SHRINKING DEMOCRACY, GROWING VIOLENCE

Internet shutdowns in 2023
Overview of 2023 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>78</td>
<td>48</td>
</tr>
<tr>
<td>2017</td>
<td>111</td>
<td>42</td>
</tr>
<tr>
<td>2018</td>
<td>202</td>
<td>68</td>
</tr>
<tr>
<td>2019</td>
<td>221</td>
<td>100</td>
</tr>
<tr>
<td>2020</td>
<td>168</td>
<td>58</td>
</tr>
<tr>
<td>2021</td>
<td>194</td>
<td>86</td>
</tr>
<tr>
<td>2022</td>
<td>201</td>
<td>116</td>
</tr>
<tr>
<td>2023</td>
<td>283</td>
<td>167</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>Shutdowns</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>27</td>
</tr>
<tr>
<td>2017</td>
<td>23</td>
</tr>
<tr>
<td>2018</td>
<td>28</td>
</tr>
<tr>
<td>2019</td>
<td>36</td>
</tr>
<tr>
<td>2020</td>
<td>34</td>
</tr>
<tr>
<td>2021</td>
<td>39</td>
</tr>
<tr>
<td>2022</td>
<td>40</td>
</tr>
<tr>
<td>2023</td>
<td>39</td>
</tr>
</tbody>
</table>

India: 116
Myanmar: 37
Iran: 34
Palestine: 16 **
Ukraine: 8 **
Pakistan: 7
Iraq: 6
Azerbaijan: 5
Ethiopia: 4
Senegal: 4

Bangladesh: 3
Russia: 3
Jordan: 3
Libya: 3
China: 2
Guinea: 2
Mauritania: 2
Oman: 2
Tanzania: 2
Turkmenistan: 2
Sudan: 2
Syria: 2
Türkiye: 2
Algeria: 1
Brazil: 1
Cuba: 1
Gabon: 1
Indonesia: 1
Kenya: 1
Lebanon: 1
Mozambique: 1
Nepal: 1
Qatar: 1
Saudi Arabia: 1
Somaliland: 1
Suriname: 1
United Arab Emirates: 1
Uganda: 1
Venezuela: 1

** Shutdowns were imposed by external parties in Palestine and Ukraine.
Shutdown triggers in 2023

<table>
<thead>
<tr>
<th>Conflicts</th>
<th>Protests</th>
<th>Exams</th>
<th>Elections</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>74</strong> shutdowns in <strong>9</strong> countries during conflicts</td>
<td><strong>63</strong> shutdowns in <strong>15</strong> countries during protests</td>
<td><strong>12</strong> shutdowns in <strong>6</strong> countries “to prevent exam cheating”</td>
<td><strong>5</strong> shutdowns in <strong>5</strong> countries tied to elections</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>Conflicts</th>
<th>Protests</th>
<th>Exams</th>
<th>Elections</th>
</tr>
</thead>
<tbody>
<tr>
<td>2023</td>
<td>74</td>
<td>63</td>
<td>12</td>
<td>5</td>
</tr>
<tr>
<td>2022</td>
<td>36</td>
<td>63</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>2021</td>
<td>19</td>
<td>39</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>2020</td>
<td>15</td>
<td>16</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>2019</td>
<td>52</td>
<td>65</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>2018</td>
<td>2</td>
<td>45</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>2017</td>
<td>3</td>
<td>37</td>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>2016</td>
<td>3</td>
<td>27</td>
<td>6</td>
<td>5</td>
</tr>
</tbody>
</table>

Emerging trigger in 2023:

- **4** shutdowns in **4** countries during natural disasters

Shutdown trends in 2023

1. **Shutdowns continue to shroud grave human rights abuses and violence**
   - **51** shutdowns in **11** countries coinciding with documented grave human rights abuses ***
   - **Azerbaijan, Ethiopia, Iran, Jordan, Mauritania, Myanmar, Palestine, Russia, Somaliland, Sudan, Ukraine**

*** Grave 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. **Authorities must refrain from normalizing platform blocks**
   - **53** blocks across **25** countries in 2023, up from **39** blocks across **29** countries in 2022
   - **Grindr is the second-most blocked messaging platform outside of India after Facebook, impacting people in 12 countries and targeting LGBTQ+ spaces**
   - **China, Indonesia, Iran, Jordan, Lebanon, Oman, Pakistan, Qatar, Saudi Arabia, Tanzania, Türkiye, United Arab Emirates**
3. **Worst offenders are entrenched and emboldened in the use of shutdowns**

