

9/14/2021 Myanmar

8/26/2023 Gabon

023 Suriname

3/9/2023 Ukraine

2/26/2022 Russia

4/23/2023 Sudan

5/3/2023 India

10/20/2021 Turkmenistan

1/4/2020 Ethiopia

10/26/2023 Palestine

SHRINKING DEMOCRACY, GROWING VIOLENCE

Internet shutdowns in 2023

#KeepItOn 



#KeepItOn

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 Andere, 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



Table of contents

I. Internet shutdowns in 2023: a global overview	5
II. Triggers for internet shutdowns in 2023	12
Shutdowns during conflicts	12
Shutdowns during protests and instability	13
Shutdowns during elections	14
Shutdowns during exams	15
Shutdowns during natural disasters	15
III. New and continuing trends in 2023	16
Shutdowns continue to shroud grave human rights abuses and violence	16
Authorities must refrain from normalizing platform blocks	17
Worst offenders are entrenched and emboldened in the use of shutdowns	21
The geographic scope of shutdowns is broadening	22
IV. Internet shutdowns by region	23
Africa	24
Shutdowns during protest, political turmoil, and instability	25
Shutdowns during elections	26
Shutdowns during conflict: Ethiopia	28
Platform blocks	29
Asia Pacific	30
Myanmar	30
India	32
East Asia	34
Shutdowns during protests and unrest	35
Eastern Europe and Central Asia (EECA)	36
Russia and Ukraine	36
Azerbaijan-Armenia conflict	38
Central Asia	40
Latin America and the Caribbean (LAC)	41
Middle East and North Africa	43
Palestine	44
Sudan	45
Iran	46
Shutdowns during exams	47
Platform blocks and other events	48
V. Fighting back in 2023: Growth, support, solidarity, and resilience	50
VI. Recommendations for stakeholders	53
VII. Join us	57



I. Internet shutdowns in 2023: a global overview

Authors' note

Year after year, since Access Now first began issuing our series of annual #KeepItOn reports,¹ we have been confronted with worsening conditions for internet shutdowns and human rights globally.² This report for 2023 is no exception, and many of the realities people faced this past year are not new, with the harms we have been documenting now for more than eight years repeating and intensifying. Even still, **2023 stands apart.**

The gravity of our findings in this year's report cannot be overstated and should be read as **an urgent call to action** for all stakeholders. Authorities have leveraged internet shutdowns as a blatant tool for enabling and exacerbating violence, war crimes, and other atrocities. Tens of thousands of lives have been taken — from Palestine to Myanmar, Sudan to Ukraine — by attackers using internet shutdowns to shield their actions from accountability. We cannot allow them to succeed.

While we discuss quantitative analysis around the number of shutdowns and how they are deployed around the world throughout the report, we must first center the individual people and communities who are impacted by them, and in particular those who have lost their lives or suffered unspeakable acts of violence while being cut off from the world.

We cannot treat these findings as the inevitable continuation of a worsening trend, but rather as a call to redouble our collective efforts to uphold human rights, particularly for the most vulnerable among us.

To the #KeepItOn community and the many frontline defenders who have made the research, documentation, and advocacy behind this report possible, we extend our gratitude and honor your efforts. This work is grueling and has taken a heavy toll on many in our community. Know that your tireless efforts are not in vain.

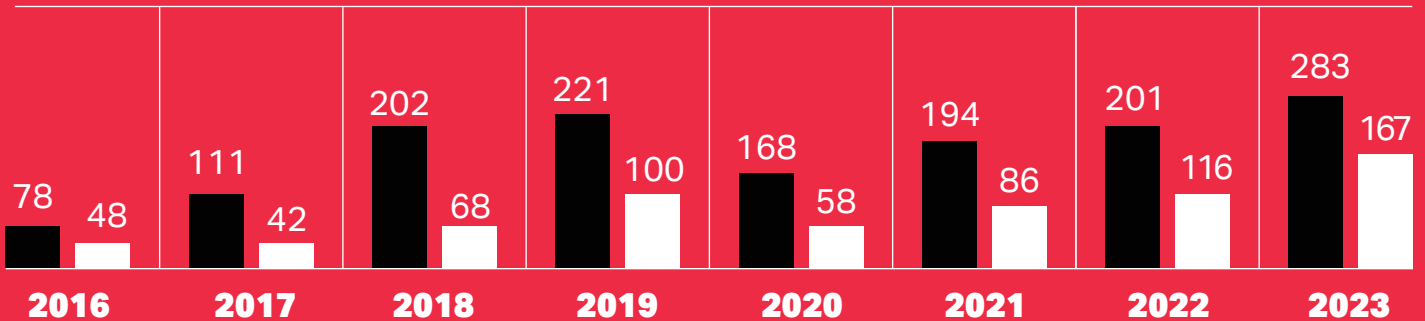
¹ Access Now (2019). *The State of Internet Shutdowns Around the World: The 2018 #KeepItOn Report*. <https://www.accessnow.org/keepiton-2018-report>; Access Now (2020). *Targeted, cut off, and left in the dark: The #KeepItOn report on internet shutdowns in 2019*. <https://www.accessnow.org/keepiton-2019-report>; Access Now (2021). *Shattered dreams and lost opportunities: A year in the fight to #KeepItOn*. <https://accessnow.org/keepiton-2020-report/>; Access Now (2022). *The return of digital authoritarianism: Internet shutdowns in 2021*. <https://accessnow.org/keepiton-2021-report>; Access Now (2023). *Weapons of control, shields of impunity: Internet shutdowns in 2022*. <https://www.accessnow.org/keepiton-2022-report>

² An internet shutdown has been defined as “an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.” An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. See Access Now (2016). *No more internet shutdowns! Let's #KeepItOn*. <https://www.accessnow.org/no-internet-shutdowns-lets-keepiton/>

Overview of 2023 data

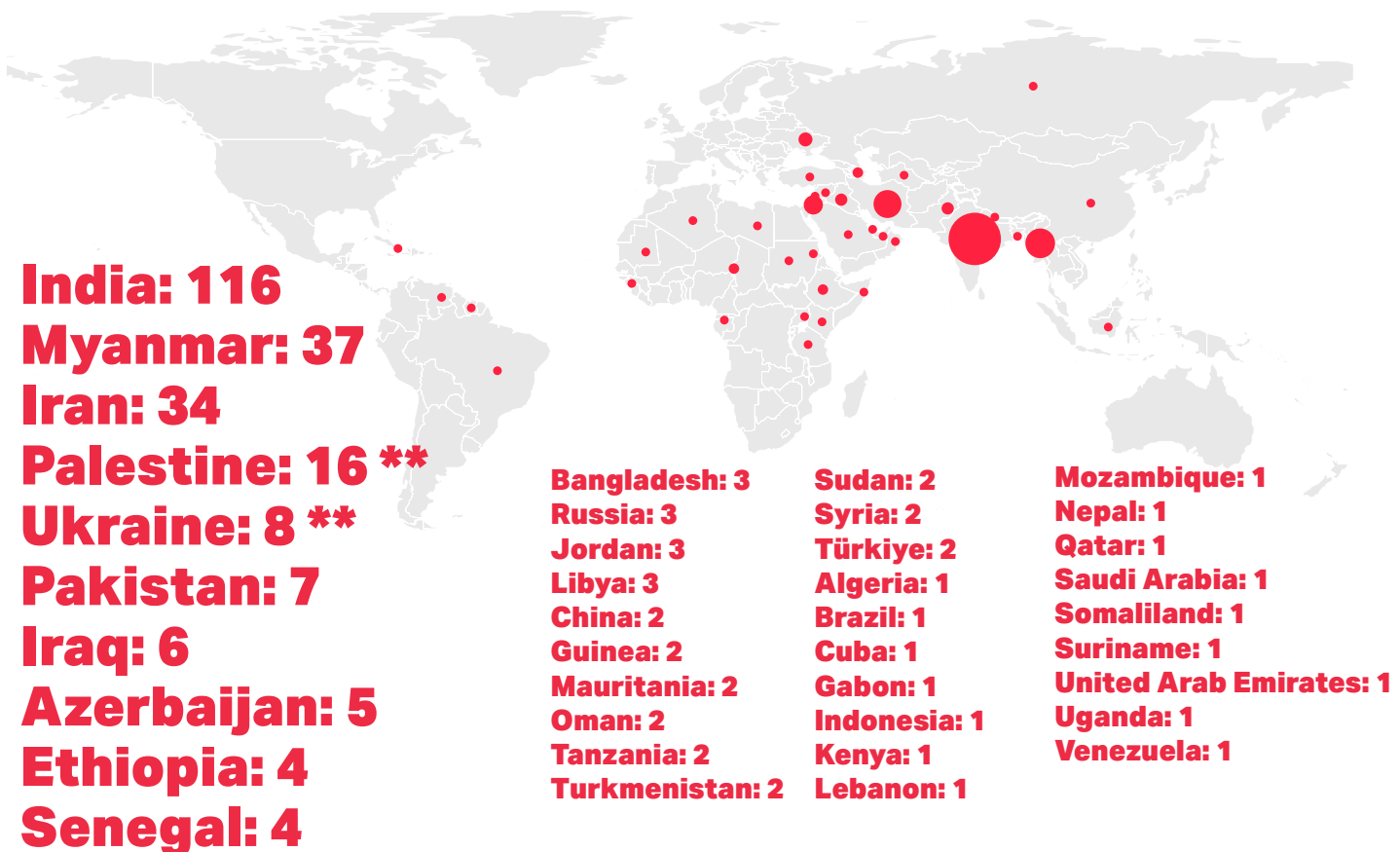
Documented internet shutdowns by year *

■ 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



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

Shutdown triggers in 2023

 Conflicts	 Protests	 Exams	 Elections
74 shutdowns in 9 countries during conflicts	63 shutdowns in 15 countries during protests	12 shutdowns in 6 countries "to prevent exam cheating"	5 shutdowns in 5 countries tied to elections
2023: 74 	2023: 63 	2023: 12 	2023: 5 
2022: 36 	2022: 63 	2022: 8 	2022: 5 
2021: 19 	2021: 39 	2021: 11 	2021: 7 
2020: 15 	2020: 16 	2020: 8 	2020: 10 
2019: 52 	2019: 65 	2019: 8 	2019: 12 
2018: 2 	2018: 45 	2018: 11 	2018: 12 
2017: 3 	2017: 37 	2017: 7 	2017: 6 
2016: 3 	2016: 27 	2016: 6 	2016: 5 

Emerging trigger in 2023:



Natural disasters

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.

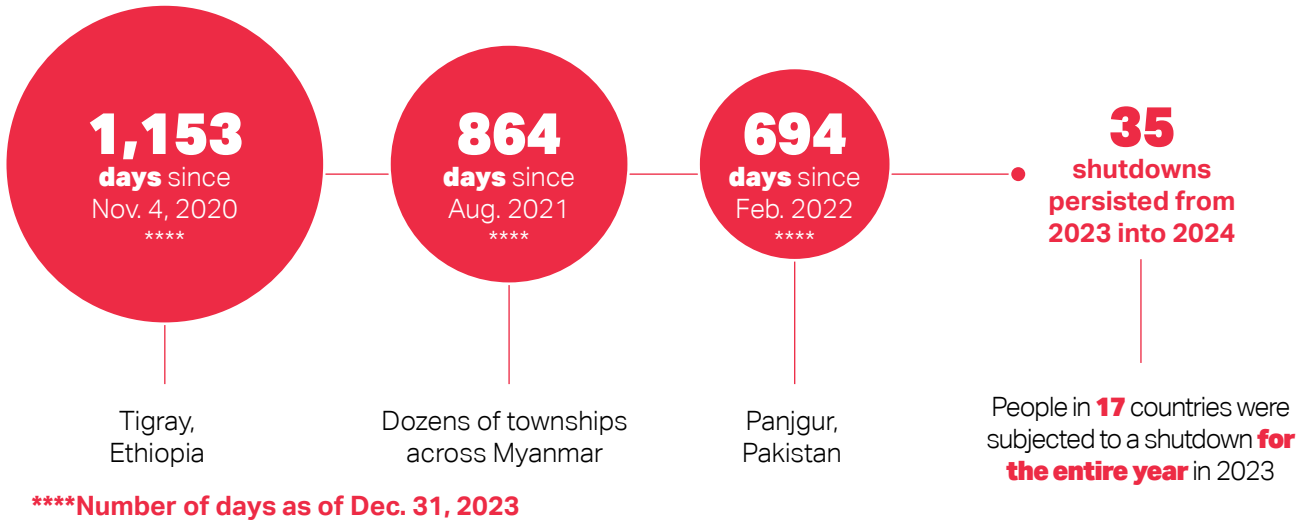
2. Authorities must refrain from normalizing platform blocks

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



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

334

#KeepItOn coalition members from **106** countries

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

By nearly every measure, 2023 is the worst year of internet shutdowns ever recorded — highlighting an alarming and dangerous trend for human rights.

From Senegal to Ethiopia, Nepal to India, Israel to Russia, governments continued to shut down the internet and critical digital communication platforms to muzzle expression, block access to life-saving information, and cover up heinous crimes against humanity. Despite the increasing momentum gathering globally against the use of internet shutdowns and key examples of past offenders charting a new course, shutdowns are continuing to emerge as the go-to tool for both democratic and authoritarian regimes to suppress fundamental human rights.

In 2023, Access Now and the #KeptOn coalition documented **283** shutdowns in **39** countries. These are staggering results, marking the highest number of shutdown incidents in a single year since we began our monitoring in 2016.³ This reflects an additional 82 shutdowns, or a **41% increase**, from 2022, when we recorded 201 shutdowns in 40 countries.⁴ It is also a **28% increase** from 2019, which was the previous record high with 221 shutdowns.⁵

Governments, militaries, and other authorities doubled down on internet shutdowns as a weapon of control during critical national moments or crises in 2023. Protests, school exams, and elections all remained notable triggers, with **63** protest-related shutdowns nearly reaching the previous high of 65 cases from 2019. We are monitoring these cases closely in 2024, as protest activities continue to rebuild after

the COVID-19 outbreak and emerge on new fronts,⁶ and elections are underway for nearly half the world's population.⁷ Importantly, **conflicts emerged for the first time as the leading driver of internet shutdowns** in 2023, and shutdowns intersecting with natural disasters surfaced as a concerning new trend.

As people struggle without access to essential platforms and services amid conflict, humanitarian disasters, and other moments of upheaval, the impact of internet shutdowns is becoming more and more devastating and increasingly an issue of life and death. More militaries are using shutdowns as part of a deliberate strategy to cut populations off from the world, either as a precursor to atrocities and violence against civilians or as part of a continuous, systematic dismantling of civilian infrastructure.⁸ Likewise, the weaponization of internet shutdowns during active conflict has resulted in compounding humanitarian crises.⁹ In conflict zones and beyond, 2023 is **the most violent year of shutdowns on record**, with 173 shutdowns corresponding to acts of violence — a **26% increase** from 2022. This trend has been increasing at an alarming rate year over year.

In 2023, people in **four** countries were impacted by shutdowns for the first time — a resurgence of the spread of internet shutdowns globally after an all-time low of **two** new offenders emerged in 2022. We are also seeing significant global shifts away from highly localized shutdowns toward disruptions impacting wider geographies, including the highest-ever number of multi-regional or nationwide blocks (**80**), leaving millions in the dark. Israel and Russia are also driving the growing number of internet shutdowns imposed from outside the impacted territory, wielded as a weapon of war or mechanism for disrupting the free flow of information, in Gaza and

³ As we disclose in our note on data at the beginning of this report, in 2023 we added information on shutdowns that were not previously recorded in our data set, including platform blocks. Figures throughout this report represent our most up-to-date information at the time of publication.

Access Now (2024). *The Shutdown Tracker Optimization Project (STOP) dataset*. <https://www.accessnow.org/keepiton-data>

⁴ *Supra* note 1. Access Now (2023).

⁵ *Supra* note 1. Access Now (2020).

⁶ Carnegie Endowment for International Peace (2023). *Protests in 2023: Widespread Citizen Anger Continues, With Sources Multiplying*. <https://carnegieendowment.org/2023/12/18/protests-in-2023-widespread-citizen-anger-continues-with-sources-multiplying-pub-91256/>

⁷ Access Now (2024). 2024 elections and internet shutdown watch. <https://www.accessnow.org/campaign/2024-elections-and-internet-shutdowns-watch/>

⁸ See, e.g., The Irrawaddy (2023). *Blockade of Myanmar's Rakhine State Leaves Residents Increasingly Desperate And Isolated*. See, e.g., <https://www.irrawaddy.com/news/burma/blockade-of-myanmars-rakhine-state-leaves-residents-increasingly-desperate-and-isolated.html>

⁹ See, e.g., Access Now (2024). *The Sudan conflict: how internet shutdowns deepen a humanitarian crisis*. <https://www.accessnow.org/the-sudan-conflict-how-internet-shutdowns-deepen-a-humanitarian-crisis/>

Ukraine, respectively.¹⁰ Cable cuts impacting Taiwan's Matsu Islands suggest China may also be among this group.¹¹ In addition, authorities continued to impose high numbers of platform blocks, cutting off entire countries from essential communications platforms as well as targeting specific vulnerable communities, as we've seen with the growing list of countries targeting LGBTQ+ people by blocking platforms like Grindr.

In 2023, we saw internet shutdowns impacting more people in more places more often, and a solidifying core of worst offenders wielded shutdowns with impunity. Despite the fact that these shutdowns flagrantly violate human rights enshrined in national, regional, and international frameworks, governments deliberately imposed shutdowns to advance their own political interests — harming people and communities and endangering lives.¹² Authorities continued to give insufficient or ill-defined reasons for implementing shutdowns, such as national security concerns, public safety, or to prevent the spread of misinformation and hate speech, using disruptions either as a disproportionate and ineffective tool for addressing a problem or in obvious efforts to oppress, silence, and control. In the majority of cases, governments took no responsibility and offered no explanation.

Despite these troubling developments, there has been overwhelming support and solidarity from the international community in our fight against internet shutdowns, and **we saw stakeholders around the world stepping up with unprecedented action in 2023 to #KeepItOn.**

As part of our collective advocacy with coalition members and partners through the #KeepItOn Election

Watch, we saw a record-high **three** countries with a history of shutdowns — the Democratic Republic of the Congo (DRC), Nigeria, and Sierra Leone — make and uphold public commitments to keep people connected during their 2023 election cycles.¹³

Common causes for internet shutdowns

Stated



National security



Public safety



Preventing the spread of misinformation and hate speech

Actual



Oppress



Silence



Control

In 2024, we welcomed similar commitments from authorities in Bangladesh to ensure people had access to open and secure internet during the general elections in February.¹⁴

The Freedom Online Coalition (FOC) — a partnership of 39 governments — also published a landmark joint statement urging governments to stop imposing internet shutdowns during electoral periods in accordance with their international human rights

¹⁰ Access Now (2023). *How Israel is shutting down the internet in Gaza*. <https://www.accessnow.org/press-release/how-israel-is-shutting-down-the-internet-in-gaza/>; Access Now (2024). *What they did in the shadows: Internet shutdowns and atrocities in Ukraine*. <https://www.accessnow.org/internet-shutdowns-and-atrocities-in-ukraine/>

¹¹ NIKKEI Asia (2023). *Taiwan's island internet cutoff highlights infrastructure risks*. <https://asia.nikkei.com/Opinion/Taiwan-s-island-internet-cutoff-highlights-infrastructure-risks/>

¹² See Access Now (2023). *U.N. passes landmark resolution condemning internet shutdowns*. <https://www.accessnow.org/press-release/un-passes-resolution-condemning-internet-shutdowns/>; Médecins sans frontières (n.d.). *The Practical Guide to Humanitarian Law; Collective punishment*. <https://guide-humanitarian-law.org/content/article/3/collective-punishment/>; Access Now (2022). *#KeepItOn: frequently asked questions; Key Stakeholder Groups*. <https://www.accessnow.org/campaign/keepiton/keepiton-faq/#key-stakeholder-groups>

¹³ Access Now (2023). *2023 elections and internet shutdowns watch*. <https://www.accessnow.org/campaign/2023-elections-and-internet-shutdowns-watch/>; Actu7 (2023). *Elections 2023: "On ne coupera pas la connexion internet le jour du vote" (Peter Kazadi)*. <https://actu7.cd/2023/12/19/elections-2023-on-ne-coupera-pas-la-connexion-internet-le-jour-du-vote-peter-kazadi/>; Sahara Reporters (2023). *Nigerian Communications Commission Says No Network Shutdown During General Elections*. <https://saharareporters.com/2023/02/24/nigerian-communications-commission-says-no-network-shutdown-during-general-elections/>; Felicia Anthonio (@FelAnthonio). X post. 4:50 pm. June 29, 2023. <https://x.com/FelAnthonio/status/1674460297715757080>

¹⁴ The Financial Express (2024). *Regulator orders nonstop telecom services during election*. <https://today.thefinancialexpress.com.bd/metro-news/regulator-orders-nonstop-telecom-services-during-election-1704387656/>

obligations, looking with particular concern to the unprecedented number of elections slated for 2024.¹⁵

For the first time, the International Telecommunication Union (ITU) — one of the world's most influential bodies on governance of digital communications technologies — took a clear stance against internet shutdowns, condemning the communications blackout in Gaza and calling for "life-saving access to networks to be restored."¹⁶

Individual policymakers and government agencies also played their part. In Iraq, where government-ordered shutdowns around exam periods have harmed communities every year since we first started recording cases in 2016, we saw the Ministry of Communications stepping up for the first time to publicly challenge the practice.¹⁷ Though it ultimately didn't change the course of exam-related shutdowns in the country for 2023, it is important to acknowledge and support these dissenting voices advocating for a more rights-respecting approach. European Union officials also stepped up amid concerning developments to affirm that the newly adopted Digital Services Act (DSA) will not be used as a vehicle for imposing internet shutdowns.¹⁸

As democratic institutions falter, civic space shrinks, and wars escalate around the world, shutdowns have become a convenient tool for oppression and marginalization. The drastically high total number of shutdowns globally, entrenched use by the worst offenders year after year, and impunity for authorities has demonstrated how challenging the fight remains to #KeepItOn. Yet civil society and impacted communities have shown time after time their strength and ingenuity in working to mitigate and prevent internet shutdowns. **With so much on the line, we must join together to bring internet shutdowns to an end.**

¹⁵ Freedom Online Coalition (2023). *Joint statement on internet shutdowns and elections*. <https://freedomonlinecoalition.com/joint-statement-internet-shutdowns-and-elections/>

¹⁶ International Telecommunication Union (@ITU). X post. 9:34 am. October 28, 2023. <https://x.com/ITU/status/1718199636932890906>

¹⁷ Kurdistan24 (2023). *Iraq's communication ministry refuses to enforce internet blackout for final exams*. <https://www.kurdistan24.net/en/story/31453-Iraq%E2%80%99s-communication-ministry-refuses-to-enforce-internet-blackout-for-final-exams/>

¹⁸ Access Now (2023). *Civil society gets its confirmation from EU Commissioner: no internet shutdowns under DSA*. <https://www.accessnow.org/press-release/commissioner-breton-responds-dsa/>

II. Triggers for internet shutdowns in 2023

Triggers of internet shutdowns refer to incidents during which authorities are more likely to impose internet shutdowns. Governments intentionally disrupted internet access to coincide with important national events such as protests and political instability, military coups, elections, examinations, conflicts, and other key events with one aim — to restrict the flow of information and control the narrative.

