I. Internet shutdowns in 2022: a global overview

Overview of 2022 data

Documented internet shutdowns by year *

- **Total number of shutdowns**
- **Total number of shutdowns, not including India**

<table>
<thead>
<tr>
<th>Year</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of shutdowns</td>
<td>75</td>
<td>106</td>
<td>196</td>
<td>213</td>
<td>159</td>
<td>184</td>
<td>187</td>
</tr>
<tr>
<td>Total number of shutdowns, not including India</td>
<td>45</td>
<td>37</td>
<td>62</td>
<td>92</td>
<td>50</td>
<td>77</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>2016</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
<th>2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td>33</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>29</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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

** Shutdowns were imposed by external forces during armed conflict in Ukraine and Yemen.
### Shutdown triggers in 2022

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protests</td>
<td>62 shutdowns in 16 countries during protests</td>
<td>Bangladesh, Ethiopia, Iran, Jordan, Kazakhstan, Myanmar, Russia, Sierra Leone, Somaliland, Sudan, Tajikistan, Uzbekistan, and active conflict zones in Ukraine and Yemen</td>
</tr>
<tr>
<td>Active conflicts</td>
<td>33 shutdowns during active conflicts</td>
<td></td>
</tr>
<tr>
<td>Exams</td>
<td>8 shutdowns in 6 countries “to prevent exam cheating”</td>
<td></td>
</tr>
<tr>
<td>Elections</td>
<td>5 shutdowns in 5 countries tied to elections</td>
<td></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:**

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

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

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
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></th>
<th>Mobile</th>
<th>Broadband</th>
<th>Unknown</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021</td>
<td>129</td>
<td>102</td>
<td>7</td>
</tr>
<tr>
<td>2022</td>
<td>102</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

Despite the apparent reduction in total shutdowns in the region from 2021 to 2022, these shifts are largely reflective of increasingly entrenched shutdowns, as well as erratic and hyperlocal disruptions, severe obstacles to documenting recurring disruptions in communities under attack, and the introduction of alternative censorship strategies layered on top of shutdowns. The Asia Pacific region remains a global leader in internet shutdowns, reflected in the case studies of India and Myanmar, where people continue to experience staggering levels of targeted disruptions. Nevertheless, people in India’s Jammu and Kashmir and Myanmar’s Sagaing and Magway regions and Chin state lived through much of 2022 with near-continuous disruptions and poor quality of service in the rare intervening moments of connectivity.

// Myanmar

In Myanmar, the military crackdown on those resisting the regime after the coup d’etat 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,}

INTERNET SHUTDOWNS IN 2022

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 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 months, and approximately 50 townships had been cut off for more than one year. Of these, more than 20 townships faced shutdowns for the entirety of 2022 and for more than 500 days, and at least 25 townships faced shutdowns for 10 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 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 of killings, torture, ill-treatment, and arrests, as well as widespread arson of property. Even when there are no military attacks, people in these villages have suffered from ongoing connectivity challenges, as significant price hikes for internet access and expanded regulations for IMEI and SIM card registration 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 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

---

Myanmar Posts and Telecommunications (MPT) and 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.

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 learn 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. 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.

<table>
<thead>
<tr>
<th>Year</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>

Shutdows during protest and unrest

Elsewhere in the Asia Pacific region, Pakistan and Bangladesh ordered shutdowns during protests, and China, Afghanistan, and Sri Lanka 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. 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.

18 Ibid.
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 Fatafa, Raman Jit Singh Chima, Wai Phyo Myint, Golda Benjamin, Anastasiya Zhyrmont, 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

#KeepItOn