I. Internet shutdowns in 2022: a global overview

Overview of 2022 data

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

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

Number of countries where shutdowns occurred

<table>
<thead>
<tr>
<th>Year</th>
<th>India:</th>
<th>Ukraine:</th>
<th>Iran:</th>
<th>Myanmar:</th>
<th>Bangladesh:</th>
<th>Jordan:</th>
<th>Libya:</th>
<th>Sudan:</th>
<th>Turkmenistan:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>84</td>
<td></td>
<td>18</td>
<td>7</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td>22**</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2020</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2021</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

## Shutdown trends in 2022

1. **Grave human rights abuses*** and violence shrouded by shutdowns on the rise
   - **48 shutdowns in 14 countries coinciding with documented human rights abuses:** Bangladesh, Ethiopia, Iran, Jordan, Kazakhstan, Myanmar, Russia, Sierra Leone, Somaliland, Sudan, Tajikistan, Uzbekistan, and active conflict zones in Ukraine and Yemen
   - ***Human rights abuses include cases where there is evidence of violence, including murder, torture, rape, or apparent war crimes by governments, militaries, and police or security forces.***

2. **Countries entrenched in repeat offenses and prolonged shutdowns**
   - **787+ days**
     - By the end of 2022, people in Tigray, Ethiopia had endured 2+ years of full communications blackout, and many remain disconnected
   - **500+ days**
     - People in many regions across Myanmar had been in the dark for 500+ days by March 2023
   - **33 of the 35 countries that imposed shutdowns are repeat offenders since 2016**
   - **16 shutdowns worldwide lasted from 2021 to 2022 and 16 are now ongoing from 2022 to 2023, compared to 8 between 2020 and 2021**

3. **Targeted shutdowns and their immeasurable harms**
   - **23 countries had 28 service-based shutdowns in 2022:**
     - Afghanistan, Algeria, Armenia, Azerbaijan, Bangladesh, Brazil, Burkina Faso, China, India, Iran, Jordan, Kazakhstan, Nigeria, Oman, Russia, Sri Lanka, Tunisia, Turkey, Turkmenistan, Uganda, Ukraine (imposed by Russian military), Uzbekistan, and Zimbabwe
   - **Layered tactics of shutdown + censorship + surveillance:**
     - **Iran:** Nationwide platform blocks + curfew-style mobile blocks in regional hotspots
     - **Myanmar:** Disrupting mobile networks, VPN access, encrypted messaging + forcing people onto heavily surveilled, military-operated ISP networks
     - **Ukraine:** Cyberattacks impacting Ukrainian ISPs + attempts to force occupied territories onto highly censored and surveilled Russian networks
Across the MENA region, authorities have increasingly relied on internet shutdowns to suppress dissent, undermine political participation, and shield perpetrators of human rights abuses from accountability. The region saw both an emergence of new shutdowns and the continuation of disruptions communities have endured for years — including ongoing airstrikes in Yemen impacting telecommunications infrastructure and social media platform blocking in Oman continuing from 2021. Authorities also imposed disruptions in the cities of Darna, Tobruk, and Benghazi coinciding with visits from Khalifa Haftar, the Commander-in-Chief of the Tobruk-based Libyan National Army. While shutdowns are becoming more entrenched, affected communities are becoming more entrenched, affected communities

INTERNET SHUTDOWNS IN 2022

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

Platform blocks

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

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

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

17 Ibid.
Exam-related shutdowns

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

// Iran

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

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

As protests persisted and grew, authorities proceeded to block access to the global internet and repeatedly shut down mobile networks, both nationally and in targeted areas, while also continuing to block Instagram and WhatsApp — cutting off access to two of the only social media platforms that have remained accessible in Iran in recent years. This layering of shutdown tactics was a clear attempt to hide atrocities and human rights violations. The government relied heavily on persistent social media blocks to prevent protesters from organizing and to keep news of atrocities and human rights violations from spreading. While they typically kept mobile networks online during work hours, an effort to minimize the economic impact of the disruptions, authorities imposed curfew-style mobile shutdowns in target areas, while also continuing to block Instagram and WhatsApp nationwide.