✦ Shutdowns during conflicts

Conflict was the leading trigger for internet shutdowns for the first time in 2023, with warring parties imposing **74** shutdowns in **nine** countries (Azerbaijan, Ethiopia, India, Libya, Myanmar, Pakistan, Palestine, Sudan, and Ukraine). This far exceeds the **36** shutdowns in **nine** countries recorded in 2022.¹⁹ Even still, evidence suggests that both for prior years and in 2023, these cases are severely underreported given the challenges people are facing to document their experience while also fending for their lives.²⁰

Authorities imposing internet shutdowns in active conflict zones have leveraged an increasingly diverse array of tactics, making prevention and circumvention challenging and introducing far-

reaching consequences for impacted communities long after the fighting recedes. Both the Myanmar junta and the Israeli military have systematically paired the deployment of targeted internet shutdowns with air strikes and other military activity, often targeting civilian populations.²¹ Cutting off access to communications channels removes any hope for civilians under attack of accessing information about possible evacuation routes or connecting with loved ones to see if they survived.²² Similarly, Israeli and Russian forces have deliberately targeted civilian telecommunications infrastructure during active conflict as a collective punishment or retaliatory action in Palestine and Ukraine, respectively,²³ while warring parties in both Sudan and Ukraine have gone head to head battling over physical control of telecommunications infrastructure.²⁴ Beyond direct kinetic attacks, we've also seen perpetrators leveraging fuel embargos to cut off energy supply to telecommunications services and cyberattacks aimed at disrupting networks in areas held by opposing forces.²⁵

Only underscoring the importance of staying connected during times of conflict, perpetrators of shutdowns in conflict zones have gotten more sophisticated at using circumvention tactics to keep themselves or bordering civilian populations online. The Israeli authorities developed a comprehensive strategy to maintain connectivity for settlements bordering Gaza, while keeping the occupied territory under siege in the dark.²⁶ From Ukraine to Sudan and beyond, low-earth-orbit satellite internet systems have emerged as an increasingly vital — and increasingly politicized — mechanism for circumvention and determining who is allowed access

¹⁹ See *supra* note 1. Access Now (2023).

²⁰ See, e.g., the section below on Myanmar for more information regarding the likelihood of underreporting.

²¹ See The Intercept (2023). *Israel Warns Palestinians on Facebook - but Bombings Decimated Gaza Internet Access*. <https://theintercept.com/2023/10/12/israel-gaza-internet-access/>; EngageMedia (2024). *Myanmar Digital Coup Quarterly: November 2023-January 2024*. <https://engagemedia.org/2024/myanmar-digital-coup-quarterly-november-2023-january-2024/>

²² See Access Now (2024). *#KeepItOn in times of war: Sudan's communication shutdown must be reversed urgently*. <https://www.accessnow.org/press-release/keepiton-sudan-shutdown/>

²³ See AlfaNet (@AlfaNetIT). Facebook post. 11:31 pm. October 7, 2023. <https://www.facebook.com/AlfaNetIT/posts/pfbid02GSsU8PdChNktczmp4RT1k3RZZdY8vN9YZXf4UUVx2F7CutcWKzu4TcuYggZ2e67sl/>; Reuters (2023). *Russian missiles pound Ukraine's energy system, force power outages*. <https://www.reuters.com/world/europe/russian-forces-strike-ukraine-air-raid-sirens-wail-across-country-2023-02-10/>; see also ICRC (n.d.). *The Principle of Distinction between Civilian Objects and Military Objectives*. <https://ihl-databases.icrc.org/en/customary-ihl/v1/rule7>; Médecins sans frontières (n.d.). *The Practical Guide to Humanitarian Law: Reprisals*. <https://guide-humanitarian-law.org/content/article/3/reprisals/>

²⁴ See, e.g., Digital Rights Lab - Sudan (@DRLab_Sudan). X post. 1:28 pm. February 24, 2024. https://x.com/DRLab_Sudan/status/1754134933772128326/; Cloudflare (2022). *Tracking shifts in Internet connectivity in Kherson, Ukraine*. <https://blog.cloudflare.com/tracking-shifts-in-internet-connectivity-in-kherson-ukraine/>

²⁵ See, e.g., Access Now (2023). *Depleting fuel and infrastructure damage: Gaza's internet lifeline must be saved*. <https://www.accessnow.org/press-release/internet-lifeline-must-be-saved-in-gaza/>; The Record (2023). *Ukraine's largest telecom operator shut down after cyberattack*. <https://therecord.media/kyivstar-cyberattack-telecom-shutdown-ukraine/>

²⁶ Israel Ministry of Communications (2023). *Summary of the activities of the Ministry of Communications - ten days into the war*. <https://www.gov.il/en/departments/news/17102023/>

when communications systems are disrupted.²⁷ We are monitoring developments around these trends closely as they continue to evolve in 2024.

The devastating impact of internet shutdowns in times of conflict cannot be overstated, exacerbating people's desperation, fear, and panic. Conflict-related shutdowns have put people's lives in real danger or even resulted in loss of life,²⁸ impeded delivery of humanitarian aid,²⁹ and blocked access to emergency healthcare services.³⁰ They have also made it extremely difficult for journalists and human rights defenders to document war crimes and other atrocities.³¹

Conflict-related shutdowns carry long-term impacts, particularly where infrastructure has been degraded or destroyed. In Ethiopia's Tigray region, after two years of complete blackouts amid devastating conflict, a negotiated peace beginning in November 2022 included agreements to restore internet access to the region.³² However, as of December 31, 2023, **1,153 days** since the start of the shutdown in Tigray, connectivity was still well below pre-war levels. Other examples from past conflicts include the ongoing blocking of TikTok in India following military clashes with China in June 2020³³ and the ongoing shutdown in Panjgur, Pakistan following clashes between regional troops and the Pakistani military in early 2022.³⁴

In situations of conflict and violence, internet shutdowns targeting civilian populations and infrastructure are a violation of international human rights and international humanitarian law, which protect non-military objects especially when needed for the provision of humanitarian assistance.³⁵ Likewise, documented internet shutdowns are an important piece of evidence in pursuing accountability for crimes against humanity and other atrocities when armed actors disconnect whole communities to enable, facilitate, or cover up their abuses.³⁶ It remains essential that states neither neglect nor derogate from their obligations under international human rights, humanitarian, and criminal law. Instead, all stakeholders should work together to strengthen international norms and accountability mechanisms around weaponization of internet shutdowns during conflict and see perpetrators brought to justice.³⁷

Shutdowns during protests and instability

In 2019, we saw the largest wave of global protests in a generation.³⁸ Authorities responded by imposing **65** protest-related internet shutdowns in 30 countries, the highest annual number of such shutdowns on record. With the outbreak of the COVID-19 pandemic in 2020, both protests and the disruptions used to counter them dropped off

²⁷ See, e.g., CNN (2024). *Ukraine relies on Starlink for its drone war. Russia appears to be bypassing sanctions to use the devices too.* <https://edition.cnn.com/2024/03/25/europe/ukraine-starlink-drones-russia-intl-cmd/index.html/>

²⁸ See, e.g., Access Now (2022). *Stranded, suffocated, and in pain: 15 stories from Tigray's internet siege.* <https://www.accessnow.org/15-stories-from-tigrays-internet-siege/>

²⁹ See, e.g., Chicago Sun Times (2023). *Internet, phone networks collapse in Gaza, threatening to worsen humanitarian crisis.* <https://chicago.suntimes.com/2023/11/16/23964979/internet-phone-networks-collapse-in-gaza-threatening-to-worsen-humanitarian-crisis/>

³⁰ See, e.g., Internews (2021). *Internet Shutdowns and the Healthcare System in Zimbabwe - Information Saves Lives.* <https://internews.org/blog/internet-shutdowns-and-the-healthcare-system-in-zimbabwe/>

³¹ Rest of World (2022). *Internet blackouts are hiding an ongoing human rights catastrophe.* <https://restofworld.org/2022/blackouts-myanmar-atrocities/>

³² Access Now (2022). *After years in the dark, Tigray is slowly coming back online.* <https://www.accessnow.org/tigray-shutdown-slowly-coming-back-online/>

³³ New York Times (2020). *India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat.* <https://www.nytimes.com/2020/06/29/world/asia/tik-tok-banned-india-china.html>

³⁴ The Express Tribune (2023). *Panjgur without internet.* <https://tribune.com.pk/letter/2254764/panjgur-without-internet/>

³⁵ ICRC (1999). *The denial of humanitarian assistance as a crime under international law.* <https://www.icrc.org/en/doc/resources/documents/article/other/57jq32.htm/>

³⁶ Access Now (2024). *Legal explainer: Internet and telecommunications shutdowns in the assessment of international crimes.* <https://www.accessnow.org/legal-explainer-internet-telecommunications-shutdowns-international-crimes/>

³⁷ See Access Now (2023). *Content and platform governance in times of crisis: applying international humanitarian, criminal, and human rights law.* <https://www.accessnow.org/cogo-in-times-of-crisis>

³⁸ The New Yorker (2019). *The Story of 2019: Protests in Every Corner of the Globe.* <https://www.newyorker.com/news/our-columnists/the-story-of-2019-protests-in-every-corner-of-the-globe/>

significantly. Since then, however, movements of all kinds have steadily rekindled around the globe, and internet shutdowns have remained a go-to tactic for authorities aiming to crack down on dissent.

In 2023, this ongoing wave of anti-government protests met with the eruption of new protests in seven countries that had not seen major protests in the previous five years.³⁹ In fact, researchers documented the emergence of new protests in at least 83 countries.⁴⁰ In this context, governments shut down the internet to crack down on dissent **63 times in 15 countries**: Bangladesh, Cuba, Ethiopia, Gabon, Guinea, India, Iran, Jordan, Libya, Mauritania, Mozambique, Pakistan, Senegal, Somaliland, and Suriname. This matches the pace of such shutdowns in 2022, when we also saw **63** disruptions during protests.

Shutdowns during elections

In 2023, we documented **five** election-related shutdowns, leveling off at the same number as 2022 following a steady downward trend since the peak of **12** election-related shutdowns in both 2018 and 2019.

Through Access Now's annual #KeepItOn Election Watch campaign — and with support, collaboration, and guidance from #KeepItOn members and partners — we successfully mobilized and advocated against election-related shutdowns in 18 countries that were past offenders or otherwise high risk.⁴¹ Out of these 18 countries, we documented only one election-related shutdown in Gabon, where incumbent authorities cut off internet access, expelled foreign press, and disallowed participation from independent election observers.⁴² In addition, Mozambique imposed its first internet shutdown on record in response to

protests over the outcome of elections,⁴³ Venezuela disrupted access in the capital Caracas amid a highly irregular primary election,⁴⁴ and state-level authorities in India issued blocking orders for Kiphire district while responding to post-poll violence.⁴⁵ Uganda also maintained its ongoing Facebook platform block for all of 2023, a shutdown that was first implemented during the 2021 election cycle.⁴⁶

We have also seen increased commitments from governments to keep internet access open and secure throughout the electoral period. As we note above, in 2023, past offenders the Democratic Republic of Congo (DRC), Nigeria, and Sierra Leone all pledged to #KeepItOn during their elections, setting an important example of reform in the region.

These proactive commitments and overall reduction in the number of election-related shutdowns are a reflection of years of tireless advocacy from #KeepItOn coalition members and like-minded supporters. We have seen a growing international consensus against the use of internet shutdowns in the context of elections, with recognition that they fundamentally inhibit the legitimacy of any democratic process. This includes the aforementioned Freedom Online Coalition (FOC) statement on election shutdowns in 2023,⁴⁷ and the more recent resolution from the African Commission on Human and Peoples' Rights (ACHPR).⁴⁸

These trends are also closely linked to the global elections landscape and the context in which elections are taking place. With an unprecedented number of elections happening at every level around the globe in 2024, this year will be an important measure of progress toward putting an end to election-related shutdowns for good.

³⁹ See *supra* note 6.

⁴⁰ Carnegie Endowment For International Peace (2024). *Global Protest Tracker*. <https://carnegieendowment.org/publications/interactive/protest-tracker/>

⁴¹ See *supra* note 1. Access Now (2023).

⁴² France 24 (2023). *Gabon blocks internet access, imposes curfew amid election voting delays*. <https://www.france24.com/en/africa/20230826-gabon-blocks-internet-access-imposes-curfew-amid-election-voting-delays/>

⁴³ allAfrica (2023). *Mozambique: Internet Shutdown as Polls Close*. <https://allafrica.com/stories/202310120129.html>

⁴⁴ Crisis24 (2023). *Venezuela: Internet service disruptions ongoing in several locations in Caracas late Oct. 22 amid primary voting*. <https://crisis24.garda.com/alerts/2023/10/venezuela-internet-service-disruptions-ongoing-in-several-locations-in-caracas-late-oct-22-amid-primary-voting/>

⁴⁵ Nagaland Post (2023). *Post-poll violence continues across Nagaland*. <https://nagalandpost.com/index.php/2023/03/01/post-poll-violence-continues-across-nagaland/>

⁴⁶ Monitor (2022). *Facebook to remain shut as govt talks with tech giant stall*. <https://www.monitor.co.ug/uganda/news/national/facebook-to-remain-shut-as-govt-talks-with-tech-giant-stall-3912172/>

⁴⁷ *Supra* note 15.

⁴⁸ African Commission on Human and Peoples' Rights (2024). *Resolution on Internet Shutdowns and Elections in Africa - ACHPR. Res.580 (LXXVIII)2024*. <https://achpr.au.int/index.php/en/adopted-resolutions/580-internet-shutdowns-elections-africa-achprres580-lxxviii/>

Shutdowns during exams

In 2023, we recorded **12** exam-related shutdowns in Algeria, India, Iran, Iraq, Kenya, and Syria. This follows a relatively consistent trend of recent years: there were **eight** such shutdowns in 2022, **11** in 2021, and **eight** in 2020. While most countries that imposed exam-related shutdowns in 2023 are long-standing annual offenders, the government of Kenya did so for the first time by restricting access to Telegram.⁴⁹ Iran also blocked internet access during national exams — the first recorded exam-related shutdown in Iran in STOP, but with reports indicating similar localized disruptions have taken place since at least 2021.⁵⁰

The implementation of shutdowns has proven futile over and over again in curbing exam cheating, and the harms to impacted communities and businesses are clearly documented.⁵¹ Yet authorities persist. We welcome and encourage efforts to move away from this practice, as we saw from the Ministry of Communications in Iraq when they challenged the Ministry of Education's request to implement blocks.⁵²

Shutdowns during natural disasters

In an alarming new development, we saw at least **four** internet shutdowns in **four** countries (Iraq, Libya, Myanmar, Türkiye) coincide with natural disasters in 2023. Rising global surface temperatures and shifts in weather patterns due to the climate crisis are

fueling natural disasters including typhoons, floods, wildfires, and cyclones across the world. In 2023, the world was hit hard by a whopping 240 calamities — a tragic record-breaking number of natural disasters — which caused irreparable damage, including deaths and displacement of tens of thousands of people.⁵³ The impact of the climate crisis coupled with growing political and economic instability is becoming global in scope and unprecedented in scale.⁵⁴

In both Myanmar and Iraq, emergencies hit regions already experiencing internet disruptions for other reasons. The ongoing digital crackdown by the military junta in Myanmar exacerbated the effects of Cyclone Mocha, which hit western Myanmar in May 2023.⁵⁵ People already deliberately disconnected, with a near-total lack of connectivity, could not access proper warning of storms, evacuation routes, or post-disaster relief assistance — which was even further restricted by the junta's refusal to allow humanitarian aid workers to enter the country.⁵⁶ In Iraq, a massive earthquake in February 2023 impacting several countries in the region struck during what were otherwise "routine" social media blocks for national exams, which cut people off from essential communications channels for at least eight hours every day.⁵⁷ The areas impacted by the earthquake, including Syria, western and northern Iraq, and Türkiye, are home to large populations of refugees and internally displaced persons, making the lack of access to communications channels both locally and across borders even more dire.⁵⁸

In Türkiye and Libya, authorities imposed internet shutdowns in the direct aftermath of natural disasters

⁴⁹ OONI Explorer (2023). *Kenya blocked Telegram during the KCSE 2023 exams*. <https://explorer.ooni.org/findings/228466228201/>

⁵⁰ Filterwatch (2024). *Old Policies, New Laws: Legal Developments Around Iran's Internet Take Centre Stage*. <https://filterwatch/en/2023/06/23/old-policies-new-laws-legal-developments-around-irans-internet-take-centre-stage/>; Digiato (2021). *Jahormi: One of the reasons for the internet disruption in the past days was to prevent the sale of exam questions*. <https://digiato.com/article/2021/07/03/%D8%A7%D8%AE%D8%AA%D9%84%D8%A7%D9%84-%D8%A7%DB%8C%D9%86%D8%AA%D8%B1%D9%86%D8%AA-%D8%A8%D9%87-%D8%AE%D8%A7%D8%B7%D8%B1-%DA%A9%D9%86%DA%A9%D9%88%D8%B1/>

⁵¹ See Access Now (2023). *Tell MENA authorities: #NoExamShutdown*. <https://www.accessnow.org/campaign/no-exam-shutdown/>

⁵² *Supra* note 17.

⁵³ Eos Data Analytics (2024). *Natural Disasters 2023: A Year of Tragic Record-Breaking*. <https://eos.com/blog/natural-disasters-2023/>

⁵⁴ United Nations (n.d.). *Global Issues: Climate Change*. <https://www.un.org/en/global-issues/climate-change/>

⁵⁵ Reuters (2023). *At least three killed as powerful storm batters Myanmar*. <https://www.reuters.com/business/environment/powerful-storm-snaps-communications-network-myanmars-rakhine-2023-05-15/>

⁵⁶ Human Rights Watch (2023). *Myanmar: Junta Blocks Lifesaving Cyclone Aid*. <https://www.hrw.org/news/2023/06/20/myanmar-junta-blocks-lifesaving-cyclone-aid/>

⁵⁷ Access Now (2024). *People need the internet during emergencies: #KeepItOn in Iraq*. <https://www.accessnow.org/press-release/internet-keepiton-iraq/>

⁵⁸ Reuters (2023). *We fled war to die in an earthquake, says Iraqi woman mourning family in Turkey*. <https://www.reuters.com/world/middle-east/we-fled-war-die-an-earthquake-says-iraqi-woman-mourning-family-turkey-2023-02-08/>

to suppress protests and online criticism of the government's handling of the crisis.⁵⁹ Access to information and communication channels is a critical lifeline that needs to be protected in times of crisis — never deliberately severed.

III. New and continuing trends in 2023

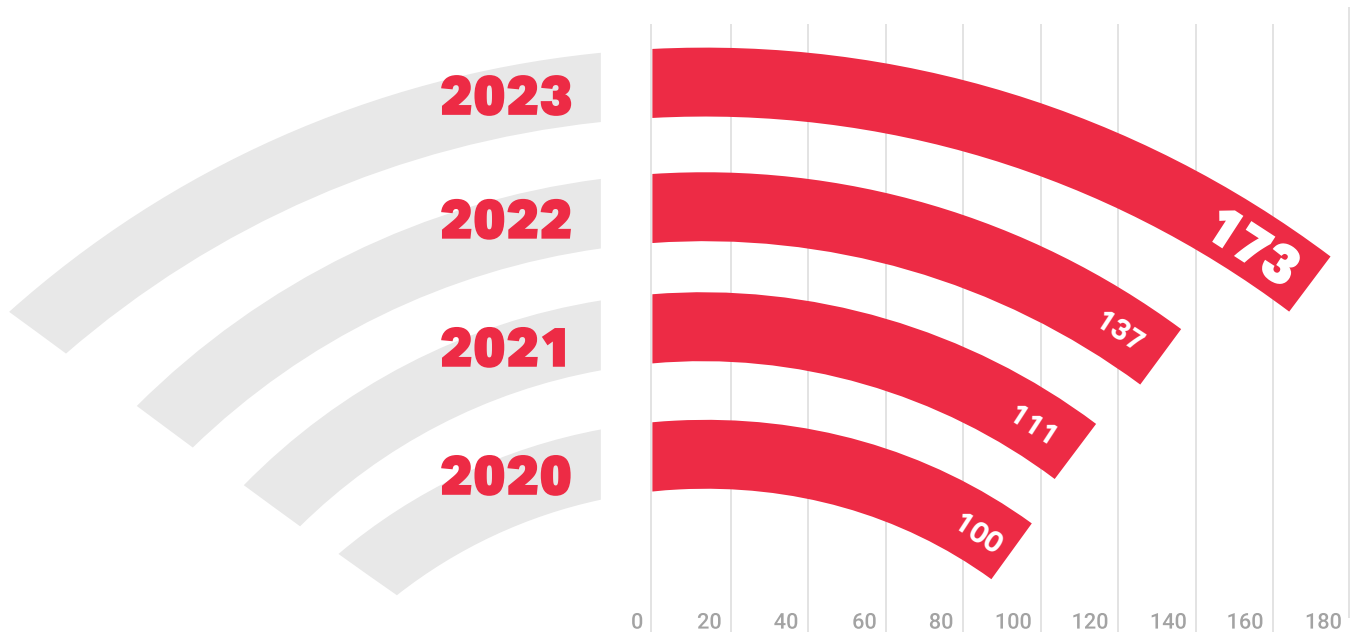
Shutdowns continue to shroud grave human rights abuses and violence

There were **173** shutdowns that occurred alongside violence in 2023, compared to **137** in 2022, **111** in 2021, and **100** in 2020. While the disturbing increase of shutdowns associated with violence is connected in part to the increase in disruptions during armed conflict, reports of violence during shutdown periods are also rampant during protests, elections, and political instability. In India alone, authorities ordered

65 shutdowns in 2023 specifically attempting to address communal violence. Overall, despite claims from authorities that they are shutting down the internet to curb violence during moments of tension, evidence shows that shutdowns are ineffective at doing so and likely have the opposite effect.⁶⁰

Far from just a misguided reactionary measure, shutdowns also impede accountability where attackers disrupt access to cover up their own horrific offenses, including killings, torture, and inhumane treatment of vulnerable people and communities.⁶¹

Shutdowns that occurred alongside violence ▾



⁵⁹ Access Now (2023). *In the aftermath of devastating earthquake, authorities in Turkey must #KeepItOn*. <https://www.accessnow.org/press-release/earthquake-turkey-keepiton/>; Access Now (2023). *Libya floods: People need reliable internet now*. <https://www.accessnow.org/press-release/libya-floods-internet/>

⁶⁰ Jan Rydzak (2019). *Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413/; see also Anita R. Gohdes (2023). *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence*, Oxford University Press. In Ch. 5, Gohdes finds that, "All else equal, Internet shutdowns and the days immediately before and after the shutdown are likely to be accompanied by a significant increase in violent state repression."

