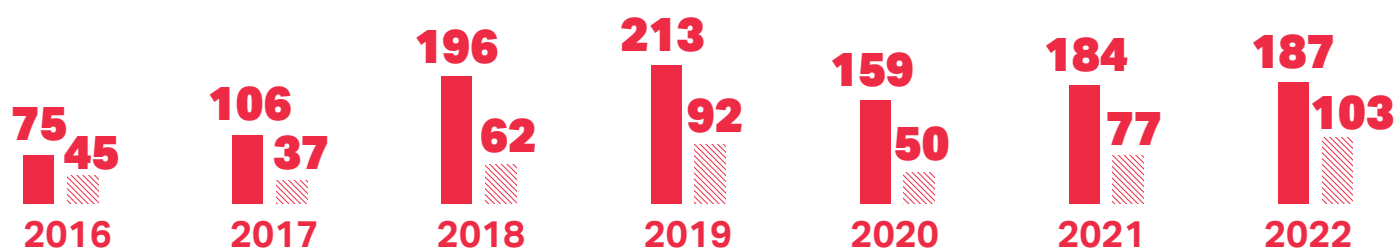


I. Internet shutdowns in 2022: a global overview

Overview of 2022 data

Documented internet shutdowns by year *

■ Total number of shutdowns
□ Total number of shutdowns, not including India



* 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



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** **Zimbabwe:** 1

** Shutdowns were imposed by external forces during armed conflict in Ukraine and Yemen.

Shutdown triggers in 2022

Protests	62 shutdowns in 16 countries during protests	Active conflicts	33 shutdowns during 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

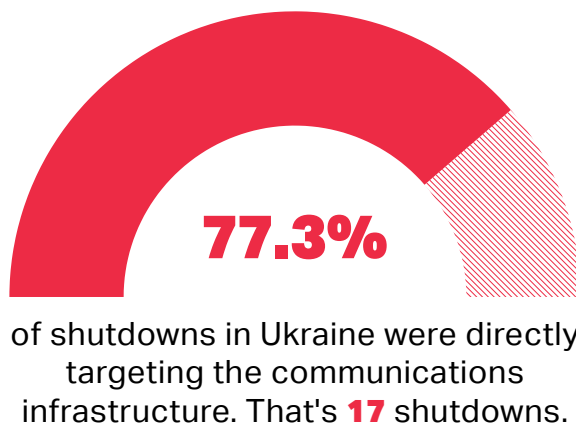
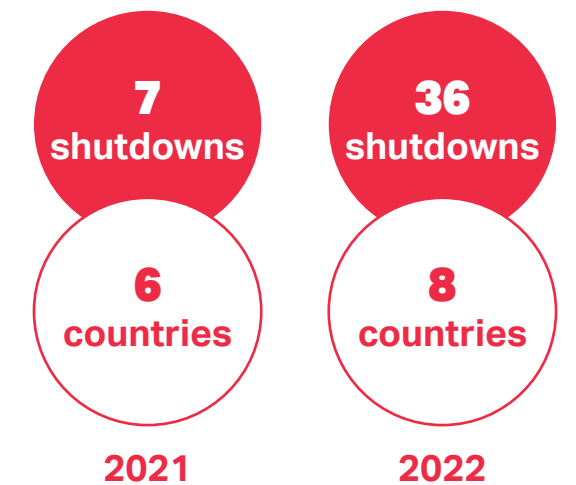
→ Layered tactics of shutdown + censorship + surveillance:

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

Eastern Europe and Central Asia Regional overview in 2022



Ukraine: 22

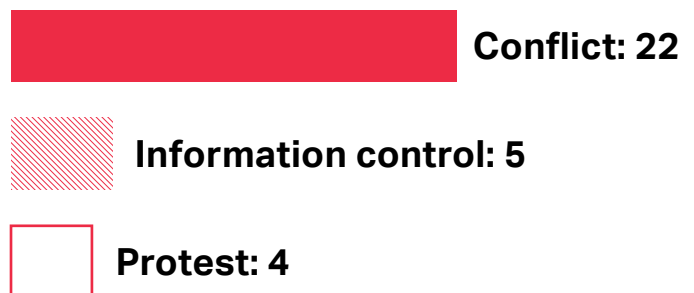
All shutdowns imposed by Russia during its invasion