- **1,153 days** since Nov. 4, 2020
  - Tigray, Ethiopia
- **864 days** since Aug. 2021
  - Dozens of townships across Myanmar
- **694 days** since Feb. 2022
  - Panjgar, Pakistan
- **35 shutdowns** persisted from 2023 into 2024
  - People in 17 countries were subjected to a shutdown for the entire year in 2023

****Number of days as of Dec. 31, 2023

4. **The geographic scope of shutdowns is broadening**

In 2023, only **30.4%** of all shutdowns were on the smallest scale (only affecting one city, county, or village), whereas **46.8%** of all shutdowns were on this scale in 2022.

**80** shutdowns impacted multiple regions or entire countries, the highest number of such shutdowns recorded since 2016.

---

**Since 2016**

- **1,458** shutdowns around the world
- **82** countries affected

**New offenders in 2023**

- **Kenya *******
- **Mozambique**
- **Nepal**
- **Suriname**

**** First shutdown imposed by the government of Kenya; previous shutdowns in 2020 were imposed by a third party

- **Lebanon**
- **Qatar**
- **United Arab Emirates**

Countries with multi-year platform blocks in place appearing in the STOP database for the first time
Asia Pacific (APAC)
Regional overview in 2023

<table>
<thead>
<tr>
<th>Country</th>
<th>Shutdowns</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>India</td>
<td>116</td>
<td>7</td>
</tr>
<tr>
<td>Myanmar</td>
<td>37</td>
<td>8</td>
</tr>
<tr>
<td>Pakistan</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Indonesia</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Nepal</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

India: 116
Myanmar: 37
Pakistan: 7 Bangladesh: 3 China: 2 Indonesia: 1 Nepal: 1

Nepal joined the offender list for the first time in 2023

6 of these 7 countries are among the most entrenched repeat offenders

76.6%

128 out of 167 shutdowns in the region occurred alongside reported violence
India: 97  Myanmar: 27  Pakistan: 4

Authorities in the Asia Pacific region deepened their suppression of digital rights in 2023, including through the heavy use of internet shutdowns. For the sixth year in a row, India leads the way in the total number of recorded government shutdown orders with **116**. However, the **37** shutdowns we were able to record in Myanmar are only a fraction of what were likely hundreds ordered by the junta, as the continued rise of violence makes documenting disruptions extremely difficult. Pakistan and Bangladesh continued to impose shutdowns, particularly during protests.\(^1\) Indonesia continued to block Grindr;\(^2\) and Nepal joined the shame list in 2023 with its blocking of TikTok.\(^3\) Against a backdrop of extensive censorship under the Great Firewall, China maintained ongoing blocks of Signal and Grindr.\(^4\)

**Myanmar**

Since February 1, 2021, when Myanmar’s junta seized

---


power in a deadly coup, the people of Myanmar have endured unrelenting attacks, both physical and digital. The military has complete control of the country’s telecommunications network and has systematically used internet shutdowns all across the country to facilitate war crimes and crimes against humanity. With the support of #KeepItOn coalition partners, we identified at least 37 shutdowns in Myanmar in 2023. However, this number only represents events that could be independently verified through news reports, information from partners, and confidential sources in Myanmar. This verification process has become increasingly challenging. The limited information authorities made available in previous years has become even more scarce as decision-making around shutdown implementation becomes more decentralized; continued escalations in violence, displacement, and crackdown on digital rights activists make the work of documentation dangerous and difficult; and the continued degradation of infrastructure has made it even more challenging to parse the specific cause of certain outages. Despite these constraints, the data available illustrates unrelenting, targeted disruptions during active conflict across the country in 2023, with only one of the 14 states or regions around the country, Ayeyarwaddy, not impacted by a shutdown.