⁶¹ See Global Partners Digital (2023). *Evading Accountability Through Internet Shutdowns: Trends in Africa and the Middle East*. <https://www.gp-digital.org/publication/evading-accountability-through-internet-shutdowns-trends-in-africa-and-the-middle-east/>

In 2023, **27** of the **63** protest-related shutdowns occurred alongside violence, including cases where authorities used shutdowns in attempts to conceal brutality by security forces.⁶² We documented the targeting of civilians and civilian infrastructure through air strikes, brutality against protesters, or other atrocities and war crimes during **51** shutdowns in **11** countries around the world (Azerbaijan, Ethiopia, Iran, Jordan, Mauritania, Myanmar, Palestine, Russia, Somaliland, Sudan, Ukraine).

Internet shutdowns are always an attack on people's human rights. But when they come without warning during moments of national tension or as part of a deliberate military strategy, they are especially harmful, cutting people off from communications lifelines when they need them most. Out of all our recorded events in 2023, in **93%** of cases, the public received no advance notice of an impending shutdown, deepening fear and uncertainty and putting more people in grave danger.

Perpetrators using shutdowns to cover up violence and serious human rights abuses was especially prevalent in conflict zones. Under a near-total communications blackout in the Amhara region of Ethiopia, security forces stoked terror and mass displacement through attacks on civilians, ranging from rape, murder of children and families, and destruction of civilian property, to indiscriminate bombing across the region.⁶³ In the Gaza Strip, the Israel military used a combination of direct attacks on civilian telecommunications infrastructure, restrictions on access to electricity, and technical disruptions to shut down the internet⁶⁴ in the midst of heavy bombardments that indiscriminately killed tens

of thousands of civilians.⁶⁵ In Sudan, the Rapid Support Forces (RSF) and the Sudanese Armed Forces (SAF), who have been fighting since April 2023, have also wielded shutdowns as a weapon of control alongside rampant targeting of civilians, looting, sexual violence, and one of the most severe displacement crises in the world.⁶⁶ In Myanmar, shutdowns and phone line disconnects preceded air strikes on residential areas, sometimes implemented with jammers on military aircraft, and usually ordered by local township officials.⁶⁷ The Russian military continued to target energy infrastructure in Ukraine, which also disrupted internet services, as they bombed residential areas.⁶⁸ Across many contexts, perpetrators used a variety of tactics to shut down the internet, including blockading of fuel, cyberattacks, and systematic targeting of specific internet service providers (ISPs) of occupied regions, seeking either to inflict harm on the civilian population directly or to conceal atrocities. Regardless of how they are implemented, repeated internet shutdowns in times of conflict exact a human toll that is immense and often incalculable.

Authorities must refrain from normalizing platform blocks

Governments continued to use communication platform blocks heavily in 2023, imposing or maintaining **53** blocks across **25** countries, up from **39** blocks across **29** countries in 2022. We recorded more service-based blocking orders in India than any other country, with an increase from **two** platform blocks in 2022 to **14** in 2023 — a resurgence of this tactic after an initial wave of app blocking in 2020.⁶⁹ Setting India aside, platform blocks were distributed

⁶² See, e.g., Crisis24 (2023). *Mauritania: Protests and clashes possible in areas across country through at least early June following recent death of individual in police custody*. <https://crisis24.garda.com/alerts/2023/05/mauritania-protests-and-clashes-possible-in-areas-across-country-through-at-least-early-june-following-recent-death-of-individual-in-police-custody/>; Internet Society Pulse (2023). *Internet shutdowns: Mauritania*. <https://pulse.internetsociety.org/shutdowns/mauritania-blocks-mobile-internet-during-protests/>

⁶³ Addis Standard (2023). *News: Rights commission reveals disturbing sexual violence in Amhara conflict, more than 200 cases of rape exposed*. <https://addisstandard.com/news-rights-commission-reveals-disturbing-sexual-violence-in-amhara-conflict-more-than-200-cases-of-rape-exposed/>

⁶⁴ Access Now (2023). *Palestine unplugged: how Israel disrupts Gaza's internet*. <https://www.accessnow.org/publication/palestine-unplugged/>

⁶⁵ Al Jazeera (2024). *Gaza death toll surpasses 30,000 with no let-up in Israeli bombardment*. <https://www.aljazeera.com/news/2024/2/29/gaza-death-toll-surpasses-30000-with-no-let-up-in-israeli-bombardment/>

⁶⁶ OHCHR (2024). *Sudan: Horrific violations and abuses as fighting spreads - report*. <https://www.ohchr.org/en/press-releases/2024/02/sudan-horrific-violations-and-abuses-fighting-spreads-report>

⁶⁷ Myanmar Now (2023). *Myanmar's military increasing use of signal jammers to foil attacks by anti-regime guerrillas*. <https://myanmar-now.org/en/news/myanmars-military-increasing-use-of-signal-jammers-to-foil-attacks-by-anti-regime-guerrillas/>

⁶⁸ *Supra* note 23. Reuters (2023).

⁶⁹ TechCrunch (2020). *India bans 43 more Chinese apps over cybersecurity concerns*. <https://techcrunch.com/2020/11/24/india-bans-another-43-chinese-apps/>; The Times of India (2023). *Government bans 14 messaging apps used by J&K terrorists*. <https://timesofindia.indiatimes.com/india/government-bans-14-messaging-apps-used-by-jk-terrorists/articleshow/99917838.cms/>

similarly across platforms from 2022 to 2023, with the largest increase impacting Telegram (**seven** to **10**).

Three out of **four** countries implementing shutdowns for the first time in 2023 blocked platforms, including Kenya (Telegram), Nepal (TikTok), and Suriname (Meta services Facebook, WhatsApp, and Instagram). We also recorded platform blocks in the United Arab Emirates (UAE), Lebanon, and Qatar that had been ongoing since 2016, 2019, and 2020, respectively — marking the first time we have included each country as a shutdown perpetrator in our records.

The persistent use of platform blocks indicates authorities may perceive them as “more acceptable” or “less harmful,” but disruption of platforms often disproportionately impacts targeted and marginalized communities or people who rely on them as their only viable mode of access to information and communication with loved ones, colleagues, customers, news sources, and service providers. In Azerbaijan, Ethiopia, Iraq, Pakistan, and Senegal, authorities combined the use of social media blocks with mobile network shutdowns during protests, school exams, and conflict to expand the scope of their information control. When they cut mobile access, block platforms, or both, authorities make it clear that they intend to silence and repress a wide swath of the population, often leaving broadband services available for government services, businesses, and wealthy elites.

The widespread blocking of Grindr — the world’s largest social networking app for gay, bisexual, transgender, and queer people — is an especially telling indicator that authorities are using blocks to deliberately marginalize specific groups of people. Jordan and Tanzania issued new blocks of Grindr in 2023 on top of ongoing blocking in another 10 countries across the MENA region (Iran, Lebanon,

Oman, Qatar, Saudi Arabia, Türkiye, UAE) and APAC region (China, Indonesia, Pakistan).⁷⁰ This clear repression of LGBTQ+ spaces reflects a global wave of intolerance and discrimination that is dehumanizing and isolating people from vital support networks.⁷¹ LGBTQ+ people already face a wide range of serious threats to their fundamental rights and physical safety, and censorship and shutdowns are only exacerbating the harm and putting people at further risk.

Even democracies that often position themselves as champions of free expression waded into dangerous waters in 2023 as policymakers put forward misguided arguments for blocking or banning certain social media platforms.⁷² This not only threatens free expression and other human rights in these countries, it sends a dangerous message of tacit endorsement to governments around the world looking to justify blocking platforms that millions rely on. Passage of legislation in India, Jordan, and Russia making it easier for authorities to impose shutdowns and prevent people from using circumvention tools like virtual private networks (VPNs) to access blocked platforms only reinforces this harmful trend.⁷³

In the U.S., policymakers debated issues around TikTok ranging from general data privacy concerns, to the potential threats China poses to U.S. national security, to the platform’s purported algorithmic manipulation of young audiences to adopt a more pro-Palestinian stance.⁷⁴ On April 24, 2024, U.S. President Joe Biden signed a bill into law that threatens to block access to TikTok nationally if the company does not divest to a U.S.-based owner — setting the stage for a string of legal challenges and, if ultimately implemented, the country’s first recorded shutdown.⁷⁵ Kenyan parliamentarians petitioned to ban the platform to protect religious and moral values.⁷⁶ And as authorities in France grappled with mass protests following

⁷⁰ OONI (2023). *Grindr blocked in Jordan: Shrinking LGBTQ spaces*. <https://ooni.org/post/2023-jordan-blocks-grindr#conclusion>

⁷¹ Access Now and Electronic Frontier Foundation (2024). *United Nations Independent Expert on Protection against Violence and Discrimination based on Sexual Orientation and Gender Identity Written Submission: Anti-LGBTQ+ Repression*. <https://www.eff.org/document/access-now-eff-written-submission-un-ie-sogie-jan-2024/>

⁷² See Euronews Next (2024). *Which countries have banned TikTok and why?* <https://www.euronews.com/next/2024/03/14/which-countries-have-banned-tiktok-cybersecurity-data-privacy-espionage-fears>

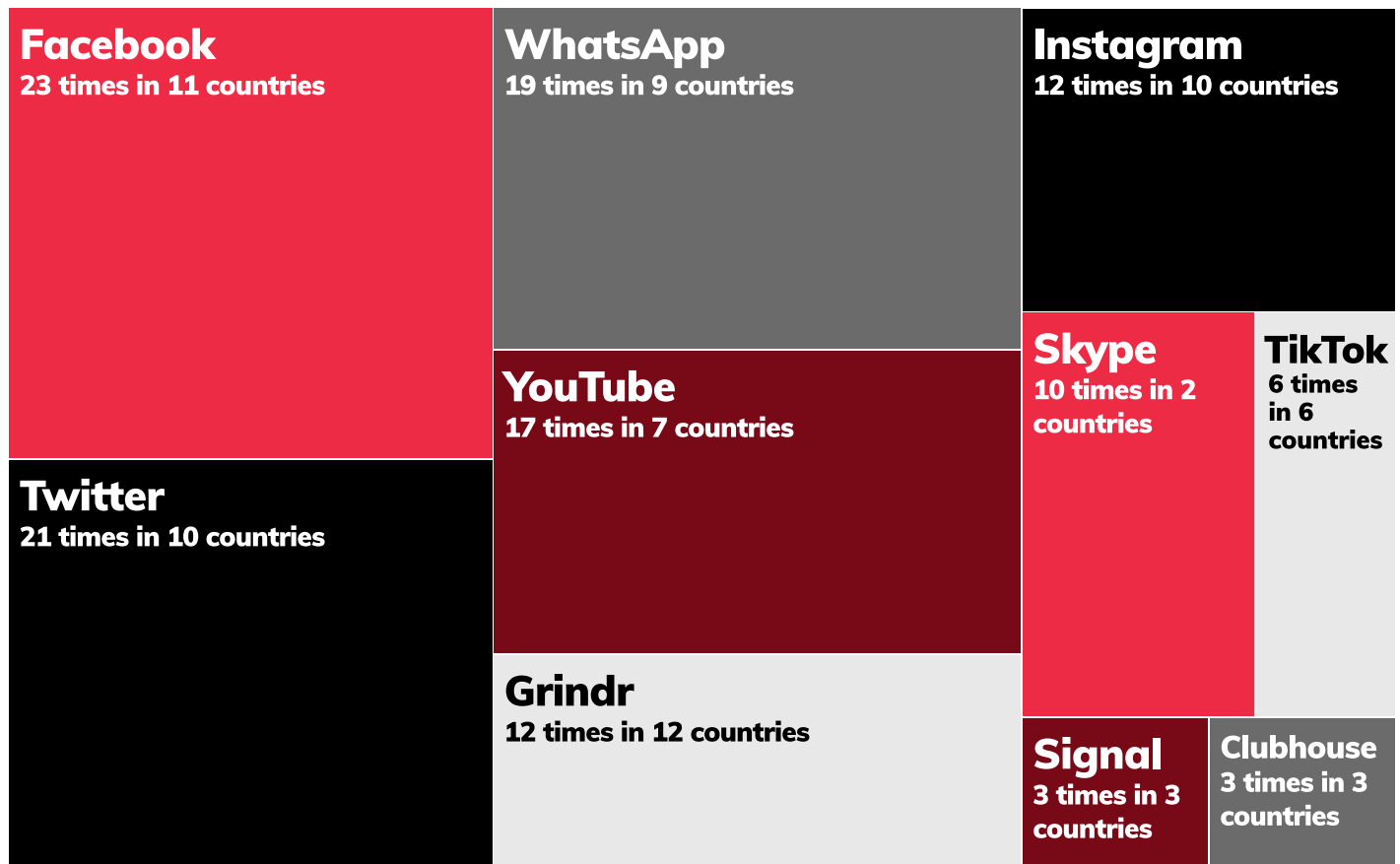
⁷³ Access Now (2023). *Indian government must withdraw the Telecommunications Bill, 2023, to protect fundamental human rights*. <https://www.accessnow.org/press-release/india-must-withdraw-the-telecommunications-bill-2023/>; Access Now (2023). *Jordan’s new proposed cybercrimes law will strongly undermine digital rights*. <https://www.accessnow.org/press-release/jordans-cybercrimes-law/>; The Moscow Times (2024). *Russia Will Block VPN Services in March, Says Safe Internet League Chief Mizulina*. <https://www.themoscowtimes.com/2024/02/05/russia-will-block-vpn-services-in-march-says-safe-internet-league-chief-mizulina-a83978>

⁷⁴ Al Jazeera (2024). *Dissecting the ‘TikTok problem.’* <https://www.aljazeera.com/program/the-listening-post/2024/3/23/dissecting-the-tiktok-problem>

⁷⁵ Axios (2024). *What happens now that Biden has signed the TikTok bill*. <https://www.axios.com/2024/04/24/joe-biden-tik-tok-ban-bill>

⁷⁶ Access Now (2023). *Kenyan parliament must reject petition to ban TikTok*. <https://www.accessnow.org/press-release/tiktok-ban-petition-kenya/>

Platform blocking in 2023 ▾



the killing of teenager Nahel Merzouk in June 2023, French President Emmanuel Macron spoke for the first time about the possibility that France would block social media platforms if riots got out of control.⁷⁷ Responding to Macron's remarks, the European Commissioner for Internal Market, Thierry Breton, also suggested that arbitrarily blocking online platforms could be justified and enforced under the EU's Digital Services Act (DSA).⁷⁸

Although the authorities did not follow through with a social media blackout in France, these remarks were alarming and raised serious concerns. Together with

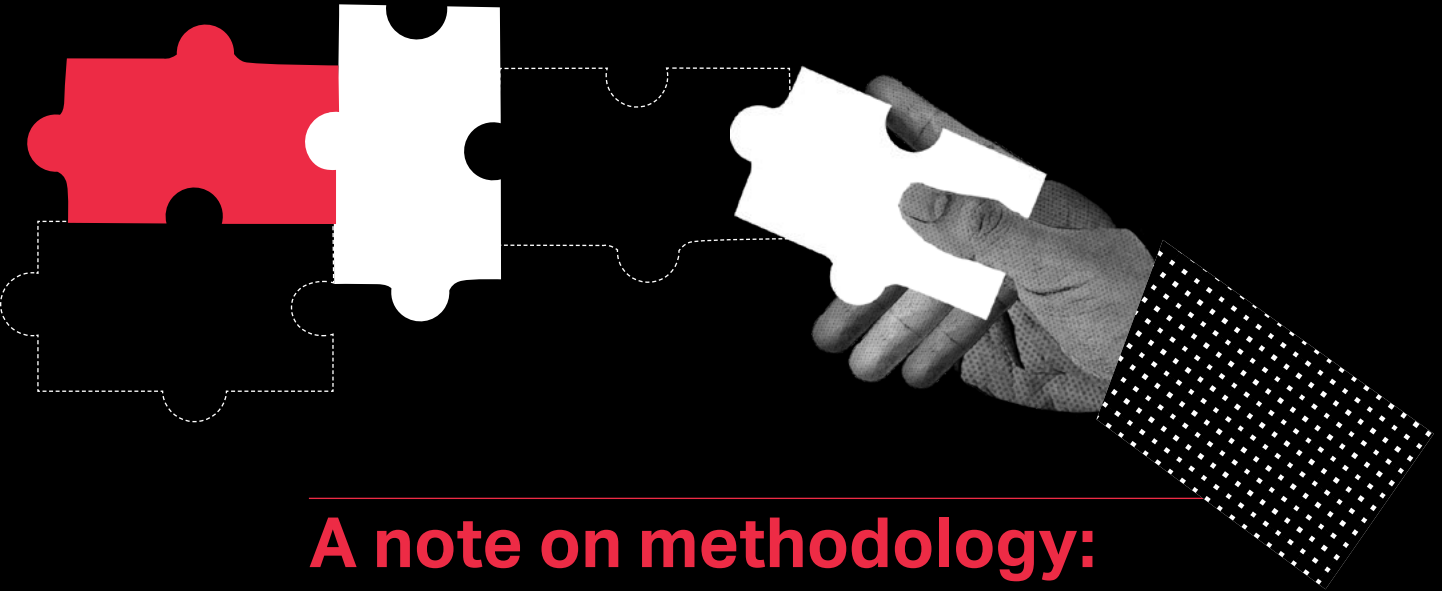
65 other organizations, Access Now sent an open letter to Commissioner Breton urging him to clarify his remarks and affirm that arbitrary internet shutdowns and social media blocking are unlawful under the DSA.⁷⁹ Commissioner Breton responded swiftly, confirming that "[the] DSA is here to protect free speech against arbitrary decisions, and at the same time protect our citizens and democracies," and it would not be used to normalize the use of internet shutdowns.⁸⁰

⁷⁷ The Washington Post (2023). *Macron says social media could be blocked during riots, sparking furor.* <https://www.washingtonpost.com/world/2023/07/06/france-macron-social-media-block-riots/>

⁷⁸ France Info (@franceinfo). X post. 7:04 am. July 10, 2023. <https://x.com/franceinfo/status/1678299190030487553/>

⁷⁹ Access Now (2023). *DSA is not a censorship tool: Commissioner Breton must clarify blocking statement.* <https://www.accessnow.org/press-release/dsa-internet-blocking/>

⁸⁰ *Supra* note 18.



A note on methodology: why platform blocks are under-counted

Platform blocks have historically been under reported, and our team has engaged in an ongoing process of updating the Shutdown Tracker Optimization Project (STOP) dataset⁸¹ to include more of these and other longstanding but previously under-counted shutdowns. Getting an accurate picture of the full scope of platform blocks underway around the world is a challenge due to the localized nature of platform preferences, limited measurement data for platforms in countries where the user base is relatively small, discrepancies when a government does not fully or consistently implement stated policies for platform blocking, and people's regular use of VPNs and other similar tools to circumvent blocks. To correct this, Access Now is adding missing data on platform blocks, which is why countries we know to have a history of platform blocking and censorship are only now appearing on the #KeepItOn shame list — notably Qatar and the UAE.⁸² With this trend clearly on the rise, we will continue to invest in strengthening our documentation in this area and holding all perpetrators to account.

⁸¹ *Supra* note 3.

⁸² See Access Now (2020). *COVID-19: Gulf governments must unblock all VoIP technologies*. <https://www.accessnow.org/press-release/gulf-unblock-voip-covid19/>

Worst offenders are entrenched and emboldened in the use of shutdowns

In 2023, we saw longstanding worst offenders double down on their use of internet shutdowns, a display of impunity that should make these countries a top priority for advocacy and accountability measures. Whether perpetrators have repeatedly ordered more targeted shutdowns or persist in imposing longer-term, all-encompassing shutdowns, or a combination of both, the patterns of entrenchment are clear.

The list of countries with at least four shutdowns recorded in a single year grew from nine in 2022 to 10 in 2023, namely Azerbaijan, Ethiopia, India, Iran, Iraq, Myanmar, Pakistan, Palestine (all imposed by Israel), Senegal, and Ukraine (six of which were imposed by Russia). **India, Iran, Myanmar, and Ukraine** made up four of the top five countries with the highest number of shutdowns in both 2022 and 2023.

These 10 countries accounted for **237** total shutdowns in 2023, keeping millions in the dark relentlessly and oftentimes unpredictably. The five countries with the highest number of shutdowns in 2023 accounted disproportionately for **211** shutdowns, or **75%** of the global total. Even when repeated shutdowns are predictable, they are punishing. Whether it is Iraqi authorities cutting off the

internet during **58** school exam periods or the Iranian province Sistan and Baluchestan imposing **28** shutdowns during Friday prayers, deliberate network disruptions are destabilizing, disproportionate, and a clear violation of human rights.

Perpetrators also continued to impose prolonged shutdowns across 2023, in most cases extending shutdowns that were in place since 2021 or 2022. There are **35** shutdowns that were carried over from 2023 into 2024, which breaks the record of **30** shutdowns that were ongoing from 2022 into 2023. Of the current ongoing shutdowns, **26** are platform blocks, while the rest are full network shutdowns in regions across Ethiopia, Myanmar, Pakistan, and Palestine. Full connectivity has still not been restored to all parts of Tigray, Ethiopia since disruptions began in November 2020, and as we have highlighted, by December 31, 2023, people in the region had endured **1,153 days** in the dark. Meanwhile, people in dozens of townships across Myanmar suffered up to **864 days** of shutdowns by the end of 2023, as the junta continued to use blackouts as a means of control. And in Panjgur, Pakistan, people have been subjected to an ongoing mobile internet shutdown that began during a military conflict in February 2022, leaving them without mobile access for **694 days** as of December 31, 2023. People in **17** countries were subjected to internet shutdowns for the full 365 days of 2023.

REPEAT OFFENDERS



While at least **57** of the **82** countries on the offenders list have had shutdowns in more than one reporting year, a group of **21** countries has shown a propensity to relentlessly reach for the kill switch again and again.

