilla, and RIPE Atlas have committed to providing us with technical insight and data on shutdowns as they occur. Google’s Jigsaw is closely monitoring shutdowns and has published a comprehensive analysis highlighting the impact of these disruptions on fundamental rights worldwide.

These initiatives are in addition to the important ongoing work of the Open Observatory of Network Interference (OONI), Internet Outage Detection Analysis (IODA), Measurement Lab (M-Lab), and Internet Society Pulse among others. The diversity of the monitoring community makes tracking more robust, preventing perpetrators from hiding their tracks.

As we consider 2021 in the context of data from the past five years, we see a year that reflects the continued challenge of preventing government authorities, those engaged in armed conflict, and military juntas from leveraging internet shutdowns as tools for control. As societies around the world struggle to stay safe and healthy during the COVID-19 pandemic, it’s clear the consequences of disruptions are dire — regardless of the context or rationale. Looking forward, we draw inspiration from the progress the global #KeepItOn coalition has been making despite the global increase in disruptions, from the promising dip in election shutdowns globally, to the court challenges in Africa, to the growth in resources and capacity to monitor, circumvent, and document disruptions. We hope to make more progress in the years ahead, building pressure to prevent the network disruptions that are causing so much harm. We urge you to join the fight.

V. Conclusion: our movement needs to keep growing

As we consider 2021 in the context of data from the past five years, we see a year that reflects the continued challenge of preventing government authorities, those engaged in armed conflict, and military juntas from leveraging internet shutdowns as tools for control. As societies around the world struggle to stay safe and healthy during the COVID-19 pandemic, it’s clear the consequences of disruptions are dire — regardless of the context or rationale. Looking forward, we draw inspiration from the progress the global #KeepItOn coalition has been making despite the global increase in disruptions, from the promising dip in election shutdowns globally, to the court challenges in Africa, to the growth in resources and capacity to monitor, circumvent, and document disruptions. We hope to make more progress in the years ahead, building pressure to prevent the network disruptions that are causing so much harm. We urge you to join the fight.

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
THE RETURN OF DIGITAL AUTHORITARIANISM
Internet shutdowns in 2021

#KeepItOn