Before 2023, internet shutdown orders came from the central government in Naypyitaw and often impacted many townships at once. However, the junta has since decentralized decision-making around when and where shutdowns are deployed, allowing local officials to more specifically target shutdowns in real time to align with military operations and troop movements, more effectively keeping communities in the dark. Out of the 37 shutdowns documented in 2023, 31 shutdowns began in 2023, with 20 ordered by local authorities and affecting a single township or village and 11 impacting multiple townships or entire states. The remaining six shutdowns were still ongoing after orders from central authorities in 2021 and 2022. These localized shutdowns were more erratic, with authorities reportedly cutting off access when the military moved into villages seemingly chosen at random and burning them down. They were also more difficult to document, both because less data is available to measure and verify hyperlocal shutdowns and because decentralized decision-making means more actors with less visibility.

Additionally, reports of leaked documents show that the use of signal jammers is now a central part of the junta’s military strategy. Community reports have documented the repeated use of scouting aircraft equipped with jamming devices ahead of military operations, and although we can’t distinguish which shutdowns were caused by these devices, many of the shutdowns we recorded took place during air strikes targeting residential areas and appear consistent with this type of jamming. At least 11 shutdowns in Myanmar in 2023 were tied to documented grave human rights abuses or war crimes, many of which include bombardments and airstrikes targeting civilians in residential areas.

In places like Rakhine State where the military has imposed strict blockades, fuel provisions for generators running telecommunications services were cut off, leaving people with little or no access to information while food, water, and other essentials were already in short supply, and with no access to mobile cash transfer apps needed to purchase what limited supplies were left. In many of Myanmar’s conflict zones where shutdowns are ongoing as a result of infrastructure damage, restrictions on movement mean telecommunications providers are unable to dispatch employees to make repairs. Other restrictions included reported throttling, website blocking, and virtual private network (VPN) bans, all of which continue to make the internet in Myanmar limited, unreliable, and increasingly censored on

---


10 Ibid.
INTERNET SHUTDOWNS IN 2023

When considered alongside actions of the State Administration Council (SAC) to imprison those who criticize the junta or show support for the resistance online, to implement biometric surveillance, and to target journalists by revoking media licenses, it is clear freedom of expression is severely restricted in all forms in Myanmar.11

In January 2024, residents in Rakhine State were suffering not only an ongoing military blockade and travel ban, but also an ongoing internet shutdown impacting 17 townships.12 The disruption has had a significant impact on the flow of information, safety, and humanitarian support, without independent media on the ground to verify events or combat disinformation during the escalating conflict. At the time of writing, there were 80 townships nationwide facing ongoing shutdowns, highlighting the continuing and dire situation for connectivity in Myanmar.13

We and our partners urge the international community to establish and commit resources for a coordinated action plan to provide the people of Myanmar with alternative access to the internet and other communication channels, which are critical for protecting lives and fundamental human rights. Companies must be held accountable for their failure to create protection mechanisms for their users or provide transparency about how their networks and services are abused by the military.14

India

India was responsible for 116 shutdowns in 2023, the highest number of shutdown orders worldwide for the sixth consecutive year. Authorities in India continue to use shutdowns as a near-default response to crises, both proactively and reactively.

Authorities in India increasingly implemented shutdowns at a regional rather than local level, compared with 2021 and 2022 when shutdowns were highly localized, especially in Jammu and Kashmir. In 2023, 64 shutdown orders affected more than one district in the same state, province, or region, driven by 47 shutdowns in Manipur but also including the statewide shutdown in Punjab in March.

From May 3 to December 3, 2023, the government of Manipur imposed a statewide shutdown affecting roughly 3.2 million people for 212 days (including a break of only three days) through a series of 44 published shutdown orders.15 It changed in scope and scale throughout the year, primarily impacting mobile networks but also including a statewide shutdown of broadband and mobile internet lasting two-and-a-half months. The impacts were severe, particularly for women, as the shutdowns made it more difficult to document rampant atrocities, including murder, rape, arson, and other gender-based violence, and thereby hold perpetrators accountable.16


In the state of Punjab, authorities blocked internet access impacting about 27 million people across the state for four continuous days — one of the country’s most extensive blackouts in recent years — as police searched for an alleged separatist on the run.¹⁸

In addition to ongoing nationwide platform blocks, in 2023, people in 13 states experienced local or statewide internet shutdowns, the same total from 2022. Among them, more authorities are repeatedly reaching for the kill switch, with the number of states employing five or more shutdowns in a year increasing from two in 2021 and three in 2022 to seven in 2023. In addition to Manipur and Punjab, authorities in Bihar (12), Haryana (11), West Bengal (6), Maharashtra (5), and Rajasthan (5) imposed shutdowns during protests, religious holidays, and exams. Jammu and Kashmir saw 17 shutdown orders, down from 49 in 2022.