Algeria, Ethiopia, India, Indonesia, Iraq, Pakistan, Saudi Arabia, Syria, Türkiye and UAE

Bangladesh, Iran, Jordan, Lebanon, Myanmar, Sudan and Yemen

Chad, China, Russia and Uganda

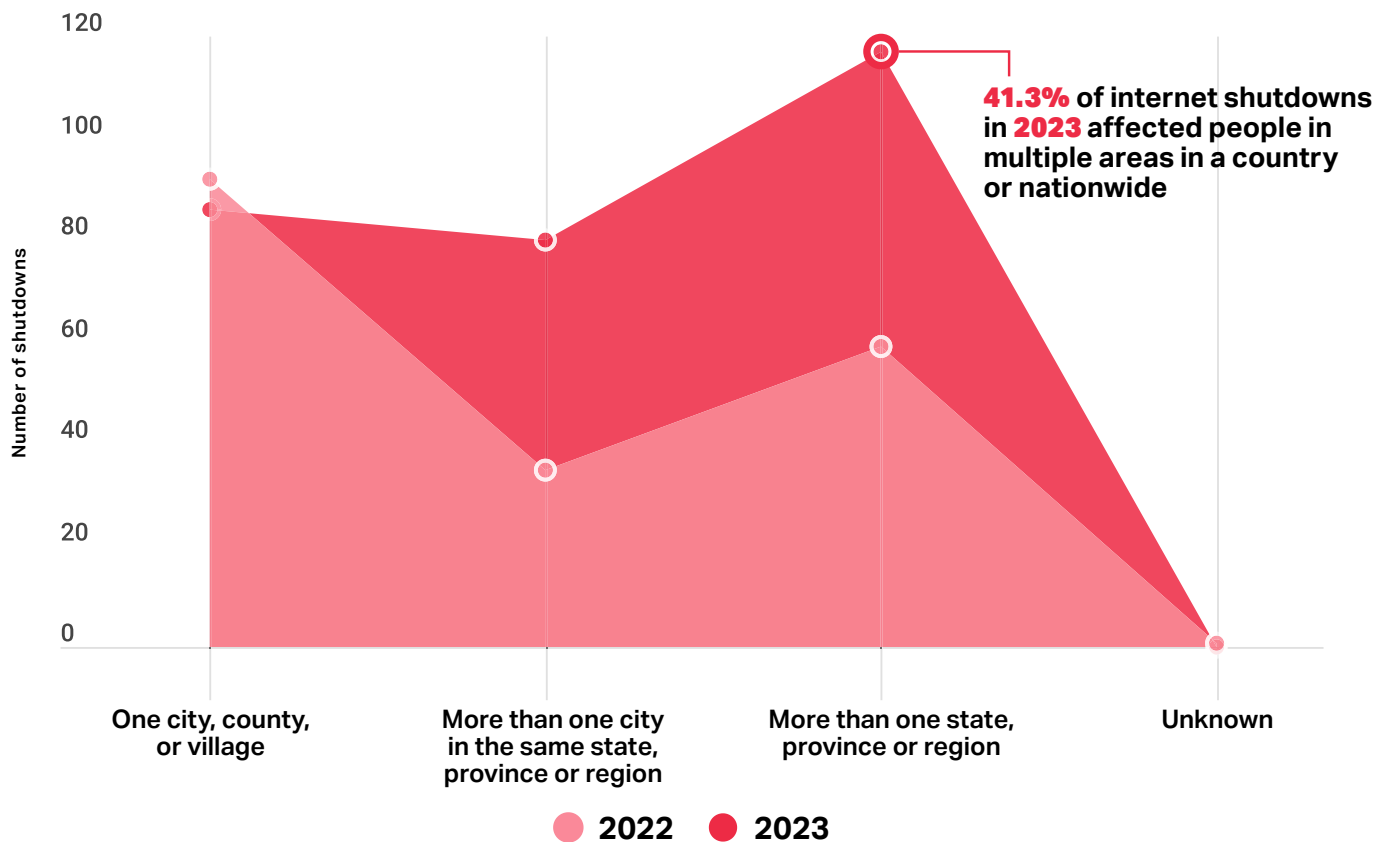
Implemented or maintained a shutdown every year since 2016

Experienced shutdowns in 5 or more consecutive years since 2016

Experienced shutdowns in 5 or more years since 2016

Algeria, Ethiopia, India, Indonesia, Iraq, Pakistan, Saudi Arabia, Syria, Türkiye, and the UAE have each implemented or maintained a shutdown every year since we began recording in 2016. Bangladesh, Iran, Jordan, Lebanon, Myanmar, Sudan, and Yemen each experienced shutdowns in five or more consecutive years. And while there may have been a gap year or two, people in Chad, China, Russia, and Uganda have also experienced shutdowns in five or more years.

The geographic scope of shutdowns is broadening



● 46.8% of shutdowns only affected one city, county, or village (94)	● 30.4% of shutdowns only affected one city, county, or village (86)
● 17.9% of shutdowns affected more than one city in the same state, province, or region (36)	● 28.3% of shutdowns affected more than one city in the same state, province, or region (80)
● 34.8% of shutdowns affected locations in more than one state, province, or region (70)	● 41.3% of shutdowns affected locations in more than one state, province, or region (117)
● 0.5% unknown (1)	

The geographic scope of shutdowns is another indicator of how authorities seek to use the digital space to marginalize and silence people. Although authorities use a variety of tactics to target specific populations, oftentimes they recklessly shut off the internet for entire regions. 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.

Myanmar was a clear exception to this trend, with **20** of 37 recorded shutdowns in 2023 imposed locally.

India significantly expanded the geographic scope of its shutdowns in 2023, imposing disruptions in more than one district in the same state, province, or region **64** times, compared to 15 in 2022. In Manipur alone, people experienced **47** shutdown orders, **44** of

which were implemented for the entire state. These shutdowns were ordered amid community clashes and widespread gender-based violence, making it even more difficult for women to report abuse.⁸³

Globally, internet shutdowns impacting entire countries or territories, or multiple regions simultaneously, are on the rise. There were **80** shutdowns at this level in 2023, compared to **70** in 2022 — the highest-ever figure recorded in a single year. Israel imposed **nine** shutdowns that impacted all of the Gaza Strip and was responsible for most of the global increase. Platform blocks also continue to be an important part of this story, since this type of shutdown is often imposed as a blanket ban across entire countries or regions. In **40** of the **53** platform blocks in 2023, bans were imposed nationwide.

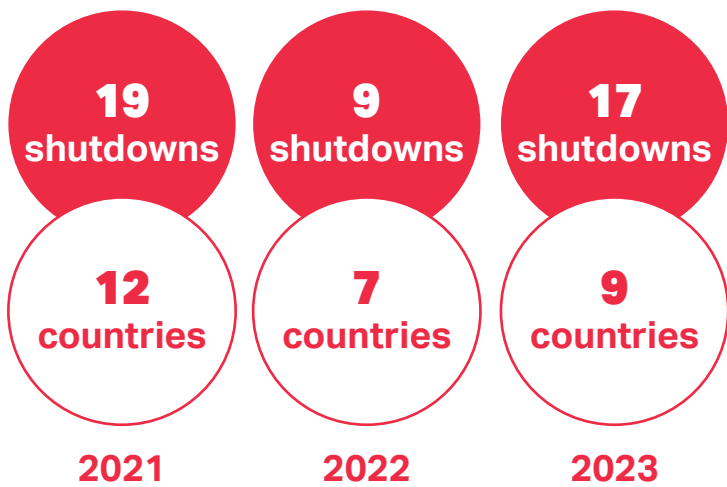
⁸³ Reuters (2023). *India internet shutdowns hurt women more, Manipur assaults show*. <https://www.reuters.com/article/india-internet-women-idUSL8N39B0AR/>

IV. Internet shutdowns by region



Africa

Regional overview in 2023



Ethiopia: 4
Senegal: 4

Guinea: 2 Tanzania: 2
Gabon: 1 Somaliland: 1 Uganda: 1

First-time offenders:

Kenya: 1
Mozambique: 1

2022 **44.5%**

2023 **58.8%**

58.8% of shutdowns related to protests

Senegal: 4 Ethiopia: 2 Gabon: 1 Guinea: 1
Mozambique: 1 Somaliland: 1

33.3%

58.8%

58.8% of shutdowns targeted platforms

Ethiopia: 2 Guinea: 2 Senegal: 2 Tanzania: 2
Kenya: 1 Uganda: 1

In 2023, we saw a resurgence of internet shutdowns in Africa with **17** incidents recorded in **nine** countries — nearly double the **nine** shutdowns in **seven** countries in 2022, which was a record low for the region following a steady downward trend from 2020. This spike in 2023 raises serious concerns about the ongoing use of shutdowns as a weapon of control in the region.

Amid an overall declining situation for human rights in Africa,⁸⁴ governments imposed shutdowns during protests, elections, national exams, and conflict. The aim: **to silence dissent and block the free flow of information.**

After a shocking **seven** countries in the region imposed their first internet shutdown in 2021, 2022 offered a reprieve, with no new countries joining the offenders list. Unfortunately, **two** new perpetrators emerged in 2023: Mozambique disrupted mobile networks while violently cracking down on protests around local elections,⁸⁵ and Kenya blocked Telegram during national exams,⁸⁶ reversing course after having rejected platform blocking during its elections the previous year.⁸⁷

Despite these setbacks, there were positive developments worth celebrating in 2023. As we've previously noted, authorities in the Democratic

⁸⁴ Freedom House (2024). *NEW REPORT: Africa Marks a Decade of Decline in Freedom, with 2023 Being Marred by Electoral Violence and Civil Conflict.* <https://freedomhouse.org/article/new-report-africa-marks-decade-decline-freedom-2023-being-marred-electoral-violence-and/>

⁸⁵ Club of Mozambique (2023). *CIP Mozambique Elections: Internet cut, counting starts.* <https://clubofmozambique.com/news/cip-mozambique-elections-internet-cut-counting-starts-246517/>

⁸⁶ Access Now (2023). *Open letter: clarification on Telegram blocking in Kenya.* <https://www.accessnow.org/press-release/open-letter-clarification-on-telegram-blocking-in-kenya/>

⁸⁷ Access Now (2023). *Warning: blocking online platforms in Kenya will spread election disinformation.* <https://www.accessnow.org/press-release/kenya-online-platforms-social-media-blocking-internet-shutdown-election/>

Republic of the Congo (DRC), Nigeria, and Sierra Leone made and upheld commitments to maintain internet access throughout their elections — a matter of great significance given election-related shutdowns' devastating impact on democracy.⁸⁸

We also saw encouraging developments in the legal battle against election shutdowns in Africa. In 2023, the Economic Community of West African States (ECOWAS) Court of Justice continued to build its jurisprudence against internet shutdowns in a ruling declaring that Guinea's shutdowns during a constitutional referendum and general election in 2020 were unlawful.⁸⁹

Shutdowns during protests, political turmoil, and instability

The region was hit hard by widespread protests against economic hardship, deteriorating democratic tenets, and political instability in 2023. In response to these protests and political turmoil, authorities shut down the internet **10** times — making protests the leading trigger in Africa for the **third** consecutive year.

Plagued by numerous protests and political instability, authorities in **Senegal** disrupted internet access or blocked platforms on **four** occasions. After protests erupted in Dakar and Ziguinchor on June 1 following the arrest of opposition leader Ousmane Sonko,

authorities blocked social media platforms including WhatsApp, Telegram, Instagram, X (formerly Twitter), and YouTube.⁹⁰ Three days later, authorities extended the shutdown to include mobile internet access.⁹¹

Sonko was subsequently arrested again on July 28, 2023. When protests broke out once more in response, authorities reached for the kill switch, cutting mobile internet access and blocking TikTok.⁹² Although authorities restored mobile internet access on August 5, they continued to block TikTok without explanation until February 2024.⁹³

The Senegalese government attempted to justify the shutdowns as necessary to prevent the spread of "hateful and subversive messages," blaming digital platforms for the riots.⁹⁴ The government had previously imposed shutdowns to quell protests after Sonko was initially incarcerated in 2021.⁹⁵ This pattern of repeated internet disruptions to silence government critics, together with journalist arrests and former President Macky Sall's push for new legislation to tighten control over social media platforms, is a warning sign of descent into digital authoritarianism.⁹⁶ With a new administration taking over after a fraught election cycle in February and March 2024, we hope to see Senegal authorities pledge to #KeepItOn.⁹⁷

The press freedom and human rights situation in **Guinea** has deteriorated drastically since the military junta overthrew the Alpha Conde government in 2021.⁹⁸ In May 2023, the military responded to

⁸⁸ *Supra* note 13.

⁸⁹ Media Defence (2023). *ECOWAS Court condemns internet shutdown in Guinea*. <https://www.mediadefence.org/news/ecowas-court-condemns-internet-shutdown-in-guinea/>

⁹⁰ Technext (2023). *Senegal limits social media access following protests over sentencing of opposition leader*. <https://technext24.com/2023/06/03/sonko-senegal-social-media/>

⁹¹ Reuters (2023). *Senegal government cuts mobile internet access amid deadly rioting*. <https://www.reuters.com/world/africa/senegal-government-cuts-mobile-internet-access-amid-deadly-rioting-2023-06-04/>

⁹² Reuters (2023). *Senegal blocks TikTok in widening clampdown on dissent*. <https://www.reuters.com/world/africa/senegal-suspends-tiktok-saying-it-was-threatening-stability-2023-08-02/>

⁹³ Access Now (2023). *Stop the internet shutdowns: Senegal authorities must end censorship*. <https://www.accessnow.org/press-release/internet-shutdowns-senegal/>; Africanews (2023). *Senegal declines to lift TikTok ban*. <https://www.africanews.com/2023/10/06/senegal-declines-to-lift-tiktok-ban/>

⁹⁴ News24 (2023). *Senegal shuts down internet as riots erupt after opposition leader sentenced for sex crime*. <https://www.news24.com/news24/africa/news/senegal-shuts-down-internet-as-riots-erupt-after-opposition-leader-sentenced-for-sex-crime-20230602/>

⁹⁵ Bloomberg (2021). *Senegal Shuts Down TV Stations, Internet Disrupted Amid Protests*. <https://www.bloomberg.com/news/articles/2021-03-05/senegal-shuts-down-tv-stations-internet-disrupted-amid-protests/>

⁹⁶ The Africa Report (2021). *Senegal's president joins the chorus against Twitter and Facebook*. <https://www.theafricareport.com/99491/senegals-president-joins-the-chorus-against-twitter-and-facebook/>; Media Foundation for West Africa (2024). *Senegal: Six journalists arrested over Minister's defamation complaint*. <https://www.mfwa.org/issues-in-focus/senegal-six-journalists-arrested-over-ministers-defamation-complaint/>

⁹⁷ Al Jazeera (2024). *Senegal's top court confirms Bassirou Diomaye Faye's election victory*. <https://www.aljazeera.com/news/2024/3/29/senegals-top-court-confirms-bassirou-diomaye-fayes-election-victory/>

⁹⁸ Reporters Without Borders (2023). *Unprecedented press freedom violations by Guinea military junta*. <https://rsf.org/en/unprecedented-press-freedom-violations-guinea-s-military-junta/>

civil society calls for protests against the junta by restricting access to WhatsApp, Facebook, Facebook Messenger, Telegram, Snapchat, and Instagram for several months.⁹⁹ While the military denied responsibility and attributed the disruption to technical problems with the submarine cable that connects Guinea to the internet,¹⁰⁰ evidence gathered by the Open Observatory of Network Interference (OONI) indicates the blocking was implemented by means of TLS interference.¹⁰¹ The junta followed up with a more extensive communications shutdown in November, jamming radio station signals, suspending TV stations, and blocking social media platforms,¹⁰² only restoring access on February 22, 2024.¹⁰³

In **Ethiopia**, where conflict continues to break out, and parts of Tigray have been disconnected for years on end, authorities continue to wield internet shutdowns in response to national crises. On February 4, 2023, after a group of church leaders called for protests, the government blocked access to social media platforms, including Facebook, TikTok, and Telegram, and maintained the block for over five months.¹⁰⁴ Ethiopian authorities had declared the protests illegal and discouraged the public from participating, warning that they would provoke unrest.¹⁰⁵

Finally, in **Mauritania**, authorities blocked mobile internet access on March 6, 2023, immediately after four prisoners, described as “terrorists” by the Interior Ministry, escaped from a jail in Nouakchott.¹⁰⁶ People could not connect to mobile networks while

authorities conducted a nationwide search for the prisoners, putting their safety at risk.¹⁰⁷ This was one of several internet shutdowns in response to jailbreaks globally in 2023 — a concerning new application of this abusive tactic by law enforcement agencies.

Shutdowns during elections

After a relatively quiet electoral year for the region in 2022, Access Now placed **11** African countries that had previously imposed internet shutdowns on the 2023 #KeptOn Election Watch — Benin, the DRC, Eswatini, Gabon, Liberia, Nigeria, Sierra Leone, and Zimbabwe.¹⁰⁸

Among the countries on the watchlist, only Gabon imposed an internet shutdown, but as we have noted, Mozambique became a first-time offender during its local elections. Uganda continued blocking Facebook, as it had since the 2021 elections, bringing the total number of election-related shutdowns recorded in Africa to **three**.

The Ali Bongo government in Gabon, which had imposed shutdowns during previous elections, blocked internet access and imposed a nighttime curfew after polls closed on August 26, amid reports of voter suppression and electoral misconduct at various polling centers.¹⁰⁹ The lack of international election observers and the suspension of foreign broadcasts prior to the elections had already cast

⁹⁹ Access Now (2023). *Stop shutting down the internet in Guinea: authorities must #KeptOn amidst protest*. <https://www.accessnow.org/press-release/stop-shutting-down-the-internet-guinea/>

¹⁰⁰ GuinéeNews (2023). *Perturbation de la connexion internet en Guinée: quand Ousmane Gaoual fait le faux-fuyant*. <https://guineenews.org/perturbation-de-la-connexion-internet-en-guinee-quand-ousmane-gaoual-fait-le-faux-fuyant/>

¹⁰¹ Open Observatory of Network Interference (@OpenObservatory). X post. 10:18 am. May 22, 2023. <https://x.com/OpenObservatory/status/1660591036316499968>; see also Access Now (2022). *A taxonomy of internet shutdowns: the technologies behind network interference*. <https://www.accessnow.org/shutdown-taxonomy-report>

¹⁰² Media Foundation for West Africa (2023). *Radio airwaves jammed, social media blocked in Guinea*. <https://www.mfwa.org/issues-in-focus/radio-airwaves-jammed-social-media-blocked-in-guinea/>

¹⁰³ Open Observatory of Network Interference (@OpenObservatory). X post. 3:23 pm. February 23, 2024. <https://x.com/OpenObservatory/status/1761049064752177282/>

¹⁰⁴ Access Now (2023). *Ethiopia authorities must stop blocking social media*. <https://www.accessnow.org/press-release/ethiopia-social-media-protest/>

¹⁰⁵ Addis Standard (2023). *News: Joint Security, Intelligence Task Force cautions against unauthorized rallies, threatens to take actions as Orthodox Church Schism takes toll*. <https://addisstandard.com/news-joint-security-intelligence-task-force-cautions-against-unauthorized-rallies-threatens-to-take-action-calls-as-orthodox-church-schism-takes-toll/>

¹⁰⁶ Cloudflare Radar (@CloudflareRadar). X post. 8:19 am. March 6, 2023. <https://x.com/CloudflareRadar/status/1632747652608581633/>

¹⁰⁷ Reuters (2023). *Two guards killed in gunfire as four break out of jail*. <https://www.reuters.com/world/africa/two-guards-killed-gunfire-four-break-out-mauritania-jail-2023-03-06/>

¹⁰⁸ *Supra* note 13. Access Now (2023).

¹⁰⁹ Reuters (2023). *Gabon cuts internet, imposes curfew amid election voting delays*. <https://www.reuters.com/world/africa/gabon-vote-president-bongo-seeks-extend-56-year-family-dynasty-2023-08-26/>

doubt on the transparency and fairness of the election.¹¹⁰ Unsurprisingly, the Gabonese Election Centre declared Bongo the victor, which would have extended his presidential tenure into a third term.¹¹¹ However, the military enacted a coup, annulled the election results, and immediately restored internet access, ending the three-day shutdown.¹¹²

In **Mozambique**, authorities responded to opposing voices during local elections in October by cracking down on opposition members, journalists, and human rights defenders, including through arbitrary arrests and shootings.¹¹³ The announcement of the election outcome sparked mass protests across the country against alleged electoral fraud,¹¹⁴ and that is when, for the first time in our records, authorities disrupted access to the internet, shutting it down for about three hours amid reports of power outages.¹¹⁵

These disruptions represent deplorable attacks on democracy. But as we highlighted above, the DRC, Nigeria, and Sierra Leone, all past offenders, each made and upheld commitments to keep people connected during elections.¹¹⁶ African countries thereby led the way globally among past offenders in demonstrating a commitment to reform, a positive example for countries in the region and around the world. There was more good news in March 2024, when the African Commission on Human and Peoples' Rights (ACHPR) issued its resolution condemning election shutdowns in Africa, crucially recognizing the importance of access to the internet for the realization of human rights, and calling for states to take action to keep people connected during elections, including through legislation and other interventions.¹¹⁷

Countries with election-related shutdowns in Africa in 2023 ▼

Gabon

Mozambique

Uganda

Past offenders who made commitments to #KeepItOn during elections in 2023 ▼

DRC

Nigeria

Sierra Leone

¹¹⁰ *Ibid.*

¹¹¹ Reuters (2023). *Gabon President Ali Bongo wins third term after disputed election*. <https://www.reuters.com/world/africa/gabon-president-ali-bongo-wins-third-term-after-disputed-election-2023-08-30/>

¹¹² Reporters Without Borders (2024). *Reacting to Gabonese army's post-coup statements, RSF issues ten recommendations for respecting press freedom*. <https://rsf.org/en/reacting-gabonese-army-s-post-coup-statements-rsf-issues-ten-recommendations-respecting-press/>

¹¹³ Club of Mozambique (2023). *Mozambique: Shootings, arrests, internet and power outages taints vote counts, Sala da Paz says*. <https://clubofmozambique.com/news/mozambique-shootings-arrests-internet-and-power-outages-taint-vote-counts-sala-da-paz-says-246532/>

¹¹⁴ ISS Africa (2023). *Fraudulent municipal elections cripple democracy in Mozambique*. <https://issafrica.org/iss-today/fraudulent-municipal-elections-cripple-democracy-in-mozambique/>

¹¹⁵ *Supra* note 43.

¹¹⁶ *Supra* note 13.

¹¹⁷ *Supra* note 48.

// Shutdowns during conflict: Ethiopia

The Ethiopian government's use of shutdowns is especially harmful during conflict. Yet despite public outcry, authorities persist in keeping people almost entirely in the dark while their lives are at stake.

In April 2023, after the Ethiopian army moved to disarm the Amhara Special Forces and other regional allies, protests and violence broke out in Gondar, Kobo, Sekota, Weldiya, and other cities in the Amhara region. As the situation escalated, federal authorities blocked mobile internet access across Amhara, cutting millions of people off from the rest of the world.¹¹⁸ When the fighting intensified in August, the government declared a state of emergency and once again shut down internet access, amid chilling reports of ethnic cleansing.¹¹⁹ Authorities also arrested journalists and blocked press access in a crackdown on coverage of the ongoing conflict.¹²⁰

Ethiopia's systematic use of internet shutdowns and media censorship during conflict makes it extremely difficult for people to access lifesaving information, as well as to get humanitarian assistance, including emergency healthcare, water, food, shelter, and protection services.¹²¹ The disruptions also make it difficult to ascertain and document the scale and scope of atrocities being perpetrated by warring parties. The Ethiopian Human Rights Commission has reported instances of extrajudicial killings, sexual

violence, physical assault, displacement, and destruction of civilian property by government security forces and state militia, as well as a deteriorating situation marked by escalating atrocities, including a disturbing increase in sexual and gender-based violence.¹²² After more than a year of fighting at the time of publication, the conflict and attacks against civilians continue to escalate.¹²³ These atrocities, which may amount to war crimes, stand in serious violation of international humanitarian law.¹²⁴

Even after a conflict is over, internet shutdowns exacerbate pain and suffering and prevent recovery from violence and devastation. As we write, the peace process initiated in November 2022 following a years-long conflict and humanitarian crisis in Tigray has yet to take hold.¹²⁵ There is persistent insecurity, drought, famine, and disruptions to humanitarian aid, all of which continue to harm civilians attempting to piece their lives back together after the war.¹²⁶ Relentless attacks on an already fragile telecommunications infrastructure, and slow progress by authorities to rebuild, have left many people in Tigray either completely disconnected, forced to travel outside their community to access a connection, or limited to extremely slow and unreliable service. As we have highlighted, that means that by the end of 2023, many had spent **1,153 days** disconnected, when they needed help the most.