26 Ibid.
the evenings to prevent coordination and documentation of protests. The Iranian regime clamped down particularly hard on dissent in regions with marginalized groups, with 50% of all shutdowns in 2022 targeting ethnic minorities from the Kurdistan, Baluchestan, and Ahvaz regions through blanket, regional shutdowns.

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

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

The crackdown and censorship in Iran drew international condemnation, with the U.S. lifting sanctions to increase internet freedom and access to information in Iran. For instance, the U.S. Department of the Treasury issued Iran General License (GL) D-2 to increase support for internet freedom in Iran by bringing U.S. sanctions guidance in line with the changes in modern technology since the issuance of the 2014 license, Iran GL D-1. Ultimately, this means U.S.-based companies can offer

---

tools and services like video conferencing, e-gaming, e-learning platforms, automated translation, web maps, user authentication services, and cloud services to people in Iran with confidence they are not breaking U.S. law. Still, work remains to combat corporate overcompliance with sanctions, and to ensure that tech companies and financial intermediaries allow the free flow of all data, hardware, software, services, and transactions possible under the newly expanded license.\textsuperscript{37} Other actors like the European Union and the Freedom Online Coalition (FOC) — a network of 36 governments advancing internet freedom globally — issued statements to denounce the internet blackout and crackdown on protesters in Iran.\textsuperscript{38}

\textbf{Sudan}

For years, the people of Sudan have been fighting for democracy and respect for human rights in their country, but their movement has been repeatedly met with weaponized internet shutdowns and social media blocks designed to suppress dissent.\textsuperscript{39} Since forcibly taking power in October 2021, the military government has increasingly taken action against those who raise their voices to resist their military rule, including four internet shutdowns in 2022. Mass protests and intermittent shutdowns gripped Sudan in the months following the October 2021 military coup.\textsuperscript{40} Authorities disrupted the internet for 12 hours on January 2, 2022,\textsuperscript{41} as thousands of people resumed their protests to demand the return of civilian rule, prompting Prime Minister Abdalla Hamdok to resign on January 3.\textsuperscript{42}

When people took to the streets across the country once again on June 30 in the “March of the Millions,” marking the third anniversary of the 2019 uprising and ousting of former Sudanese President Omar Al-Bashir, eight protesters\textsuperscript{43} were reportedly shot dead by the military amidst an internet blackout.\textsuperscript{44} Authorities similarly took mobile networks offline nationwide amid protests on the one-year anniversary of the military coup on October 25.\textsuperscript{45}

The military government has also taken aim at civil society organizations challenging the use of shutdowns in the country, including by revoking accreditation from the Sudanese Consumers Protection Society (SCPS), which has been a leader in challenging internet shutdowns through litigation.\textsuperscript{46} In 2021, SCPS helped get millions back online after a court ruled in its favor and ordered telecommunications companies to fully restore internet connectivity across the country.\textsuperscript{47}

\begin{itemize}
\item \textsuperscript{40} Access Now (2021). \textit{Internet shutdowns and blockings continue to hide atrocities of military coup in Sudan}. Retrieved February 18, 2023, from https://www.accessnow.org/update-internet-shutdown-sudan/.
\item \textsuperscript{41} Doug Madory (@DougMadory) Twitter Post. 10:01 PM. January 4, 2022. Retrieved February 18, 2023, from https://twitter.com/DougMadory/status/1478441370721337349.
\item \textsuperscript{44} Cloudflare Radar (@CloudflareRadar) Twitter Post. 11:34 AM. June 30, 2022. Retrieved February 18, 2023, from https://twitter.com/CloudflareRadar/status/1542426430625161216.
\item \textsuperscript{45} Doug Madory (@DougMadory) Twitter Post. 9:04 PM. October 25, 2022. Retrieved February 18, 2023, from https://twitter.com/DougMadory/status/1584969055399596032.
\item \textsuperscript{46} Alarabiya News (2022). \textit{Sudan suspends NGO that took government to court over internet access}. Retrieved February 18, 2023, from https://english.alarabiya.net/News/middle-east/2022/10/23/Sudan-suspends-NGO-that-took-government-to-court-over-internet-access.
\end{itemize}
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