Not only were shutdowns implemented at wider geographic scales, they lasted longer in 2023. The share of shutdowns in India spanning across five days or more shot up from 15% of shutdowns in 2022 to more than 41% in 2023. When combined with nationwide blocking of 14 messaging apps starting in early May, 7,502 URL-blocking orders issued between January and October 2023, and India’s new telecom law giving the central government nearly unchecked power to impose internet shutdowns, trends in India point not only to a high number of short shutdowns but a spectrum of harmful, increasingly longer, and wider-ranging disruptions shrinking the civic space in the country.¹⁹

Four years after the historic Supreme Court judgment affirming the right to free speech and the fundamental right to carry out one’s trade or profession via the internet, officials continue to fail to publish shutdown orders and have been repeatedly corrected by courts for failing to comply, underscoring the urgent need for reform.²⁰ Meanwhile, the harms of shutdowns in the country continue to be immense and multi-faceted, impairing education, healthcare, press freedom, and more.²¹

Among them, internet shutdowns have deep impacts on India’s economy at all levels. According to calculations using the Internet Society’s NetLoss Calculator, a single-day shutdown can push up to 379 people into unemployment in India.²² Shutdowns reportedly cost the country $1.9 billion and a loss of $118 million in foreign investment in the first half of 2023 alone.²³ On an individual level, the economic damage of shutdowns can be devastating. For people in a large section of the workforce in India, shutdowns


³¹ Bhasin v. Union of India. [https://globalfreedomofexpression.columbia.edu/cases/bhasin-v-union-of-india/](https://globalfreedomofexpression.columbia.edu/cases/bhasin-v-union-of-india/)


INTERNET SHUTDOWNS IN 2023

Shutdowns especially hurt marginalized groups who rely on the internet for newer revenue streams and for accessing gatekept opportunities. These harms are amplified further when placed in the context of India’s race to digitize access to services. For people who are being pushed toward systems that depend on internet connectivity and access to mobile networks to function, the negative impact of internet shutdowns is only becoming more severe. In 2023, 59% (68) of the shutdowns in India exclusively targeted mobile networks — and where almost 96% of people with internet access depend on wireless services, disruption to mobile internet essentially equates to a full internet blackout. Rather than protecting communities, internet shutdowns in India are deepening the digital divide and undermining efforts toward equitable and inclusive digitization.

Despite clear economic effects, disproportionate impacts on marginalized groups, and the shielding of atrocities, authorities continue to implement shutdowns at all levels across India during protests, exams, elections, and communal violence.

East Asia

China’s government is equipped with some of the most sophisticated censorship and surveillance infrastructure in the world. For many years, through the Great Firewall, authorities have restricted access to websites, search engines, social media platforms, games, and more, leaving behind a heavily censored and highly surveilled internet ecosystem. In 2023, the government further tightened the vise, causing a reported spike in VPN use inside the country as people attempted to regain access despite severe punishments for those caught using circumvention technologies.

Due to the nature of China’s entirely state-controlled internet, which is splintered off from the rest of the world, remotely measuring internet traffic is nearly impossible and on-network investigations are very dangerous, making it extremely challenging to document distinct instances of network disruptions or throttling. In addition, while reports indicate shutdowns continue to happen with some frequency at a local level, the increasing totality of China’s surveillance and censorship regime means that authorities are able to deploy both wide nets of censorship and highly targeted disruptions, even targeting home and mobile connections of individual activists, reducing the need for full-network shutdowns. Many of China’s restrictions on communications platforms that operate from outside the country have been in place for a decade or longer and are not currently reflected in the KeepItOn database, which began in 2016. Our current data reflects China’s blocking of Signal and Grindr, both ongoing since 2021.

In Taiwan, following repeated damage to underwater cables in February 2023, 14,000 residents of the Matsu Islands lost internet and phone service for at least two months. Taiwanese authorities suspect the cables were cut by a Chinese fishing vessel and a Chinese cargo ship, each independently severing the cable in separate incidents only six days apart. Experts indicated the levels of damage to the steel-encased cables were “highly unusual.” According to Chunghwa, Taiwan’s largest telecoms provider, the cables have been cut 27 times in the past five years.