¹¹⁸ The Guardian (2023). *Gun battles erupt in Ethiopia as PM axes Amhara region's security force*. <https://www.theguardian.com/global-development/2023/apr/12/gun-battles-erupt-in-ethiopia-as-pm-axes-amhara-regions-security-force/>

¹¹⁹ The Guardian (2023). *Ethiopia declares a state of emergency in Amhara amid increasing violence*. <https://www.theguardian.com/global-development/2023/aug/04/ethiopia-declares-a-state-of-emergency-in-amhara-amid-increasing-violence/>; OHCHR (2023). *Comprehensive investigative findings and legal determinations. International Commission of Human Rights Experts on Ethiopia*. <https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/chreethiopia/a-hrc-54-crp-3.pdf>

¹²⁰ Addis Standard (2023). *News: CPJ urges authorities to release journalist detained without charge*. <https://addisstandard.com/news-cpj-urges-authorities-to-release-journalist-detained-without-charge/>

¹²¹ See *supra* note 119.

¹²² Ethiopian Human Rights Commission (2023). *Amhara Region: Concerning human rights violations in the context of the armed conflict*. <https://ehrc.org/amhara-region-concerning-human-rights-violations-in-the-context-of-the-armed-conflict/>

¹²³ Foreign Policy (2024). *Ethiopia's Amhara Conflict Could Spark Civil War*. <https://foreignpolicy.com/2024/03/06/ethiopia-amhara-conflict-civil-war/>

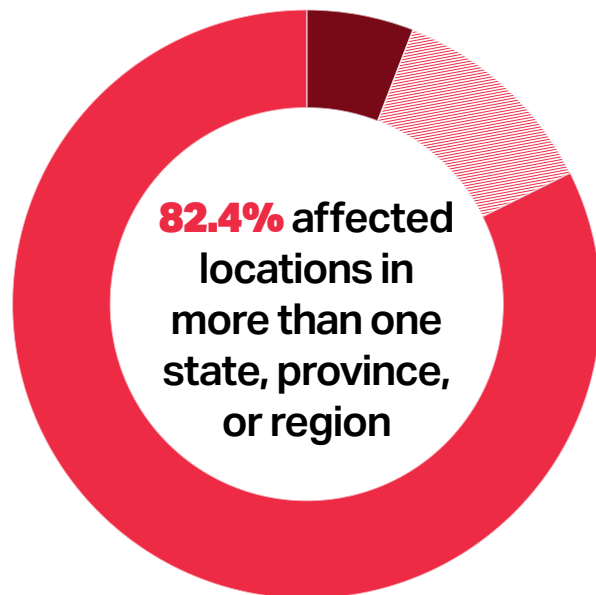
¹²⁴ Amnesty International (2024). *Ethiopia: End extrajudicial Executions in Amhara region, bring perpetrators to justice*. <https://www.amnesty.org/en/latest/news/2024/02/ethiopia-end-extrajudicial-executions-in-amhara-region-bring-perpetrators-to-justice/>

¹²⁵ *Supra* note 32.

¹²⁶ See AP News (2024). *Ethiopia's Tigray region is now peaceful, but extreme hunger afflicts its children*. <https://apnews.com/article/ethiopia-hunger-crisis-tigray-malnutrition-health-7e085f5bd2ac138a27fdc0ec544fb296/>

Shutdowns in Africa in 2023 ▼

- **5.9%** only affected one city, county, or village
- ▨ **11.8%** affected more than one city in the same state, province, or region



Platform blocks

In **10** of the region's 17 shutdowns, authorities specifically targeted social media platforms. During protests in **Ethiopia** and **Senegal** and elections in **Guinea**, governments blocked access to a suite of social media platforms, in attempts to restrict the flow of information and suppress dissent. Authorities in **Kenya** blocked access to Telegram for the first time during national exams in November.¹²⁷ While the government did not issue any formal public shutdown order, the blocking was reportedly imposed to limit the spread of leaked examination materials.¹²⁸

Uganda's blocking of Facebook starting during the 2021 election has continued to cause serious damage to human rights and the digital market.¹²⁹ Yet even after legal threats from the Urban Smart Traders Business Association Limited in October 2023, and an ongoing challenge filed at the East African Court of Justice in 2021, the government failed to lift the

block.¹³⁰ In January 2024, Uganda's Minister for ICT and National Guidance claimed that the Uganda Communications Commission (UCC) was in talks with Facebook about how to resume operation in the country after the three-year blockade, but as we write, the outcome of any such talks is uncertain.¹³¹

In **Tanzania**, authorities imposed service-based shutdowns for the first time since 2020, signaling an increasing crackdown on digital spaces. In January, authorities blocked access to Grindr, as part of a wider campaign to suppress the rights of LGBTQ+ people and communities.¹³² In August, they also blocked Clubhouse, a social networking app based on audio-chat, with no explanation.¹³³ A few months later, the Tanzania Communication Regulatory Authority (TCRA) issued a directive restricting the use of virtual private networks (VPNs), which can assist people in regaining access to blocked platforms.¹³⁴

¹²⁷ Access Now (2023). *Telegram in Kenya: keep people connected during national exams*. <https://www.accessnow.org/press-release/telegram-kenya-connected-national-exams/>

¹²⁸ TechCabal (2023). *Telegram is disrupted in Kenya as internet authorities remain silent*. <https://techcabal.com/2023/11/21/telegram-offline-in-kenya/>

¹²⁹ Monitor (2022). *We'll reopen Facebook when they stop playing games – Museveni*. <https://www.monitor.co.ug/uganda/news/national/we-ll-reopen-facebook-when-they-stop-playing-games-museveni-4064942>

¹³⁰ allAfrica (2023). *Uganda: Govt Given Two Week Ultimatum to Reopen Facebook or Face Legal Action*. <https://allafrica.com/stories/202310250583.html>; East African Court of Justice (2021). *Reference No. 12 of 2021 East African Law Society v. The Attorney General of the Republic of Uganda & The Secretary General of the East African Community*. <https://www.eacj.org/?cases=reference-no-12-of-2021-east-african-law-society-v-the-attorney-general-of-the-republic-of-uganda-the-secretary-general-of-the-east-african-community>

¹³¹ New Vision (2024). *Govt, Facebook in talks to end three year blockade*. https://www.newvision.co.ug/category/news/govt-facebook-in-talks-to-end-three-year-bloc-NV_179442/

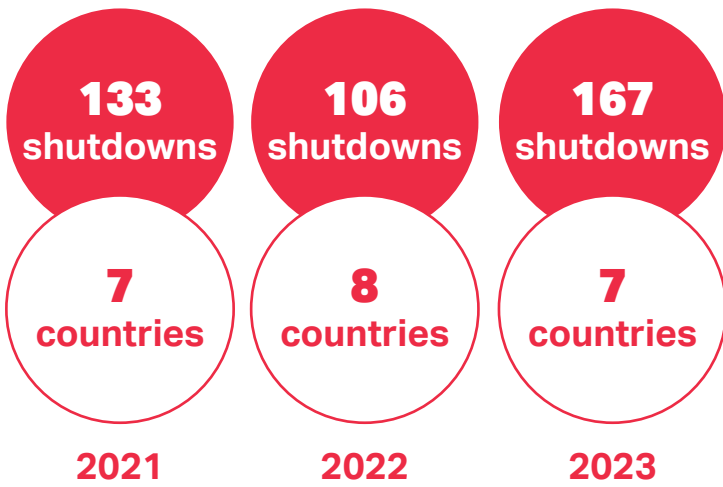
¹³² OONI (2023). *Tanzania blocked Grindr*. <https://explorer.ooni.org/findings/203466718601/>

¹³³ OONI (2023). *Tanzania blocked Clubhouse*. <https://explorer.ooni.org/findings/185407756401/>

¹³⁴ CIO Africa (2023). *Tanzania Imposes Ban On VPN Usage Without A Permit*. <https://cioafrica.co/tanzania-imposes-ban-on-vpn-usage-without-a-permit/>

Asia Pacific (APAC)

Regional overview in 2023



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;¹³⁵

Indonesia continued to block Grindr;¹³⁶ and Nepal joined the shame list in 2023 with its blocking of TikTok.¹³⁷ Against a backdrop of extensive censorship under the Great Firewall, China maintained ongoing blocks of Signal and Grindr.¹³⁸

Myanmar

Since February 1, 2021, when Myanmar's junta seized power in a deadly coup, the people of Myanmar

¹³⁵ See, e.g., Cloudflare (2023). *Cloudflare's view of Internet disruptions in Pakistan*. <https://blog.cloudflare.com/cloudflares-view-of-internet-disruptions-in-pakistan/>; The Daily Star (2023). *BTRC asks telecom operators to shut down internet for 9 hours in Nayapaltan*. <https://www.thedailystar.net/news/bangladesh/news/btrc-asks-telecom-operators-shut-down-internet-9-hours-nayapaltan-3454956/>

¹³⁶ Time (2016). *Indonesia Wants to Ban Grindr and Dozens of Other Gay-Networking Apps*. <https://time.com/4496531/indonesia-lgbt-grinder/>; OONI (2024). *Web Connectivity Test, www.grindr.com*. https://explorer.ooni.org/chart/mat?test_name=web_connectivity&axis_x=measurement_start_day&since=2023-01-01&until=2024-04-01&time_grain=day&probe_cc=ID&domain=www.grindr.com

¹³⁷ Time (2023). *Nepal Bans TikTok and Tightens Control Over All Social Media Platforms*. <https://time.com/6334769/nepal-tiktok-ban-social-media-regulation/>

¹³⁸ TechCrunch (2021). *Rising encrypted app Signal is down in China*. <https://techcrunch.com/2021/03/15/signal-is-down-in-china/>; NBC News (2022). *Grindr disappears from app stores in China amid internet clean-up campaign*. <https://www.nbcnews.com/news/world/grindr-dating-disappears-china-app-stores-internet-clean-campaign-rcna14531/>

have endured unrelenting attacks, both physical and digital.¹³⁹ 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.¹⁴⁰ 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.¹⁴¹ 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.¹⁴² 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.¹⁴³ 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.¹⁴⁴ 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 top of the ongoing and targeted shutdowns.¹⁴⁵

¹³⁹ Access Now (2024). *The world must bring down Myanmar's digital iron curtain*. <https://www.accessnow.org/press-release/third-year-myanmar-coup/>

¹⁴⁰ See, e.g., Access Now (2022). *Internet shutdowns shroud and facilitate brutality of Myanmar junta's airstrike in Hpakant township*. <https://www.accessnow.org/press-release/myanmar-internet-shutdown-hpakant/>

¹⁴¹ Radio Free Asia (2022). *Myanmar military said to kill hundreds in Sagaing, Magway after blocking internet*. <https://www.rfa.org/english/news/myanmar/internet-09282022162550.html/>

¹⁴² *Supra* note 67.

¹⁴³ *Supra* note 8; see also Narinjara (2024). *MPT and Mytel Phone Lines Disrupted in Some Rakhine State Townships Due to Fuel Shortages Impacting Cell Towers*. <https://www.narinjara.com/news/detail/657762eb30a7ecc1ceb008cd/>

¹⁴⁴ *Ibid.*

¹⁴⁵ OHCHR (2022). *Myanmar: UN experts condemn military's "digital dictatorship"*. <https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship/>; Article 19 (2023). *UN: Myanmar junta tightens its grasp on online spaces*. <https://www.article19.org/resources/un-myanmar-junta-tightens-its-grasp-online-spaces/>; VOA News (2023). *How Myanmar's Junta Uses Telecom Companies to Target Journalists*. <https://www.voanews.com/a/how-myanmar-s-junta-uses-telecom-companies-to-target-journalists/7096082.html/>

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.¹⁴⁶

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.¹⁴⁷ 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.¹⁴⁸

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.¹⁴⁹

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.¹⁵⁰ 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.¹⁵¹

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

¹⁴⁶ Myanmar Internet Project (2024). *Examining the Situation of Digital Repression in Myanmar in 2023*. https://www.myanmarinternet.info/post/blog_014-1/

¹⁴⁷ Radio Free Asia (2024). *Two-month travel ban extended in western Myanmar*. <https://www.rfa.org/english/news/myanmar/rakhine-travel-ban-02222024060301.html/>; see also The Irrawaddy (2024). *Rakhine state registration holders military council travel restrictions*. <https://burma.irrawaddy.com/news/2024/03/20/381225.html/>

¹⁴⁸ See, e.g., Rehmonnya FM (@Rehmonnya FM). Facebook post. 8:34 am. March 27, 2024. <https://www.facebook.com/rehmonnyafm/videos/1749056002286449/>

¹⁴⁹ Access Now (2024). *A call for global solidarity and decisive action to end Myanmar's military rule and ensure victory for the people resisting dictatorship*. <https://www.accessnow.org/press-release/statement-myanmar-coup-en/>

¹⁵⁰ Access Now (2023). *Manipur, India, internet shutdowns; stop shielding abuse against women*. <https://www.accessnow.org/press-release/india-internet-shutdowns-women/>; National Commission on Population (2020). *Report Of The Technical Group On Population Projections*. https://main.mohfw.gov.in/sites/default/files/Population%20Projection%20Report%202011-2036%20-%20upload_compressed_0.pdf/

¹⁵¹ *Ibid.* Access Now (2023).

searched for an alleged separatist on the run.¹⁵²

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.¹⁵³

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.¹⁵⁴ Meanwhile, the harms of shutdowns in the country continue to be immense and multi-faceted, impairing education, healthcare, press freedom, and more.¹⁵⁵

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.¹⁵⁶ Shutdowns reportedly cost the country **\$1.9 billion** and a loss of **\$118 million** in foreign investment in the first half of 2023 alone.¹⁵⁷ On an individual level, the economic damage of shutdowns can be devastating. For people in a large section of the workforce in India, shutdowns can translate to no work, no pay, and no food.¹⁵⁸ Shutdowns especially hurt marginalized groups who rely on the internet for newer revenue streams and for accessing gatekept opportunities.¹⁵⁹

These harms are amplified further when placed in the context of India's race to digitize access to services.¹⁶⁰

¹⁵² CNN (2023). *India cuts internet to 27 million as Punjab police hunt Sikh separatist*. <https://edition.cnn.com/2023/03/20/india/india-separatist-manhunt-internet-shutdown-intl-hnk/index.html/>

¹⁵³ Quartz (2023). *India has blocked 14 mobile messenger apps on security fears*. <https://qz.com/india-has-blocked-14-messenger-apps-on-security-fears-1850390425/>; *Supra* note 73; Government of India (2023). *Regulation of Activities of Intermediaries and Social Media*. <https://sansad.in/getFile/annex/262/AU732.pdf?source=pqars>

¹⁵⁴ Global Freedom of Expression (2020). *Bhasin v. Union of India*. <https://globalfreedomofexpression.columbia.edu/cases/bhasin-v-union-of-india/>; LiveLaw (2023). *Manipur High Court Orders State To Operationalise Mobile Towers In Violence Free Areas 'On Trial Basis'*. <https://www.livelaw.in/high-court/manipur-high-court/manipur-internet-ban-mobile-tower-restoration-high-court-241772/>; The Hindu (2024). *Supreme Court directs publication of final orders of panel reviewing 'proportionality' of Internet suspensions in J&K*. <https://www.thehindu.com/news/national/supreme-court-on-panel-reviewing-internet-suspensions-in-jammu-kashmir/article67878209.ece/>

¹⁵⁵ India Today (2023). *How Manipur students battling crisis and appearing for the university exams*. <https://www.indiatoday.in/education-today/news/story/how-students-of-manipur-are-battling-crisis-and-appearing-for-the-university-exams-2419060-2023-08-10/>; The Wire (2023). *India's Internet Shutdowns Hurt Women More, Manipur Assaults Show*. <https://thewire.in/security/indias-internet-shutdowns-hurt-women-more-manipur-assaults-show/>; Newslandry (2023). *No internet, frenzied mobs: Manipur journalists on 'biggest challenges' to reporting on the conflict*. <https://www.newslandry.com/2023/05/17/2023/05/10/no-internet-frenzied-mobs-manipur-journalists-on-biggest-challenges-to-reporting-on-the-conflict/>; Newslick (2023). *Manipur Internet Shutdown Hurting Patients: Doctors*. <https://www.newslick.in/manipur-internet-shutdown-hurting-patients-doctors/>; Imphal Free Press (2023). *Internet ban affecting professionals in Manipur*. <https://www.ifp.co.in/manipur/internet-ban-affecting-professionals-in-manipur/>

¹⁵⁶ Internet Society Pulse (n.d.). *Netloss Calculator*. <https://pulse.internetsociety.org/netloss/>

¹⁵⁷ The Economic Times (2023). *Internet shutdowns cost \$1.9 billion to India in Jan-Jun 2023: Report*. <https://economictimes.indiatimes.com/tech/technology/internet-shutdowns-cost-1-9-billion-to-india-in-jan-jun-2023-report/articleshow/101368283.cms>

¹⁵⁸ Human Rights Watch (2023). *"No Internet Means No Work, No Pay, No Food"*. <https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic/>

¹⁵⁹ Rest of World (2022). *Connection unstable: Kashmir's influencers seek internet fame but can't get online*. <https://restofworld.org/2022/kashmir-influencers-blackouts/>; see also The Wire (2021). *The Internet Belongs to Dalit-Bahujan People Too*. <https://thewire.in/caste/dalit-bahujan-social-media-tiktok-jai-bhim/>

¹⁶⁰ See Digital India (n.d.). *Digital India*. <https://www.digitalindia.gov.in/>

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.¹⁶¹ 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.¹⁶² 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.¹⁶³

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.¹⁶⁴ 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 2021.¹⁶⁵

In **Taiwan**, following repeated damage to undersea cables in February 2023, 14,000 residents of the Matsu Islands lost internet and phone service for at least two months.¹⁶⁶ 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.¹⁶⁷ Experts indicated the levels of damage to the steel-encased cables were "highly unusual."¹⁶⁸ According to Chunghwa, Taiwan's largest telecoms provider, the cables have been cut 27 times in the past five years, which is disproportionate to other regions globally.¹⁶⁹ 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.¹⁷⁰ This disruption has further highlighted the immense vulnerability of internet infrastructure for Taiwan

¹⁶¹ See Telecom Regulatory Authority of India (2023). *The Indian Telecom Services Performance Indicators: July–September, 2023*. https://traai.gov.in/sites/default/files/QPIR_09022024_0.pdf

¹⁶² Freedom House (2024). *Freedom In The World 2024; China*. <https://freedomhouse.org/country/china/freedom-world/2024/>

¹⁶³ VOA News (2024). *China's VPN Usage Nearly Doubles Amid Internet Censorship*. <https://www.voanews.com/a/china-s-vpn-usage-nearly-doubles-amid-internet-censorship/7488465.html/>

¹⁶⁴ Freedom House (2021). *Freedom On The Net 2021*. <https://freedomhouse.org/country/china/freedom-net/2021/>

¹⁶⁵ *Supra* note 138.

¹⁶⁶ AP News (2023). *Taiwan suspects Chinese ships cut islands' internet cables*. <https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366d7a7c70/>

¹⁶⁷ *Ibid.*

¹⁶⁸ *Ibid.*

¹⁶⁹ Vice (2023). *'A Warning Sign': Chinese Ships Accused of Cutting Off Internet to a Taiwanese Island*. <https://www.vice.com/en/article/bvj8x3/taiwan-internet-cables-matsu-china/>

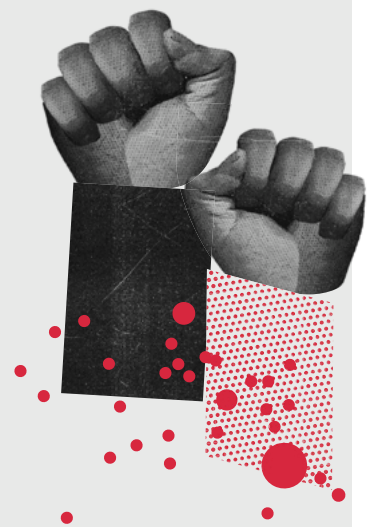
¹⁷⁰ See, e.g., Reuters (2021). *China's latest weapon against Taiwan: the sand dredger*. <https://www.reuters.com/graphics/TAIWAN-CHINA/SECURITY/jbyvrnzerve/>

and the region.¹⁷¹ 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.¹⁷² 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.¹⁷³ 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.¹⁷⁴ 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.¹⁷⁵



¹⁷¹ 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>

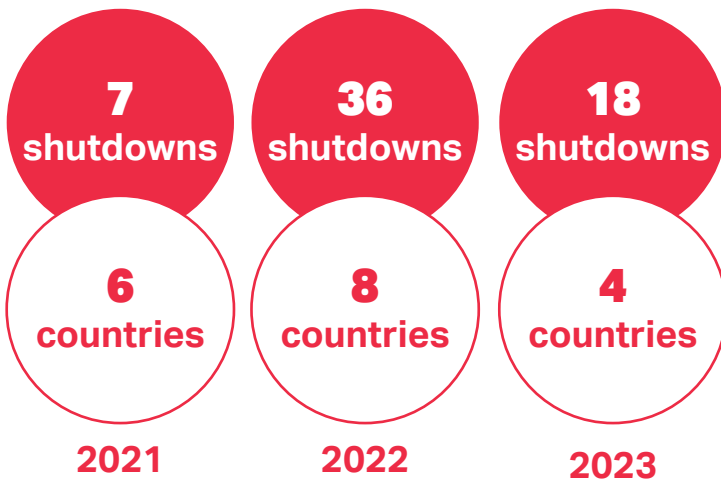
¹⁷² *Supra* note 11.

¹⁷³ See, e.g., *supra* note 135. Cloudflare (2023).

¹⁷⁴ Access Now (2024). *#KeepItOn: To defend democracy authorities must immediately reconnect Pakistan's internet.* <https://www.accessnow.org/press-release/keepiton-restore-internet-pakistan-elections-2024/>; see also The Diplomat (2024). *Pakistan's X Restrictions Near 1-Month Mark, Despite Court Ruling.* <https://thediplomat.com/2024/03/pakistans-x-restrictions-near-1-month-mark-despite-court-ruling/>

¹⁷⁵ See *supra* note 135. The Daily Star (2023).