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



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.¹ 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.² The impacts have been devastating, disrupting people's access to food, healthcare, education, and life-saving information.³

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.⁴

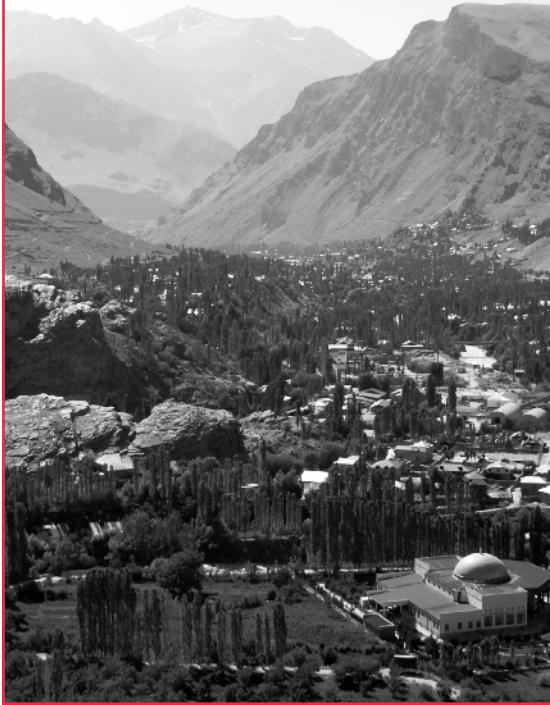
¹ Access Now (2022). *Digital dictatorship: authoritarian tactics and resistance in Eastern Europe and Central Asia*. Retrieved February 19, 2023, from <https://www.accessnow.org/digital-dictatorship-and-resistance-in-eastern-europe-and-central-asia/>.

² *Ibid.*

³ Access Now (2022). *In Central Asia, internet shutdowns are harming all kinds of rights*. Retrieved February 18, 2023, from <https://www.accessnow.org/central-asia-internet-shutdowns-harm-rights/>.

⁴ Access Now (2022). *Timeline: Kazakhstan internet shutdowns aim to crush protests, hide state violence*. Retrieved February 18, 2023, from <https://www.accessnow.org/kazakhstan-internet-shutdowns-protests-almaty-timeline-whats-happening/>.

Shutdown impact story: Tajikistan



"I owned two pharmacies in Khorog, where I come from. We provided medications and medical supplies to hospitals and individuals. The internet played a key role in this business, since all transfers, settlements with suppliers, filing taxes, basically, all business control was carried out remotely via the internet.

But everything changed for me and my business when authorities in Tajikistan imposed a four months-long internet shutdown to quell protests in Khorog. My business was undoubtedly hit hard as we couldn't operate efficiently anymore. I was forced to let go of my staff and eventually closed down the business. I lost over [USD] \$15,000."

A businessman in Khorog

Photo: [Kondephy](#)

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

⁵ Access Now (2022). *Uzbekistan region in information vacuum, authorities must #KeepItOn*. Retrieved February 18, 2023, from <https://www.accessnow.org/uzbekistan-information-vacuum-keepiton/>.

⁶ The Diplomat (2022). *Tajikistan Lifts Internet Block on GBAO. What's Next?* Retrieved February 18, 2023, from <https://thediplomat.com/2022/06/tajikistan-lifts-internet-block-on-gbao-whats-next/>.

⁷ Access Now (2021). *What Turkmenistan internet shutdowns tell us about digital repression in Central Asia*. Retrieved February 18, 2023, from <https://www.accessnow.org/turkmenistan-internet-shutdowns/>.