31 Supra note 4.
33 Ibid.
34 Ibid.
which is disproportionate to other regions globally.\textsuperscript{26} While there is not sufficient evidence to definitively confirm the 2023 cable cut as an intentional attack — and we therefore have not counted the disruption as an intentional shutdown in the #KeepItOn STOP database — the tactics are consistent with China’s overall “gray-zone warfare” strategy against Taiwan.\textsuperscript{26} This disruption has further highlighted the immense vulnerability of internet infrastructure for Taiwan and the region.\textsuperscript{27} China’s increased influence over undersea cable projects in the South China Sea and reduced U.S. investments in undersea cable projects in the region have both threatened to further destabilize an already precarious situation.\textsuperscript{28} To avoid disruptions to vital telecommunications services for people in Taiwan, as well as across East and Southeast Asia, it is vitally important to strengthen and secure digital infrastructure. The #KeepItOn coalition will continue to monitor internet disruptions from undersea cable cuts, in East Asia and around the world, as well as the potential weaponization of cable cuts and their impact on vulnerable communities.

// Shutdowns during protests and unrest

In Pakistan and Bangladesh, authorities imposed shutdowns throughout 2023 during protests, primarily related to political instability and election cycles. Pakistan saw seven shutdowns across 2023, with four of these directly linked to disrupting election campaigning, protests, and public expression as the Pakistani establishment tried to disrupt political mobilization by a prominent opposition party.\textsuperscript{39} Shutdowns in Pakistan have continued to escalate in 2024 as authorities suspended mobile internet on election day in February 2024 and blocked X (formerly Twitter) for weeks.\textsuperscript{40} Bangladesh saw three shutdowns in 2023, continuing a trend from 2022 where the ruling government used shutdowns to suppress political dissent by opposition parties during rallies.\textsuperscript{41}

\begin{itemize}
\item \textsuperscript{27} See, e.g., Reuters (2021). China’s latest weapon against Taiwan: the sand dredger. https://www.reuters.com/graphics/TAIWAN-CHINA/SECURITY/jbyvrnzerve/
\item \textsuperscript{28} Independent (2022). Potential threat to Taiwan’s undersea internet cables pose risk to global economy, experts warn. https://www.independent.co.uk/tech/undersea-internet-cables-taiwan-china-b2157223.html
\item \textsuperscript{29} NIKKEI Asia (2023). Taiwan’s island internet cutoff highlights infrastructure risks. https://asia.nikkei.com/Opinion/Taiwan-s-island-internet-cutoff-highlights-infrastructure-risks/
\end{itemize}
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 334 members from 106 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 Donna Wentworth, Ángela Alarcón, Bridget Andre, Golda Benjamin, Raman Jit Singh Chima, Giulio Coppi, Marwa Fatafta, Osei Manu Kagyah, Natalia Krapiva, Jaimee Kokonya, Namrata Maheshwari, Peter Micek, Kassem Mnejja, Wai Phyo Myint, Shruti Narayan, Laura O’Brien, Naro Omo-Osagie, Gaspar Pisanu, Prateek, Alexia Skok, Vakau, Aymen Zaghdoudi, and Anastasiya Zhyrmont for their contributions. We would also like to thank Advocacy Assembly Shutdown Academy, Athan, Cloudflare, Digitally Right, Internet Outage Detection and Analysis (IODA), Kentik, Miaan Group, Myanmar Internet Project, Open Observatory of Network Interference (OONI), Software Freedom Law Centre India (SFLC.in), and other members of the #KeepItOn coalition for providing valuable information and insights, 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 Loren Giordano and 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 2023. 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. In 2023, we gained insight into shutdowns from previous years that were added to the dataset retrospectively, and documentation of these changes can be found here: https://accessnow.org/keepiton-data. All data below reflects the most up-to-date information as of publication.

Visit https://accessnow.org/keepiton-data-methodology for the latest information on our methodology, commonly asked questions, and ongoing work.

May 2024
#KeepItOn

SHRINKING DEMOCRACY, GROWING VIOLENCE

Internet shutdowns in 2023