Eastern Europe and Central Asia (EECA) Regional overview in 2023



13 shutdowns during conflict in 2023:

- ✦ 5 missile strikes targeting civilian infrastructure by the Russian military
- ✦ 4 deliberate disconnections in the Nagorno-Karabakh region
- ✦ 3 cyberattacks in Ukraine
- ✦ 1 conflict-related platform block in Azerbaijan (TikTok)

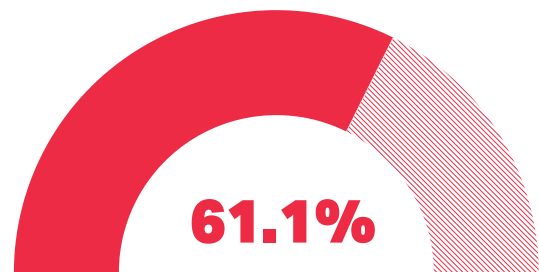
The total number of shutdowns in the EECA region dropped by more than **50%** from 2022 to 2023, due to the shifting situation on the battlefield during Russia's continued illegal invasion and occupation of Ukraine, and a downturn in new cases in Central Asia after a spike in 2022.¹⁷⁶ However, the region still saw **18** shutdowns, **13** of which were implemented during active conflict where military use of targeted missile strikes, cyberattacks, and deliberate disconnections led to spotty connectivity and a variety of shutdowns. Authorities in Russia and Turkmenistan combined repressive censorship and efforts to build isolated national intranets with multi-year platform blocks to assert control over the flow of information domestically. Overall, Russia's outsized impact is impossible to ignore: in 2023, it alone implemented **50%** of all shutdowns in the EECA region.

Ukraine: 8*

***6 of these imposed by Russia**

Azerbaijan: 5

Russia: 3 Turkmenistan: 2



of shutdowns in the region corresponded to documented **grave human rights abuses**

Russia and Ukraine

As Russia's illegal invasion of Ukraine continued to draw condemnation domestically and internationally, Russian authorities also continued to wield shutdowns as part of their military strategy in Ukraine and as a tool to silence critics at home.¹⁷⁷ In 2023, Access Now and the #KeptItOn coalition recorded **nine** shutdowns perpetrated by Russian authorities in Russia and Ukraine.

Russian authorities imposed **six** shutdowns in **Ukraine** in 2023, compared to **22** in 2022. While the total number of shutdowns decreased, the scale, scope, and impact were just as significant. In 2022, Russia repeatedly attacked and attempted to gain control

¹⁷⁶ See The Washington Post (2023). *How Russia learned from mistakes to slow Ukraine's counteroffensive*. <https://www.washingtonpost.com/world/2023/09/08/russia-ukraine-defense-counteroffensive/>

¹⁷⁷ See Consilium.europa.eu (2024). *EU response to Russia's war of aggression against Ukraine*. <https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/>

over Ukraine's telecommunications infrastructure.¹⁷⁸ In occupied Ukrainian territories where Russia has rerouted Ukrainian internet infrastructure to connect to Russian-controlled networks, people may now be less likely to experience full network disruptions. However, Russia-controlled internet also subjects these communities to Russia's ongoing surveillance and censorship, putting them at further risk.

That said, Russia has continued to conduct military attacks that impact communications infrastructure. Throughout 2023, the military launched missiles targeting Ukraine's energy facilities and power grids across the country, resulting in emergency power outages in major metropolitan areas including Kharkiv, Lviv, Ivano-Frankivsk, Zaporizhzhia, Vinnytsia, and Kyiv.¹⁷⁹ The assault caused internet outages that blocked millions of people's access to information during the ongoing invasion.¹⁸⁰

In December 2023, Russia launched a cyberattack that caused a service outage at one of Ukraine's biggest telecoms, Kyivstar. This left millions without an internet connection.¹⁸¹ The shutdown caused ATMs to fail and disrupted the proper functioning of air-raid alert systems.¹⁸² According to Ukrainian officials, the attack was intended to gather intelligence and cause psychological distress for Ukrainians.¹⁸³

Ukrainian actors also imposed **two** shutdowns as part of a strategy of resistance against Russia's ongoing occupation. In May 2023, Ukrainian hackers disabled the website of Russian internet service provider Miranda Media.¹⁸⁴ And in October 2023, the Ukraine IT Army confirmed they had temporarily disabled the services of three Russian internet providers operating in Crimea: Miranda Media, Krimtelekom, and MirTelekom.¹⁸⁵

Meanwhile, Russian authorities continued blocking online platforms both in Russia and the occupied territories of Ukraine in attempts to control the narrative and more effectively spread disinformation and propaganda through official channels.¹⁸⁶ They maintained blocks of X (formerly Twitter), Facebook, and Instagram, and made threats of censorship against other social media platforms, such as YouTube and WhatsApp, to force them to comply with government content moderation directives.¹⁸⁷ For example, both Facebook and Instagram have been blocked since October 2022, when authorities designated their parent company Meta an extremist organization and accused it of "Russiaphobia" for allowing criticism of Russia's invasion of Ukraine to circulate on its platforms.¹⁸⁸ In 2023, Meta was also forced to drop the launch of its WhatsApp Channels in Russia, which would have enabled people to publicly broadcast information to wider audiences on the app, after the country's federal censorship agency,

¹⁷⁸ *Supra* note 1. Access Now (2023).

¹⁷⁹ See, e.g., CNN (2023). *Missile strikes will lead to emergency power cuts across Ukraine, energy minister says*. https://www.cnn.com/europe/live-news/russia-ukraine-war-news-1-14-23/h_cb548fad3d1247ec433677f6358cea4e

¹⁸⁰ Cyberscoop (2023). *Russian attacks on Ukrainian infrastructure cause internet outages, cutting off a valuable wartime tool*. <https://cyberscoop.com/ukraine-internet-outages-infrastructure-attacks/>

¹⁸¹ Reuters (2023). *Ukraine's top mobile operator hit by biggest cyberattack of war*. <https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/>

¹⁸² Reuters (2024). *Exclusive: Russian hackers were inside Ukraine telecoms giant for months*. <https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/>

¹⁸³ Cybercrime Programme Office (2024). *Cybercrime Digest: 1-15 January 2024*. <https://rm.coe.int/cyber-digest-cproc-2024-01-01/1680ae548a>

¹⁸⁴ The Record (2023). *Russia's 'Silicon Valley' hit by cyberattack; Ukrainian group claims deep access*. <https://therecord.media/skolkovo-foundation-cyberattack-russia-ukraine>

¹⁸⁵ The Record (2023). *Ukrainian hackers disrupt internet providers in Russia-occupied territories*. <https://therecord.media/ukrainian-hackers-disrupt-internet-providers-crimea>

¹⁸⁶ Access Now (2022). *Updates: Digital rights in the Russia-Ukraine conflict*. <https://www.accessnow.org/russia-throttled-twitter/>

¹⁸⁷ Access Now (2021). *Russia throttled Twitter to censor content — Here's what happens next*. <https://www.accessnow.org/russia-throttled-twitter/>; The Verge (2022). *Russia bans Instagram as promised, blocking access for 80 million users*. <https://www.theverge.com/2022/3/14/22976603/russia-bans-instagram-facebook-meta-call-to-violence>. *Are they preparing to block YouTube in Russia? What is known about this* <https://www.dw.com/ru/v-rossii-gotovat-blokirovku-youtube-cto-ob-etom-izvestno/a-66622887>; The Bell (2023). *Russia's authorities are talking about blocking WhatsApp. What would this mean in reality?* <https://en.thebell.io/russias-authorities-are-talking-about-blocking-whatsapp-what-would-this-mean-in-reality/>

¹⁸⁸ The Moscow Times (2022). *Russia Adds Meta to List of 'Terrorist and Extremist' Orgs*. <https://www.themoscowtimes.com/2022/10/11/russia-adds-meta-to-list-of-terrorist-and-extremist-orgs-a79057>

Roskomnadzor, threatened to block WhatsApp entirely if the new feature rolled out.¹⁸⁹

The Putin regime has a history of using threats against platforms to silence the opposition. During parliamentary elections in 2021, the government successfully pressured Google and Apple to block opposition leader Alexey Navalny's Smart Voting project app from their stores and platforms, reportedly by threatening criminal prosecution and office raids.¹⁹⁰ Navalny was arrested that same year, and in 2024, he died in prison amid accusations of murder by the Russian government.¹⁹¹

In addition to directly blocking platforms, Russian authorities are banning and blocking the tools to bypass these blocks, including virtual private networks (VPNs).¹⁹² As of November 2023, Russia had reportedly blocked the domains of **eight** of the 15 most popular VPN services.¹⁹³ While authorities officially banned any tools that could be used for circumvention in 2020, they are now going further. As of March 1, 2024, the government has also banned any advertising of these tools.¹⁹⁴ That could include

sites that provide instructions for accessing VPNs, such as Wikipedia.¹⁹⁵

In early 2024, we have already recorded incidents of Russian authorities disrupting access to mobile internet and social media platforms at night, as well as restricting access to VPNs.¹⁹⁶

Azerbaijan-Armenia conflict

Azerbaijan perpetrated a total of **five** shutdowns in 2023 in the context of its ongoing territorial dispute with Armenia.¹⁹⁷ Of these disruptions, **four** targeted the disputed Nagorno-Karabakh region and **one** impacted all of Azerbaijan — all taking place alongside human rights violations and deepening the humanitarian crisis.¹⁹⁸

189 The Moscow Times (2022). *WhatsApp Drops Channels Launch in Russia Over Ban Threat*. <https://www.themoscowtimes.com/2023/09/26/whatsapp-drops-channels-launch-in-russia-over-ban-threat-a82564>

190 Access Now (2023). *Not good enough: Apple, Google bow to government pressure, censor content during Russia elections*. <https://www.accessnow.org/press-release/apple-google-censor-russian-elections/>; see also The New York Times (2021). *Google and Apple, Under Pressure From Russia, Remove Voting App*. <https://www.nytimes.com/2021/09/17/world/europe/russia-navalny-app-election.html>; Financial Times (2021). *Apple and Google drop Navalny app after Kremlin piles pressure*. <https://www.ft.com/content/faaada81-73d6-428c-8d74-88d273adb3>; Al Jazeera (2021). *Why are Google and Apple still silent on Russian censorship?* <https://www.aljazeera.com/opinions/2021/11/1/why-are-google-and-apple-still-silent-on-russia-censorship>

191 The Guardian (2024). *Russian activist and Putin critic Alexei Navalny dies in prison*. <https://www.theguardian.com/world/2024/feb/16/russian-activist-and-putin-critic-alexei-navalny-dies-in-prison>

192 RosKomSvoboda (2023). *VPN in Russia: from blocking services to blocking protocols*. https://roskomsvoboda.org/uploads/en_vpn_in_russia_from_blocking_services_to_blocking_protocols.pdf; see also Al Jazeera (2022). *VPN use skyrockets in Russia during Ukraine invasion*. <https://www.aljazeera.com/news/2022/5/7/vpn-use-skyrockets-in-russia-during-ukraine-invasion>

193 OONI (2023). *How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine*. <https://ooni.org/post/2023-russia-a-year-after-the-conflict/>; RosKomSvoboda (2023). *VPN in Russia: from blocking services to blocking protocols*. <https://roskomsvoboda.org/ru/analysis/vpn-russia-2023-eng/>

194 Tass (2024). *Ban on advertising VPN services to take effect on March 1 — media watchdog*. <https://tass.com/economy/1742101>; see also The New York Times (2024). *Russia Strengthens Its Internet Controls in Critical Year for Putin*. <https://www.nytimes.com/2024/03/15/technology/russia-internet-censors-vladimir-putin.html>

195 Meduza (2023). *Russian government authorizes federal censor to block websites with instructions for bypassing website blocks*. <https://meduza.io/en/news/2023/11/18/russian-government-authorizes-federal-censor-to-block-websites-with-instructions-for-bypassing-website-blocks>; Meduza (2024). *Russia may block Wikipedia due to article on VPNs that help reach blocked sites, says lawmaker*. <https://meduza.io/en/news/2024/03/03/russia-may-block-wikipedia-due-to-article-on-vpns-that-help-reach-blocked-sites-says-lawmaker>

196 See Meduza (2024). *Nighttime mobile Internet outages in Russian regions reportedly linked to anti-drone measures, not routine technical work*. <https://meduza.io/en/news/2024/01/29/nighttime-mobile-internet-outages-in-russian-regions-reportedly-linked-to-anti-drone-measures-not-routine-technical-work>; The Moscow Times (2024). *Widespread Telegram, WhatsApp Outages Reported Across Russia*. <https://www.themoscowtimes.com/2024/01/24/widespread-telegram-whatsapp-outages-reported-across-russia-a83830>

197 Access Now (2023). *Turn TikTok on: authorities in Azerbaijan and Armenia must not restrict access*. <https://www.accessnow.org/press-release/tiktok-azerbaijan-armenia/>

198 See Human Rights Watch (2024). *New Wave of Arrests Targets Journalists and Activists in Azerbaijan*. <https://www.hrw.org/news/2024/03/07/new-wave-arrests-targets-journalists-and-activists-azerbaijan>; Crisis Group (2023). *Responding to the Humanitarian Catastrophe in Nagorno-Karabakh*. <https://www.crisisgroup.org/europe-central-asia/caucasus/nagorno-karabakh-conflict/responding-humanitarian-catastrophe-nagorno>

The Nagorno-Karabakh crisis

People in the Nagorno-Karabakh region had already been suffering under a worsening humanitarian crisis since December 2022, when Azerbaijani troops blockaded the Lachin corridor, completely cutting off the only road connecting Nagorno-Karabakh to Armenia.¹⁹⁹ UN experts raised the alarm, emphasizing that the blockade had resulted in “acute shortages of food staples, medication, and hygiene products, impacted the functioning of medical and educational institutions, and placed the lives of the residents — especially children, persons with disabilities, older persons, pregnant women, and the sick — at significant risk.”²⁰⁰ On January 12, 2023, after more than a month of the blockade, an internet disruption only made the situation more dire, raising concerns that people would be unable to contact emergency services and underscoring the importance of ensuring connectivity during crisis and conflict.²⁰¹

On September 19, 2023, Azerbaijan launched its so-called “anti-terrorist” operation, attacking Armenian forces in Nagorno-Karabakh and re-taking control of the territory. At least 200 people, including civilians and children, were reportedly killed, and over 400 others were wounded.²⁰² The offensive resulted in almost all ethnic Armenians — a population of about 120,000 — fleeing Nagorno-Karabakh.²⁰³ As Azerbaijan started its offensive, authorities throttled internet access in Karabakh’s Fuzuli district and cut access to TikTok for the entire country, both to restrict the flow of information.²⁰⁴ Both disruptions lasted for more than a month.²⁰⁵ On September 20, Azerbaijani authorities also cut off mobile and internet access in Stepanakert City amid heavy bombardment.²⁰⁶ Karabakh residents reported disruptions in several other districts, which we were unable to conclusively confirm.²⁰⁷

Both parties in the conflict have used platform blocking in attempts to control the narrative. Alarmingly, they have also defended the use of internet shutdowns during conflict. In September 2022, Azerbaijan and Armenia each blocked TikTok.²⁰⁸ When civil society challenged Armenia’s TikTok ban, the chief of staff at the National Security Service Director’s office defended the government’s actions, claiming that a legal provision granting the power to “oversee information security matters”

¹⁹⁹ See Human Rights Watch (2024). *New Wave of Arrests Targets Journalists and Activists in Azerbaijan*. <https://www.hrw.org/news/2024/03/07/new-wave-arrests-targets-journalists-and-activists-azerbaijan>; Crisis Group (2023). *Responding to the Humanitarian Catastrophe in Nagorno-Karabakh*. <https://www.crisisgroup.org/europe-central-asia/caucasus/nagorno-karabakh-conflict/responding-humanitarian-catastrophe-nagorno>

²⁰⁰ OHCHR (2023). *UN experts urge Azerbaijan to lift Lachin corridor blockade and end humanitarian crisis in Nagorno-Karabakh*. <https://www.ohchr.org/en/press-releases/2023/08/un-experts-urge-azerbaijan-lift-lachin-corridor-blockade-and-end>; see also Forbes (2023). *Lachin Corridor Blockade Starves Nagorno-Karabakh*. <https://www.forbes.com/sites/ewelinaochab/2023/08/08/lachin-corridor-blockade-starves-nagorno-karabakh/>

²⁰¹ Radio Azatutyun (2023). *The almost complete failure of internet and telephone creates new problems in Karabakh*. <https://rus.azatutyun.am/a/32222107.html>

²⁰² CNN (2023). *Azerbaijan launches operations against Armenian forces in Nagorno-Karabakh*. <https://edition.cnn.com/2023/09/19/asia/armenia-azerbaijan-nagorno-karabakh-bombardment-intl/index.html>

²⁰³ The Guardian (2023). *Almost all ethnic Armenians have left Nagorno-Karabakh*. <https://www.theguardian.com/world/2023/sep/30/almost-all-ethnic-armenians-have-left-nagorno-karabakh-azerbaijan>

²⁰⁴ Al Jazeera (2023). *Azerbaijan forces attack Nagorno-Karabakh as threat of new war looms*. <https://www.aljazeera.com/news/2023/9/19/azerbaijan-forces-attack-nagorno-karabakh-as-threat-of-new-war-looms>; AIW (2023). *Internet disruptions in Fuzuli*. <https://www.az-netwatch.org/news/internet-disruptions-in-fuzuli/>; OONI Explorer (2023). *Azerbaijan blocked TikTok and Google Play Store amid military offensive in Nagorno-Karabakh*. <https://explorer.ooni.org/findings/67768606801>

²⁰⁵ *Ibid.*

²⁰⁶ CNN (2023). *Azerbaijan launches operations against Armenian forces in Nagorno-Karabakh*. <https://edition.cnn.com/2023/09/19/asia/armenia-azerbaijan-nagorno-karabakh-bombardment-intl/index.html>; <https://explorer.ooni.org/findings/67768606801>; see also, CNN (2023). *‘We are starving to death.’ Inside Nagorno-Karabakh’s blockade on the edge of Europe*. <https://edition.cnn.com/2023/09/06/europe/nagorno-karabakh-blockade-azerbaijan-armenia-intl-cmd/index.html>

²⁰⁷ *Supra* note 204. AIW (2023).

²⁰⁸ OONI (2022). *Azerbaijan and Armenia block TikTok amid border clashes*. <https://ooni.org/post/2022-azerbaijan-and-armenia-blocks-tiktok/>; see also Turan.az (2020). <https://turan.az/en/question-answer/the-issue-of-blocking-the-internet-should-be-reviewed-in-the-interests-of-the-country-2089770>

provides the authority to impose such blocks.²⁰⁹ The Armenian government is also seeking to legitimize shutdowns in the future by amending the existing law.²¹⁰

Central Asia

It was not only conflict that sparked shutdowns in the ECA region in 2023. Governments in Central Asia continued using them in efforts to curb dissent. Authorities across Central Asia used shutdowns to crack down on a wave of protests in 2022.²¹¹ Repressive measures led to more limited protests activity in 2023, and therefore an overall drop in the number of shutdowns in the region, but the problem persists and authorities have not demonstrated a willingness to reform.

In **Kazakhstan**, for example, after tens of thousands took to the streets in 2022, authorities deployed a relentless campaign against activists and community organizers, making it nearly impossible to organize public demonstrations without facing serious repercussions.²¹² At local rallies and events dedicated to the anniversary of the 2022 protests, community members reported the suspected use of signal jammers, indicating authorities' continued willingness to use disruptions to silence people.²¹³

In **Turkmenistan**, authorities continued to block major social media platforms and VPNs as a measure of control.²¹⁴ They also shut down internet access across the country for several days in June 2023 during the launch of a new city named in honor of Gurbanguly Berdimukhammedov, who had ended a 16-year presidential term after handing the role over to his son.²¹⁵

²⁰⁹ Access Now (2023). *Open letter: Armenian government must safeguard internet access and freedom of expression, abandon the provision in law "On the Legal Regime of Martial Law."* <https://www.accessnow.org/press-release/open-letter-armenian-law-must-prohibit-internet-shutdowns/>; Access Now (2023). *Armenia National Security Service Director Letter.* <https://www.accessnow.org/armenia-national-security-service-director-letter-tiktok-blocking>

²¹⁰ Eurasianet (2023). *Armenian authorities seek new internet censorship powers under martial law.* <https://eurasianet.org/armenian-authorities-seek-new-internet-censorship-powers-under-martial-law>

²¹¹ *Supra* note 1. Access Now (2023).

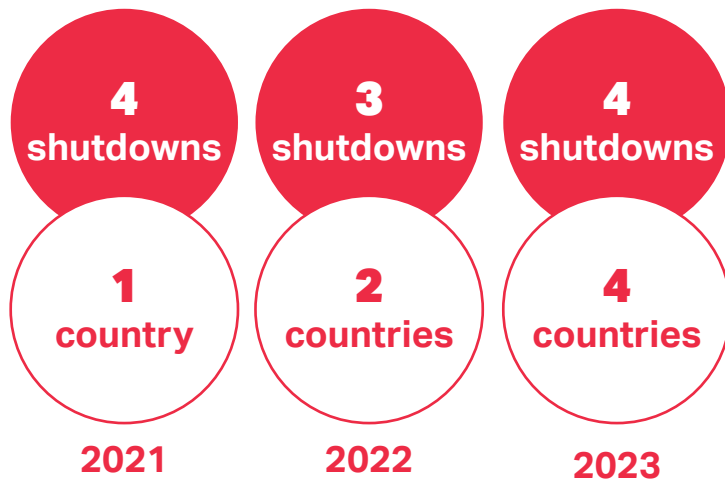
²¹² Radio Free Europe (2023). *Kazakhstan Still Not Allowing Space For Protests.* <https://www.rferl.org/a/kazakhstan-not-allowing-protests/32648115.html>

²¹³ Vlast (2021). *Hundreds of people attended a rally of the Democratic Party in Almaty.* <https://vlast.kz/novosti/44711-sotni-celovek-vysli-na-miting-dempartii-v-almaty.html>; see also Radio Azattyk (2020). *"Nazarbayev, ket!" Calls for the resignation of the "leader of the nation" at a rally for reforms.* <https://rus.azattyq.org/a/kazakhstan-almaty-rally-on-political-reforms/30922602.html>; Mediazona (2021). *Women's march and rally in Almaty.* <https://mediazona.ca/online/2021/03/08/marsh>

²¹⁴ Turkmen News (2023). *Digital vacuum. What hostings, providers, and services are blocked in Turkmenistan?* <https://turkmen.news/cifrovoy-vakuum-kakie-hostingi-provajdery-i-servisy-zablokirovany-v-turkmenistane/>; Progres (2024). *The State Directed Internet Blockade Continued in Turkmenistan in 2023.* <https://progres.online/society/the-state-directed-internet-blockade-continued-in-turkmenistan-in-2023/>; Access Now (2023). *What Turkmenistan internet shutdown tells us about digital repression in Central Asia.* <https://www.accessnow.org/turkmenistan-internet-shutdowns/>

²¹⁵ Civicus Monitor (2023). *Internet disruptions, deportations of Turkey-based activists and bread protests.* <https://monitor.civicus.org/explore/internet-disruptions-deportations-of-turkey-based-activists-and-bread-protests/>; AP News (2023). *Turkmenistan's president expands his father's power.* <https://apnews.com/article/politics-gurbanguly-berdimuhamedov-turkmenistan-a8e746a5bb9935323f3f52e193b54468>

Latin America and the Caribbean (LAC) Regional overview in 2023



Cuba: 1
Brazil: 1
Suriname: 1
Venezuela: 1

Suriname
joined the offender list
for the first time in 2023

Cuba imposed a shutdown for the fourth year in a row

In Latin America and the Caribbean, we documented **four** shutdowns in **four** countries in 2023 — the highest number of countries to impose shutdowns in the region in a single year on record. While the total is low compared to other regions, we are alarmed to see more countries disrupting access year after year and yet another new offender emerge.