⁸ The Diplomat (2022). *Uzbekistan Unblocks Twitter, TikTok Still Restricted*. Retrieved February 18, 2023, from <https://thediplomat.com/2022/08/uzbekistan-unblocks-twitter-tiktok-still-restricted/>.

⁹ Access Now (2022). *#KeepItOn: Who is shutting down the internet in Ukraine?* Retrieved February 22, 2023, from <https://www.accessnow.org/who-is-shutting-down-the-internet-in-ukraine/>.

¹⁰ Human Rights Watch (2022). *Ukraine: Mariupol Residents Trapped by Russian Assault*. Retrieved February 18, 2023, from <https://www.hrw.org/news/2022/03/07/ukraine-mariupol-residents-trapped-russian-assault>.

"invincibility centers" where people can get warm, eat, charge devices, and connect to the internet.¹¹ 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.¹²

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.¹³ 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.¹⁴ Ukraine fought back against Russia's efforts, with Ukrainian service providers implementing blocks where Russia had gained access to their equipment, and Ukrainian intelligence services destabilizing the newly run fiber optic cable.¹⁵ While important acts of resistance, the battle for control over telecommunications infrastructure further exacerbated disruptions in service for the people of Ukraine.

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.¹⁶ As a response to Russia's pressure on platforms, TikTok took its own measures to severely limit access to its services in the country.¹⁷ 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.¹⁸

// 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.**¹⁹

¹¹ The Kyiv Independent (2022). *People seek relief at 'invincibility centers' amid long power outages*. Retrieved February 18, 2023, from <https://kyivindependent.com/news-feed/people-come-to-invincibility-centers-in-kyiv-amid-long-power-outages>.

¹² *Ibid.*

¹³ The New York Times (2022). *How Russia Took Over Ukraine's Internet in Occupied Territories*. Retrieved February 18, 2023, from <https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html>.

¹⁴ See *supra* note 9.

¹⁵ Liga.net (2022). *Інтерв'ю | Росія – законна ціль. Голова Держспецзв'язку Юрій Щиголь про санкції та невдалі кібератаки РФ [Interview | Russia is a legitimate target. Head of the State Special Forces Yuriy Shchygol on sanctions and failed cyberattacks of the Russian Federation]*. Retrieved February 18, 2023, from <https://tech.liga.net/ua/ukraine/interview/glava-gosspetssvyazi-yuriy-schigol-o-svyazi-v-hersone-tehnosanktsiyah-i-starlink-v-poezdah>.

¹⁶ Access Now (2022). *Updates: Digital rights in the Russia-Ukraine conflict*. Retrieved February 18, 2023, from <https://www.accessnow.org/digital-rights-ukraine-russia-conflict/>.

¹⁷ Coda Story (2022). *A Russian user looks inside TikTok's propaganda-filled digital bubble*. Retrieved February 18, 2023, from <https://www.codastory.com/newsletters/russia-tiktok-propaganda/>.

¹⁸ Access Now (2022). *UK protects free flow of information amidst Russia sanctions*. Retrieved February 22, 2023, from <https://www.accessnow.org/uk-information-russia-sanctions/>; Access Now (2022). *U.S. moves to keep the Russian people connected despite sanctions*. Retrieved February 22, 2023, from <https://www.accessnow.org/u-s-treasury-russia-sanctions-internet/>.

¹⁹ Access Now (2022). *Turn TikTok on: authorities in Azerbaijan and Armenia must not restrict access*. Retrieved February 18, 2023, from <https://www.accessnow.org/tiktok-azerbaijan-armenia/>.

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 Fatafta, Raman Jit Singh Chima, Wai Phyo Myint, Golda Benjamin, Anastasiya Zhyrmont, Natalia Krapiva, Ángela Alarcón, Bridget Andere, 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

