I. Internet shutdowns in 2022: a global overview

Overview of 2022 data

Documented internet shutdowns by year *

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

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

Number of countries where shutdowns occurred

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

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


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

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

Shutdown triggers in 2022

Protests  62 shutdowns in 16 countries during protests

Active conflicts

Exams  8 shutdowns in 6 countries “to prevent exam cheating”

Elections  5 shutdowns in 5 countries tied to elections

Shutdown trends in 2022

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

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

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

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

2. Countries entrenched in repeat offenses and prolonged shutdowns

787+ days

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

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

500+ days

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

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

3. Targeted shutdowns and their immeasurable harms

23 countries had 28 service-based shutdowns in 2022:

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

Layered tactics of shutdown + censorship + surveillance:

Iran: Nationwide platform blocks + curfew-style mobile blocks in regional hotspots

Myanmar: Disrupting mobile networks, VPN access, encrypted messaging + forcing people onto heavily surveilled, military-operated ISP networks

Ukraine: Cyberattacks impacting Ukrainian ISPs + attempts to force occupied territories onto highly censored and surveilled Russian networks
As countries in Eastern Europe and Central Asia (EECA) sink deeper into authoritarianism, internet shutdowns and censorship have become increasingly prevalent during protests and elections. In the context of conflict and crisis across the region, from Russia’s attacks on Ukraine to governments’ violent crackdowns on protests across Central Asia, authorities have weaponized internet shutdowns to keep people in the dark and to carry out human rights abuses with impunity.

Central Asia

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

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

Eastern Europe and Central Asia
Regional overview in 2022

- **Ukraine**: 22 shutdowns imposed by Russia during its invasion
- **Armenia**: 1 first internet shutdown on record
- **Turkmenistan**: 4
- **Kazakhstan**: 2
- **Russia**: 2
- **Tajikistan**: 2
- **Uzbekistan**: 2
- **Azerbaijan**: 1

Top 3 triggers of shutdowns in the region

- **Conflict**: 22
- **Information control**: 5
- **Protest**: 4

77.3% of shutdowns in Ukraine were directly targeting the communications infrastructure. That’s 17 shutdowns.

---


2 Ibid.


Uzbek and Tajik authorities also met protests with violent crackdowns and internet blackouts in the autonomous region of Karakalpakstan⁵ and the Gorno-Badakhshan Autonomous Region (GBAO),⁶ respectively — highlighting the disproportionate impact shutdowns often have on marginalized communities like the Karakalpak and Pamiri ethnic groups.

Authorities in Turkmenistan⁷ and Uzbekistan⁸ both implemented communications platform shutdowns, a tactic they have increasingly deployed in the past few years alongside censorship of websites and blocking of VPNs in an effort to control information and squash dissent.

// Russia's invasion of Ukraine

In 2022, during the course of Russia’s full-scale invasion of Ukraine beginning in February, the Russian military imposed 22 shutdowns on Ukrainian cities and oblasts through a combination of cyber attacks, targeted air strikes, and deliberate dismantling of telecommunications infrastructure.⁹

Russia has systematically targeted civilian infrastructure across Ukraine, attempting to break down popular resistance to the invasion, restrict the flow of information, and inflict damage to communities in retaliation when Ukraine has successfully forced Russian troops out of occupied cities. These tactics have inflicted devastating harms, and at least 12 of the 22 shutdowns that occurred in Ukraine took place in parallel to documented human rights abuses. Lack of electricity, water, and food, combined with indiscriminate and brutal killings of civilians¹⁰ have been common throughout the invasion, often alongside disrupted communications and internet blackouts. In response, Ukraine has set up 4,000

---


“invincibility centers” where people can get warm, eat, charge devices, and connect to the internet. The government is also requiring ISPs to stock enough batteries, generators, and solar panels to stay online for at least three days in the case of blackouts.

In formerly occupied Kherson, one of the areas Russia attempted to use as a foothold to serve as a base for its incursions deeper into Ukrainian territory, Russian forces systematically worked to displace Ukrainian telecommunications services with Russian ones, going so far as to reroute traffic and even lay new fiber optic cables from Crimea. These efforts resulted in significant lapses in connectivity for Ukrainians, and where Russia restored connection, it forced people onto the heavily censored and surveilled Russian internet.

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

// Armenia-Azerbaijan territorial dispute

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

12 Ibid.
14 See supranote 9.
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