Since joining the offenders list in 2020, **Cuba** has imposed at least **one** shutdown every year, including in 2023. These disruptions have been part of an intensifying crackdown on dissent and freedom of assembly, which has included attacks on press freedom and tightening control of online spaces.²¹⁶ In May 2023, hundreds of Cubans reported internet outages throughout the country after mass demonstrations erupted in the Guantanamo

municipality of Caimanera with shouts of “freedom,” and protesters were met with police brutality.²¹⁷

Suriname is the first country in the region to join the shame list as a new offender since Cuba in 2020. In February 2023, authorities responded to mass protests in the capital, Paramaribo, and calls for the president and vice president to resign by imposing a 12-hour curfew and disrupting access to social media platforms across the country.²¹⁸ An International Monetary Fund (IMF) rescue plan pushing for reduced spending led the government to take drastic economic measures, like removing subsidies on electricity and fuel.²¹⁹ These policies made an already dire economic situation even worse for people suffering under extreme price hikes and currency devaluation in a country where the majority of the population live on a

²¹⁶ See, e.g., Civicus Monitor (2023). *Cuba: Government authorities crack down on activists and journalists during the G77+China Summit*. <https://monitor.civicus.org/explore/cuba-government-authorities-crack-down-on-activists-and-journalists-during-the-g77-china-summit/>; RSF (2023). *New digital law tightens clampdown on press freedom in Cuba*. <https://rsf.org/en/new-digital-law-tightens-clampdown-press-freedom-cuba>

²¹⁷ Cloudflare Radar (@cloudflareradar). X post. 2:15 am. May 7, 2023. <https://x.com/CloudflareRadar/status/1655042548023402496>; see also Erika Guevara Rosas (@ErikaGuevaraR). X post. 1:18 am. May 7, 2023. <https://x.com/erikaguevarar/status/1655019347151134727>; Camila Acosta (@CamilaAcostaCU). X post. 3:24 am. May 7, 2023. <https://x.com/camilaacostacu/status/1655050974480723970>

²¹⁸ FranceInfo (2023). *Suriname: looting, arrests and internet shutdowns on the sidelines of demonstrations against the high cost of living*. <https://la1ere.francetvinfo.fr/martinique/suriname-pillages-arrestations-et-coupure-d-internet-en-marge-de-manifestations-contre-la-vie-chere-1367742.html>

²¹⁹ *Ibid.*

minimum wage of 57 cents per hour.²²⁰ Cutting people off from channels to organize, express dissent, and access crucial information only makes matters worse.

In **Venezuela**, authorities returned to old patterns of imposing internet shutdowns during critical national events, including elections and protests.²²¹ In October 2023, there were widespread reports of internet disruptions in several areas in Caracas coinciding with primary voting for opposition candidates.²²² Although the government claimed the disruptions were due to power outages, the timing aligns with patterns of past disruptions, and the government has since taken repeated steps to undermine the election process. A Supreme Court ruling suspended the primary process and disqualified the winning opposition candidate from running against President Nicolás Maduro.²²³ The court also ordered the opposition to submit all voter registrations to the electoral commission for investigation, raising serious concerns about future retaliation against opposition supporters and further irregularities in the presidential election scheduled for July 2024.²²⁴

Brazil, another repeat offender, blocked Telegram for the second year in a row, after what had seemed to be a move away from platform blocking orders following two cases in 2016.²²⁵ On April 26, 2023, a federal judge ordered internet service providers to block Telegram across the country in an attempt to force the company to give the police information about participants in suspected hate group chat rooms.²²⁶ The block was lifted on April 29 after another federal judge intervened, stating that a complete shutdown "is not reasonable, given the broad impact throughout the national territory on the freedom of communication of thousands of people who are absolutely strangers to the facts under investigation."²²⁷ The judge that initially ordered the block had done the same thing in 2022, ordering the blocking of Telegram for two days for failing to comply with police and judicial orders to remove disinformation in the lead-up to the presidential election.²²⁸

²²⁰ *Ibid.*

²²¹ Access Now (2023). *Connectivity problems raise red flags ahead of Venezuelan elections*. <https://www.accessnow.org/connectivity-problems-raise-red-flags-ahead-venezuelan-elections/>

²²² *Supra* note 44.

²²³ The Guardian (2023). *Venezuela primary results suspended in latest blow directed at opposition*. <https://www.theguardian.com/world/2023/oct/30/venezuela-primary-election-results-suspended-machado-maduro>

²²⁴ *Ibid.*; *supra* note 7.

²²⁵ See Access Now (2016). *Brazil moves to block WhatsApp (again)*. <https://www.accessnow.org/brazil-moves-block-whatsapp/>

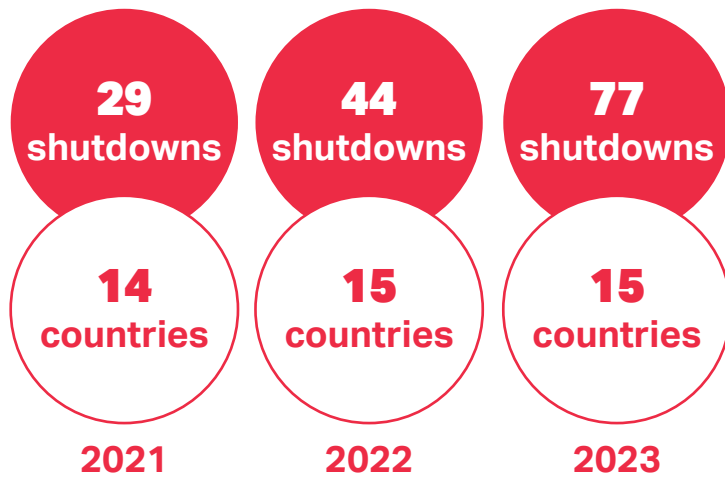
²²⁶ AP (2023). *Brazil judge orders temporary suspension of Telegram*. <https://apnews.com/article/brazil-telegram-suspension-social-media-school-violence-d72acaacd3c1b4d07c2c4fcb094f4ce6>; see also OONI Explorer (2024). *Telegram Test: Brazil*. https://explorer.ooni.org/chart/mat?test_name=telegram&axis_x=measurement_start_day&since=2023-04-17&until=2023-05-02&time_grain=day&probe_cc=BR

²²⁷ AP (2023). *Telegram app back on in Brazil after judge lifts suspension*. <https://apnews.com/article/brazil-violence-schools-technology-1f48e38bddef741e11a4a05e2e242ffa>

²²⁸ DW (2022). *Brazil blocks messaging app Telegram*. <https://www.dw.com/en/brazil-telegram-messaging-app-blocked-by-top-court/a-61183805>

Middle East and North Africa (MENA)

Regional overview in 2023



Iran: 34

Palestine: 16*

*all imposed by Israel

Iraq: 6

Jordan: 3 Libya: 3 Mauritania: 2
Oman: 2 Sudan: 2 Syria: 2
Türkiye: 2 Algeria: 1 Lebanon: 1
Qatar: 1 Saudi Arabia: 1
United Arab Emirates: 1

Grindr is blocked in 8 countries:

Iran, Jordan, Lebanon, Oman, Qatar, Saudi Arabia, Türkiye, United Arab Emirates

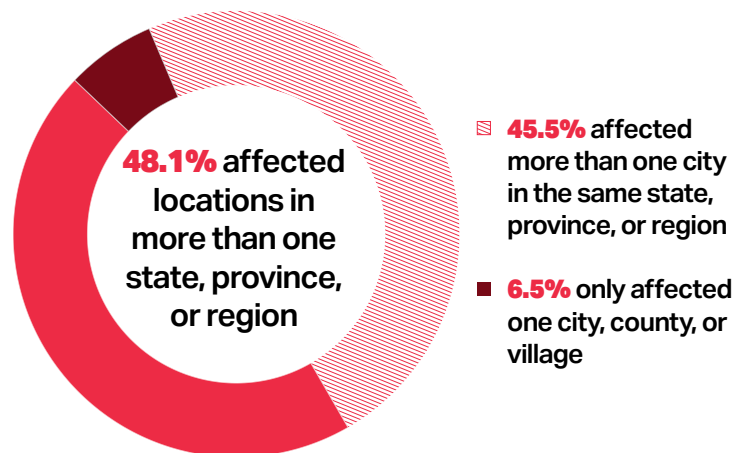
Shutdowns during natural disasters:



Earthquake
in Türkiye
and Iraq



Floods
in Libya



In 2023, people across the MENA region faced an onslaught of violence and upheaval, including the outbreak of conflict between competing military factions in Sudan and Israel's war in Gaza following the Hamas attack on October 7. The region also saw devastating natural disasters in Libya, Syria, Iraq, and Türkiye and a continued crackdown on protesters and women in Iran.²²⁹ Amid these tumultuous and tragic developments that have resulted in some of the worst humanitarian crises in recent history — including tens of thousands of deaths, famine, and displacement of millions across the region — authorities tightened control over the flow of information, causing further havoc and suffering.

In 2023, Access Now and the #KeepItOn coalition documented **77** shutdowns in **15** countries — the highest annual number of both shutdown incidents and perpetrators on record in the region since 2016. In 2022, we documented **44** shutdowns in **15** countries. Iran, which is known for its repressive tactics, accounted for **34** shutdowns in 2023, most of which targeted protesters. Israel perpetrated all **16** shutdowns recorded in Palestine as part of its attack on the Gaza Strip.

The increasing deployment of internet shutdowns during armed conflicts, continued use of shutdowns during exams, and targeting of vulnerable groups in the MENA region in the past few years is alarming and must be condemned by all actors.

²²⁹ Atlantic Council (2023). *2023: A year in the Middle East*.

<https://www.atlanticcouncil.org/blogs/menasource/2023-a-year-in-the-middle-east>

Palestine

Since Hamas attacked Israel on October 7, 2023, the Israeli military has committed unspeakable horrors against Palestinians in the Gaza Strip. As we write, the official death toll exceeding 30,000 people is still climbing daily as thousands more remain missing under the rubble.²³⁰ Israeli authorities have systematically impeded entry of humanitarian aid, including food, water, and healthcare, while destroying all essential civilian infrastructure in the Gaza Strip, including telecommunications, hospitals, and schools.²³¹ Israel's incessant disruption of humanitarian and emergency aid in Gaza is severely limiting people's access to food, spurring the World Health Organization (WHO) to warn of looming famine and starvation that put children especially at risk.²³² UN human rights experts have issued stark warnings about the potential genocide in the Gaza Strip,²³³ the International Court of Justice (ICJ) has ordered Israel to respect and uphold its binding obligations to prevent genocide,²³⁴ and the UN Security Council has passed a resolution calling for a "lasting sustainable ceasefire."²³⁵ Access Now supports this call.²³⁶

Since the start of the war, Israeli authorities have weaponized internet shutdowns through a range of tactics, including imposing intermittent communications blackouts coinciding with intense bombing and shelling, destroying telecommunications infrastructure, cutting off traffic to individual internet service providers (ISPs), and blocking access to fuel required to power telecommunications services.²³⁷ Together, these shutdowns have kept people in Gaza almost entirely in the dark and have cut them off from an essential lifeline.

Starting on October 9, at least **15** out of the 19 ISPs in Gaza were facing complete shutdown of their mobile and broadband services, while the remaining four were encountering substantial, though differing, degrees of disruption, affecting millions across the Gaza Strip.²³⁸ Throughout the rest of the year, and with heavy bombardment continuing and fuel depleting, internet traffic in the Gaza Strip significantly plummeted, with at least **eight** full communication blackouts for the entirety of the Strip occurring between October and December.²³⁹ Israel has also reportedly targeted repair workers attempting to restore internet access after the destruction. This includes two workers from Palestinian telecom provider Jawwal who were killed when an Israeli missile hit their car on January 13,

²³⁰ NPR (2024). *Gaza's death toll now exceeds 30,000. Here's why it's an incomplete count.* <https://www.npr.org/2024/02/29/1234159514/gaza-death-toll-30000-palestinians-israel-hamas-war>

²³¹ Refugees International (2024). *Siege and Starvation: How Israel Obstructs Aid to Gaza.* <https://www.refugeesinternational.org/reports-briefs/siege-and-starvation-how-israel-obstructs-aid-to-gaza/>; BBC News (2024). *World Food Programme says northern Gaza aid convoy blocked.* <https://www.bbc.com/news/world-middle-east-68486248>; International Rescue Committee (2024). *The collapse of Gaza's health system.* <https://www.rescue.org/article/collapse-gazas-health-system>; Human Rights Watch (2023). *Gaza: Unlawful Israeli Hospital Strikes Worsen Health Crisis.* <https://www.hrw.org/news/2023/11/14/gaza-unlawful-israeli-hospital-strikes-worsen-health-crisis>; Al Jazeera (2024). *How Israel has destroyed Gaza's schools and universities.* <https://www.aljazeera.com/news/2024/1/24/how-israel-has-destroyed-gazas-schools-and-universities>; Wired (2023). *The Destruction of Gaza's Internet Is Complete.* <https://www.wired.com/story/gaza-internet-blackout-israel/>; *Supra* note 10. Access Now (2023).

²³² Tedros Adhanom Ghebreyesus (@DrTedros). X post. 12:22 pm. March 6, 2024. <https://x.com/DrTedros/status/1765352292197261356>

²³³ OHCHR (2023). *Gaza: UN experts call on international community to prevent genocide against the Palestinian people.* <https://www.ohchr.org/en/press-releases/2023/11/gaza-un-experts-call-international-community-prevent-genocide-against>; OHCHR (2024). *States must adhere to obligations under Genocide Convention to prevent further loss of life in Gaza, says Special Rapporteur Francesca Albanese.* <https://www.ohchr.org/en/press-releases/2024/03/states-must-adhere-obligations-under-genocide-convention-prevent-further>

²³⁴ International Court of Justice (2024). *Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel): The Court indicates provisional measures.* <https://www.icj-cij.org/sites/default/files/case-related/192/192-20240126-pre-01-00-en.pdf>

²³⁵ Amnesty International (2024). *UN resolution must pave way for enduring ceasefire to alleviate mass suffering in Gaza.* <https://www.amnesty.org/en/latest/news/2024/03/un-resolution-must-pave-way-for-enduring-ceasefire-to-alleviate-mass-suffering-in-gaza/>

²³⁶ Access Now (2023). *Human rights organizations join the open call for an immediate physical and digital ceasefire in Gaza, and for Palestinians globally.* <https://www.accessnow.org/press-release/palestine-israel-physical-digital-ceasefire/>

²³⁷ *Supra* note 64.

²³⁸ *Ibid.*

²³⁹ *Supra* note 25. Access Now (2023); see also Access Now (@accessnow). X post. 4:30 pm. December 7, 2023. <https://x.com/accessnow/status/1732799830131351995>; Paltel (@paltelco). X post. 2:54 pm. December 17, 2023. <https://x.com/Paltelco/status/1736398936750117082>

while they were traveling to repair telecommunications infrastructure in Khan Yunis.²⁴⁰ These ongoing internet shutdowns deepen the suffering of people in Gaza, and make the work of UN bodies and humanitarian organizations to assist over two million people — 85% of whom are internally displaced, starved, and traumatized — an “impossible mission.”²⁴¹

While people in Gaza struggled to stay connected and get help, major social media platforms were simultaneously censoring Palestinian and pro-Palestinian voices on their platforms.²⁴² Since October 7, advocates have faced increased censorship online.²⁴³ This censorship has been particularly heavy on Meta-owned platforms Facebook and Instagram, where activists have documented systematic silencing of Palestinian voices through arbitrary content removals, suspension of prominent Palestinian and Palestine-related accounts, restrictions on pro-Palestinian users and content, and shadow-banning.²⁴⁴ Through the #StopSilencingPalestine campaign, Access Now and our partners have called on Meta to put an end to its long-standing practice of censoring Palestinian voices and to overhaul its content moderation policies.²⁴⁵

Sudan

In Sudan, the ongoing conflict between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF) has taken a devastating toll, claiming at least 12,000 lives by the end of 2023, with the numbers of people killed, injured, and displaced continuing to climb daily.²⁴⁶ The tragic situation has led to what experts describe as “one of the world’s worst” humanitarian crises.²⁴⁷ Within Sudan, more than nine million people have been forced to flee their homes, with the World Food Program (WFP) warning of an impending hunger crisis of unprecedented proportions.²⁴⁸ We recorded at least **two** shutdowns in 2023 during this conflict, but the impact on telecommunications services has been more far-reaching than has been possible to document and verify under current conditions. Major shutdowns continue in 2024, including a month-long shutdown starting in February²⁴⁹ which impacted the entire country after the RSF reportedly took over telecommunications facilities in Khartoum.²⁵⁰

Sudanese authorities have a long history of using internet shutdowns to curtail fundamental human rights, control the narrative during turmoil, and cover up atrocities. The warring parties in Sudan have weaponized internet shutdowns by instructing telecommunications companies to limit access or by damaging ISP data centers — a tactic to gain control

²⁴⁰ Jawwal (@JawwalPal). X post. 5:12 pm. January 13, 2024. <https://x.com/JawwalPal/status/1746218633221591108>

²⁴¹ ReliefWeb (2024). *The war in Gaza must end - Statement by Martin Griffiths, Under-Secretary-General for Humanitarian Affairs and Emergency Relief Coordinator*, 5 January 2024. <https://reliefweb.int/report/occupied-palestinian-territory/war-gaza-must-end-statement-martin-griffiths-under-secretary-general-humanitarian-affairs-and-emergency-relief-coordinator-5-january-2024-enhear>

²⁴² Al Jazeera (2023). *Are social media giants censoring pro-Palestine voices amid Israel’s war?* <https://www.aljazeera.com/features/2023/10/24/shadowbanning-are-social-media-giants-censoring-pro-palestine-voices>

²⁴³ 7amleh (2023). *Briefing on The Palestinian Digital Rights Situation Since October 7th, 2023*. <https://7amleh.org/2023/11/01/briefing-on-the-palestinian-digital-rights-situation-since-october-7th-2023>; 7amleh (2024). *Hashtag Palestine 2023: Palestinian Digital Rights During War*. <https://7amleh.org/2024/01/17/hashtag-palestine-2023-palestinian-digital-rights-during-war>

²⁴⁴ Human Rights Watch (2023). *Meta’s Broken Promises*. <https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and>; Access Now (2024). *It’s not a glitch: how Meta systematically censors Palestinian voices*. <https://www.accessnow.org/publication/how-meta-censors-palestinian-voices/>

²⁴⁵ Access Now (2023). *#StopSilencingPalestine: Meta must overhaul its biased content moderation*. <https://www.accessnow.org/press-release/meta-stop-silencing-palestine/>; see also Access Now (2023). *A coalition of international organizations demands that Meta refrain from censoring criticism of Zionism on its platforms*. <https://www.accessnow.org/press-release/meta-zionism-policy/>

²⁴⁶ Al Jazeera (2024). *Nearly eight million people displaced by war in Sudan: UN*. <https://www.aljazeera.com/news/2024/1/31/nearly-eight-million-people-displaced-by-war-in-sudan-un>; UN OCHA (2024). *Sudan Situation Report*. <https://reports.unocha.org/en/country/sudan/>

²⁴⁷ AA (2023). *Sudan suffering ‘one of world’s worst humanitarian crisis’: UN*. <https://www.aa.com.tr/en/americas/sudan-suffering-one-of-worlds-worst-humanitarian-crisis-un/3081788>

²⁴⁸ ReliefWeb (2024). *Sudan Humanitarian Update (4 February 2024)*. <https://reliefweb.int/report/sudan/sudan-humanitarian-update-4-february-2024>; UN World Food Programme (2024). *Sudan’s war risks creating the world’s largest hunger crisis, warns WFP Chief*. <https://www.wfp.org/news/sudans-war-risks-creating-worlds-largest-hunger-crisis-warns-wfp-chief>

²⁴⁹ Cloudflare Radar (@cloudflaradar). X post. 2:52 pm. March 3, 2024. <https://x.com/CloudflareRadar/status/1764302833715749347>

²⁵⁰ See *supra* note 22.

and impede the free flow of information in areas controlled by opposing factions.²⁵¹ When fighting between the ruling SAF and paramilitary groups led by the RSF broke out in Khartoum on April 15, 2023, SAF authorities immediately ordered telecommunications providers to shut down their services nationwide.²⁵² With hundreds dead and millions trapped in their homes in Khartoum running low on food and water amid the fighting, a tensely negotiated 72-hour ceasefire was set to begin the night of April 24.²⁵³ In the hours leading up to the ceasefire deadline, yet another nationwide blackout went into place across multiple providers.²⁵⁴ At the same time, in the city of El Geneina in West Darfur, RSF fighters began escalating attacks on civilians as SAF forces withdrew to their base, leaving the community to fend for themselves.²⁵⁵ This was the start of a months-long reign of terror claiming at least 10,000 lives, with reports of mass killings, rampant sexual violence, forced labor, and other war crimes and crimes against humanity.²⁵⁶ During this period, fighting between RSF and SAF forces caused significant damage to telecommunications infrastructure, contributing to ongoing intermittent blackouts and overall degradation of connectivity.²⁵⁷ These disruptions severely limited people's ability to access essential information and to communicate with the world about the crimes being perpetrated. Witness reports also point to a clear strategy by RSF fighters to cover up their attacks on civilians and to prevent documentation, including by

confiscating mobile devices during raids on people's homes and at checkpoints where people were trying to flee the city.²⁵⁸

Military actors in Sudan have a long track record of committing heinous crimes against people amid internet blackouts — from the weeks-long shutdown during the infamous Khartoum massacre in June 2019 to at least four disruptions during the #June30March protests demanding return to civilian rule in 2022.²⁵⁹ People in Sudan have been subjected to internet shutdowns every year since 2018, and 2024 has proven no exception. Both the RSF and SAF have continued to weaponize internet shutdowns during the ongoing conflict, worsening the suffering of **millions** who were cut off from the world once again.²⁶⁰

Iran

In 2023, Access Now and the #KeepItOn coalition recorded a surge in internet shutdowns in Iran, reaching **34** compared to **19** in 2022.²⁶¹ Iran continued its oppressive tactics with internet shutdowns and platform blocking, a trend that intensified following protests responding to the tragic death of Mahsa (Jini) Amini in 2022.²⁶² Iranian authorities use a range of methods to interfere with internet access, silence people, and stifle dissent, from shutting down the global internet to force people onto the highly

²⁵¹ Ayin network (2024). *Sudan Conflict Monitor #10*. <https://3ayin.com/en/scm10/>

²⁵² Reuters (2023). *Sudanese telecom providers block internet services, MTN official says*. <https://www.reuters.com/article/sudan-politics-internet/sudanese-telecoms-provider-mtn-blocks-internet-services-mtn-officials-say-idINS8N35N0D8/>; see also Cloudflare (2023). *Effects of the conflict in Sudan on Internet patterns*. <https://blog.cloudflare.com/sudan-armed-conflict-impact-on-the-internet-since-april-15-2023/>

²⁵³ Al Jazeera (2023). *Sudan factions agree to 72-hour ceasefire as foreigners evacuated*. <https://www.aljazeera.com/news/2023/4/24/us-says-sudan-factions-agree-to-ceasefire-as-foreigners-evacuated>

²⁵⁴ Cloudflare Radar (@cloudflareradar). X post. 11:09 pm. April 23, 2023. <https://x.com/CloudflareRadar/status/1650275825126629377>

²⁵⁵ Reuters (2024). *How Arab fighters carried out a rolling ethnic massacre in Sudan*. <https://www.reuters.com/investigates/special-report/sudan-politics-darfur/>

²⁵⁶ Reuters (2024). *Ethnic killings in one Sudan city left up to 15,000 dead, UN report says*. <https://www.reuters.com/world/africa/ethnic-killings-one-sudan-city-left-up-15000-dead-un-report-2024-01-19/>; OHCHR (2024). *UN experts alarmed by reported widespread use of rape and sexual violence against women and girls by RSF in Sudan*. <https://www.ohchr.org/en/press-releases/2023/08/un-experts-alarmed-reported-widespread-use-rape-and-sexual-violence-against>

²⁵⁷ See Dabanga Radio TV Online (2023). *Communication problems in Darfur as clashes continue*. <https://www.dabangasudan.org/en/all-news/article/communication-problems-in-darfur-as-clashes-continue>; Hamid Khalafallah (@HamidMrutada). X post. 7:45 am. April 24, 2023. <https://x.com/HamidMurtada/status/1650405615498305543>

²⁵⁸ Reuters (2023). *The Slaughter of El Geneina*. <https://www.reuters.com/investigates/special-report/sudan-politics-darfur/>

²⁵⁹ Access Now (2023). *#IAmTheSudanRevolution: There's a direct link between internet shutdowns and human rights violations in Sudan*. <https://www.accessnow.org/iamthesudanrevolution-theres-a-direct-link-between-internet-shutdowns-and-human-rights-violations-in-sudan/>; Access Now (@accessnow). X post. 10:35 am. June 30, 2022. <https://x.com/accessnow/status/1542456849802244097>

²⁶⁰ See *supra* note 22; *supra* note 9.

²⁶¹ Access Now (2023). *Internet shutdowns in MENA in 2022: continued abuses and impunity*. <https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2022-mena/>

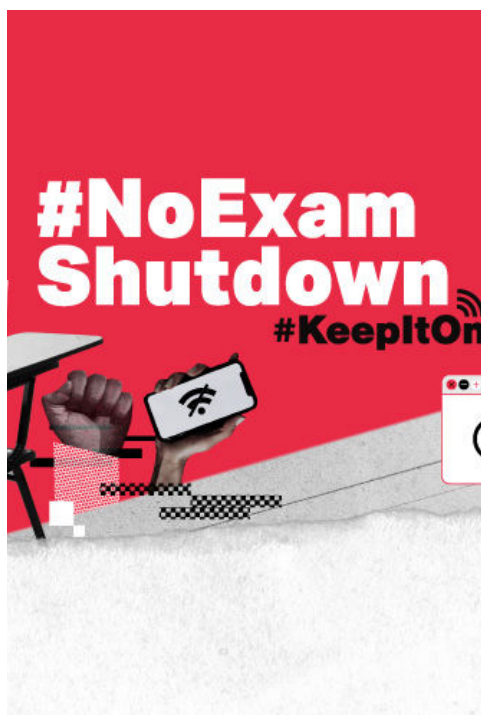
²⁶² Access Now (2023). *The world must not forget Mahsa Amini*. <https://www.accessnow.org/the-world-must-not-forget-mahsa-amini>

censored national intranet, to restricting mobile access and blocking social media and messaging platforms.²⁶³ In 2023, this authoritarian approach reached its peak during protests and crackdowns on ethnic minorities, with at least **28** shutdowns coinciding with weekly protests during Friday prayers in vvv and Baluchistan.²⁶⁴

Throughout 2023, Iranian authorities maintained long-standing blocks of specific apps and services, such as Signal, which has been restricted since January 2021,²⁶⁵ and WhatsApp, Instagram, Skype, LinkedIn,

and Viber, all of which have been restricted since 2022.²⁶⁶ Iranians rely heavily on the internet and these platforms for organizing protests, communicating, and sharing important information.²⁶⁷

Iran has also expanded its use of internet shutdowns in other contexts. In January 2023, authorities disrupted local internet access during university admission exams in an attempt to prevent leaking of exam questions and other forms of cheating.²⁶⁸ This caused significant disruption, negatively impacting businesses and people residing in those areas.²⁶⁹ Authorities also cut internet access in Kurdistan in November, aligning with Iranian President Ebrahim Raisi's visit.²⁷⁰



Shutdowns during exams

Authorities in the MENA region have clung to using internet shutdowns as a method to stop cheating during exams, which has proven to be disproportionate, draconian, and a violation of human rights. Not only do these shutdowns disrupt businesses, banking, emergency services, and people's daily lives, they have failed to stop cheating or leaking of exam questions.²⁷¹ Our monitoring underscores the need for governments and educational leaders to identify measures to address cheating that do not have broad negative impacts for entire populations.²⁷² The governments of Iraq, Syria, Algeria, and Iran imposed a total of **10** shutdowns during exams in 2023.

²⁶³ Reuters (2023). *Iran steps up internet crackdown one year after Mahsa Amini death*. <https://www.reuters.com/article/idUSL8N3AJ203/>

²⁶⁴ Filterwatch (2023). *Cloudflare and Protests in Sistan and Baluchestan become targets of internet disruptions*. <https://filterwatch/en/2023/03/22/cloudflare-and-protests-in-sistan-and-baluchestan-become-targets-of-internet-disruptions/>

²⁶⁵ Al Jazeera (2021). *Iran blocks Signal messaging app after WhatsApp exodus*. <https://www.aljazeera.com/news/2021/1/26/iran-blocks-signal-messaging-app-after-whatsapp-exodus>

²⁶⁶ Euronews (2023). *Iran maintains block on WhatsApp and Instagram*. <https://www.euronews.com/2023/02/01/iran-maintains-block-on-whatsapp-and-instagram>; OONI (2022). *Technical multi-stakeholder report on Internet shutdowns: The case of Iran amid autumn 2022 protests*. <https://ooni.org/post/2022-iran-technical-multistakeholder-report/>

²⁶⁷ Access Now (2023). *Stop suppressing the population: authorities in Iran must #KeepItOn*. <https://www.accessnow.org/press-release/iran-authorities-must-keepiton/>; see also Los Angeles Times (2022). *In protests over death of Mahsa Amini, internet is key to planning. Can Iran block access?* <https://www.latimes.com/world-nation/story/2022-09-28/for-iranian-protesters-a-digital-double-edged-sword>

²⁶⁸ *Supra* note 50. Filterwatch (2024).

²⁶⁹ *Ibid*.

²⁷⁰ IODA (@IODA_live). X post. 7:19 am. November 2, 2023. https://x.com/IODA_live/status/1720053084020240693

²⁷¹ See SMEX (2022). *Internet Shutdowns to Prevent Cheating During Exams: The Impact on Society and Economy in the MENA Region*. <https://smex.org/internet-shutdowns-to-prevent-cheating-during-exams-the-impact-on-society-and-economy-in-the-mena-region/>

²⁷² *Supra* note 51.

Iraqi officials ignored the public outcry against the use of shutdowns during exams, disrupting internet access on **six** occasions during academic exams in February, June, July, August (including platform blocks), and much of September.²⁷³ This resulted in **58** total exam periods where the internet was shut down, with **seven** affecting Kurdistan alone, **eight** impacting all states except Kurdistan, and **43** impacting the entire country. Iraq's Ministry of Education persisted in requesting the shutdowns despite the Ministry of Communication's initial commitment to ensure open and secure internet access throughout the exam period, and ultimately got its request fulfilled, failing the test for respecting human rights.²⁷⁴

Authorities in Syria disrupted internet access on **two** occasions during exams, while Algerian and Iranian authorities each perpetrated **one** exam shutdown. **Syria**, which has a long history of imposing exam-related shutdowns, enforced nationwide internet blackouts on June 25 and 26, imposing a three-and-a-half-hour blackout each day.²⁷⁵ The government of **Algeria** flipped the kill switch for five consecutive days during national exams on June 11–15.²⁷⁶ And as we note above, **Iranian** authorities cut access for university exams in January, but officials in the Ministry of Information and Communications Technology were reportedly able to prevent additional disruptions during the July exam period.²⁷⁷

Jordan and **Mauritania**, which have imposed exam shutdowns in the past,²⁷⁸ seem to be departing from such restrictive measures and showing a commitment to finding alternatives that respect people's rights. Access Now, the Internet Society, and SMEX began the #NoExamShutdown campaign in 2023 to encourage more of these countries to do the same, and in 2024, we will continue to advocate for an end to exam-related shutdowns across the MENA region and beyond.²⁷⁹

Platform blocks and other events

In 2023, **nine** countries across MENA — Iran, Iraq, Jordan, Lebanon, Oman, Qatar, Türkiye, Saudi Arabia, and the United Arab Emirates (UAE) — continued to block access to digital communications platforms that facilitate people's access to information and discourse on national issues. Grindr, a social networking app for gay, bisexual, transgender, and queer people, is blocked in **eight** countries. **Seven** of these blocks have been ongoing for years (Iran, Lebanon, Oman, Qatar, Saudi Arabia, Türkiye, UAE) and were retroactively added to our STOP dataset in 2023.²⁸⁰

Authorities in **Jordan** began blocking access to Grindr for the first time, as one of their **three** shutdowns in

²⁷³ Access Now (2023). *Open Letter: The Prime Minister of Iraq must commit to #KeepItOn at the upcoming cabinet meeting, and put an end to internet shutdowns during exams.* <https://www.accessnow.org/press-release/open-letter-iraq-prime-minister-must-keepiton-during-exams/>; SMEX (@SMEX). X post. 3:13 am. February 6, 2023. <https://x.com/SMEX/status/1622523800704221187>; Cloudflare (@CloudflareRadar). X post. 7:23 am. Jun 15, 2023. <https://x.com/CloudflareRadar/status/1669319814869860352>; Cloudflare (@CloudflareRadar). X post. 9:06 am. July 15, 2023. <https://x.com/CloudflareRadar/status/1680217252971401216>; Cloudflare (@CloudflareRadar). X post. 9:35 pm. August 20, 2023. <https://x.com/CloudflareRadar/status/1693451780963618945>; OONI (2023). Iraq temporarily blocked Telegram. <https://explorer.ooni.org/findings/64077907701>; Cloudflare (@CloudflareRadar). X post. 9:10 pm. September 16, 2023. <https://x.com/CloudflareRadar/status/1703230002303476058>

²⁷⁴ Iraqi News Agency (2023). *Minister of Communications: We rejected a request to cut off internet service during ministerial exams.* <https://www.ina.iq/185179--.html>; Iraq Ministry of Education (وزارة التربية العراقية).

Facebook post. 9:31 am. May 29, 2023. <https://www.facebook.com/Iraq.Ministry.of.Education/posts/pfbid02vDYcpc8db8m2bgGkEvrfsCZGEoA4QkPLUG8A19Y6jgg5pckdB3qHs23VzLLBDDF2l>

²⁷⁵ Dyn Research (2016). *Syria goes to extremes to foil cheaters.* <https://web.archive.org/web/20161221030229/http://research.dyn.com/2016/08/syria-goes-to-extremes-to-foil-cheaters/>; Cloudflare Radar (@cloudflare). X post. 2:09 pm. June 25, 2023. <https://x.com/CloudflareRadar/status/1672970318401421312>; IODA (@IODA_live). X post. 12:48 pm. June 26, 2023. https://x.com/IODA_live/status/1673312245114195971

²⁷⁶ Cloudflare Radar (@cloudflareradar). X post. 12:26 pm. June 16, 2023. <https://x.com/CloudflareRadar/status/1669682739568693248>; SMEX (2023). *Internet shutdowns in Algeria: a blow to human rights and the national economy.* <https://smex.org/internet-shutdowns-in-algeria-a-blow-to-human-rights-and-the-national-economy/>

²⁷⁷ ZoomIT (2023). *Ministry of Communications: Internet will not be interrupted for any test.* <https://www.zoomit.ir/tech-iran/405167-internet-outage-final-exam/>

²⁷⁸ See Media Foundation for West Africa (2019). *Authorities Shut Internet during National Exams.* <https://www.mfwa.org/country-highlights/mauritania-shuts-internet-during-national-exams/>; Roya News (2021). *Instant messaging apps to be blocked in schools during Tajjhi exams: TRC.* <https://en.royanews.tv/news/28968/2021-06-20>

²⁷⁹ *Supra* note 51.

²⁸⁰ *Supra* note 70.

2023, expanding the list of social media apps banned in the country, which includes TikTok and Clubhouse.²⁸¹ The blocking of Grindr came as part of a wave of attacks — including calls to criminalize homosexuality by the country's conservative parliamentarians — against the country's LGBTQ+ community.²⁸² In recent times, Jordan has seen a hike in the level of hate speech and threats against members of the LGBTQ+ community and its supporters on social media sites.²⁸³

Authorities in Jordan also continue to block VPNs, a practice that has been ongoing for years.²⁸⁴ Many widely used VPN services and servers remain inaccessible, and further restrictions have been imposed under Jordan's new cybercrime law passed in 2023. Article 12 of the law stipulates penalties for IP address circumvention, making it more risky for people to use tools that allow them to bypass blocking, such as VPNs, proxies, and Tor.²⁸⁵ This comes at a time when Jordan is blocking more websites, such as the satirical news website AlHudood, which has been blocked since June 2023.²⁸⁶

When southern and central Türkiye and northern and western Syria were hit by series of earthquakes on February 6, 2023, which killed over 55,000 people, authorities in **Türkiye** began blocking access to social

media platform X (formerly Twitter), thereby denying people access to critical information regarding relief or humanitarian assistance.²⁸⁷ In an unrelated incident, just a few months later, in the lead-up to Türkiye's 2023 national elections, authorities issued threats of throttling against platforms for non-compliance with content removal demands. X publicly disclosed that Turkish authorities singled it out as the only platform not complying with removal requests, influencing X's decision to take action on the content.²⁸⁸

In September in **Libya**, access to the internet was disrupted for at least 42 hours following the flooding disaster in Derna, one of the cities hit hardest by floods that claimed at least 11,300 lives and displaced 43,000 others.²⁸⁹ Although the government said the internet disruption was a result of cut fiber optic cables, the shutdown occurred amid large protests demanding answers about the catastrophic flood and burst dams, and while authorities reportedly asked journalists to leave the city during these protests.²⁹⁰ Internet access was restored on September 19, following a wave of criticism against the government.²⁹¹ The incident only underscores the value of the internet and digital platforms as a critical lifeline for people to access information during crises.

²⁸¹ *Ibid.*; SMEX (2023). *Beyond Jordan's TikTok Ban*. <https://smex.org/beyond-jordans-tiktok-ban/>; JOSA (2021). *Blocking Clubhouse in Jordan: A Quick Analysis of Internet Censorship Methods in Use*. <https://www.josa.ngo/ar/blog/78>.

²⁸² Al-Monitor (2023). *Jordan's LGBTQ community faces increased attacks, including from Islamists*.

<https://www.al-monitor.com/originals/2023/07/jordans-lgbtq-community-faces-increased-attacks-including-islamists>

²⁸³ *Ibid.*

²⁸⁴ 7iber (2021). *About blocking of virtual private networks (VPN) in Jordan*. <https://www.7iber.com/technology/%D8%AD%D8%AC%D8%A8-%D8%A7%D9%84%D8%B4%D8%A8%D9%83%D8%A7%D8%AA-%D8%A7%D9%84%D8%A7%D9%81%D8%AA%D8%B1%D8%A7%D8%B6%D9%8A%D8%A9-%D8%A7%D9%8-4%D8%AE%D8%A7%D8%B5%D8%A9-vpn/>

²⁸⁵ *Supra* note 73. Access Now (2023).

²⁸⁶ Middle East Eye (2023). *Jordan blocks satirical news site AlHudood*.

<https://www.middleeasteye.net/news/jordan-blocks-satirical-news-site-alhudood>

²⁸⁷ Al Jazeera (2023). *Death toll climbs above 50,000 after Turkey, Syria earthquakes*.

<https://www.aljazeera.com/news/2023/2/25/death-toll-climbs-above-50000-after-turkey-syria-earthquakes>; *supra* note 59.

²⁸⁸ X Global Government Affairs Team (@GlobalAffairs). X post. 3:29 pm. May 15, 2023. <https://x.com/GlobalAffairs/status/1658208072215437314>; Reuters (2023). *Twitter objects to Turkish court orders after pre-election warnings*.

<https://www.reuters.com/world/middle-east/twitter-objects-turkish-court-orders-after-pre-election-warnings-2023-05-16/>

²⁸⁹ France 24 (2023). *UN says death toll at least 11,300 in Libya's flood-hit Derna*. <https://www.france24.com/en/live-news/20230917-aid-arrives-as-libya-cope-with-flooding-aftermath>; Front Page (2023). *Libya: Flood update Flash Update No.6 (21 September 2023) (as of 4pm local time)*. <https://www.unocha.org/publications/report/libya/libya-flood-update-flash-update-no6-21-september-2023-4pm-local-time>

²⁹⁰ Access Now (2023). *Libya floods: people need reliable internet now*. <https://www.accessnow.org/press-release/libya-floods-internet/>; BBC News (2023). *Libya flood: Derna mayor's house burnt down in protests*.

<https://www.bbc.com/news/world-africa-66849131>; Elizia Volkmann (@EliziaVolkmann). X post. 11:45 am. September 19, 2023.

<https://x.com/EliziaVolkmann/status/1704099303168352621>

²⁹¹ The New York Times (2023). *Residents see Signs of Crackdown on Dissent After Libya Floods*.

<https://www.nytimes.com/2023/09/21/world/middleeast/libya-floods-derna-crackdown.html>; LPTIC

(@LPTIC). Facebook post. 7:32 am. September 19, 2023. <https://www.facebook.com/LPTIC/posts/pfbid02P4cqLPpKF4RCz4rzqNyCjZvEGp7Mvp19iu8pytStZ59t8H7YvZTfqdwpPJ7gFe13!>

V. Fighting back in 2023: growth, support, solidarity, and resilience

With governments increasingly wielding internet shutdowns during active conflict to cover up heinous crimes against humanity, silence their critics, and marginalize and oppress people, **the fight against internet shutdowns is more important than ever.** Through collaboration, solidarity, awareness raising, and resilience to authoritarian regimes, the #KeepItOn coalition continues to fight internet shutdowns across all corners of the world.

With a membership of over 334 organizations across at least 106 countries worldwide, **our movement to push back against internet shutdowns and digital repression keeps growing stronger.** The coalition is made up of a diverse community of advocates and experts, working together to prevent, document,

and circumvent shutdowns, and to hold perpetrators to account. In particular, our relationship with the internet shutdowns measurement community — which provides technical evidence on disruptions — has expanded, enabling us to more rapidly detect, verify, gather evidence, and report on shutdowns happening around the world. We also made important strides in our efforts to galvanize support from governments, private companies, grassroots groups, academia, and the international community. All these efforts by diverse actors continue to demonstrate the importance of collaboration and coordination at the core of the growth of the #KeepItOn campaign. The following are just some examples of areas where we advanced our collective efforts in 2023:

Campaigns

#KeepItOn Election Watch

Since its launch in 2016, the #KeepItOn coalition has actively monitored high-risk elections. In 2023, Access Now and the #KeepItOn coalition identified 18 countries at risk and mobilized three governments to make proactive commitments to ensure unhindered access to internet and telecommunications services during elections.²⁹² We also galvanized support from the 39 governments in the Freedom Online Coalition, which issued a statement denouncing election shutdowns and urging governments to stop imposing them.²⁹³ Together with partners, we are continuing to monitor elections for shutdowns in 2024, a super election year.²⁹⁴

#NoExamShutdown

In 2023, we launched a dedicated campaign jointly with our partners SMEX and the Internet Society to increase momentum in advocating against exam-related shutdowns, particularly in the Middle East and North Africa region.²⁹⁵ Through the #NoExamShutdown campaign, we seek to mobilize efforts to prevent such shutdowns, and to effectively engage with governments to find alternative, rights-respecting solutions to prevent exam cheating.²⁹⁶

Shutdown Impact Stories Project

The impact of internet shutdowns on people and communities is unquantifiable. Through this project we continue to amplify the voices of victims and document the dangers of shutdowns and the repercussions for people's health and safety, education, and business. Over the years, we have gathered stories from around the world, including Bangladesh, Ethiopia, Iran, Sudan, Tanzania, Togo, and Uganda.²⁹⁷

²⁹² *Supra* note 13. Access Now (2023).

²⁹³ *Supra* note 15.

²⁹⁴ *Supra* note 7.

²⁹⁵ *Supra* note 51.

²⁹⁶ *Supra* note 271.

²⁹⁷ Access Now (2024). *Shutdown Stories Archives*. <https://www.accessnow.org/tag/shutdown-stories/>

	<p>In 2023, the Open Observatory of Network Interference (OONI) launched new OONI Explorer features for investigating internet shutdowns which integrated data from Internet Outage Detection and Analysis (IODA), Cloudflare Radar, and Google traffic data to enable people to more easily track and identify internet connectivity disruptions based on signals from various datasets. OONI also produced an outreach toolkit that was localized in five languages, making its measurement tools more accessible to more people, and added a feedback mechanism to improve the quality of OONI data.²⁹⁸</p>
<p>Measurement Tools</p>	<p>Since 2021, the IT service management firm Cloudflare has facilitated evidence-gathering for tracking of shutdowns globally. In 2023, they added a notifications feature to Cloudflare Radar, enabling anyone to get automatic notifications about confirmed outages (including shutdowns) and observed traffic anomalies (which can indicate a shutdown). The company also began to provide the public with direct updates on shutdowns using various digital platforms.²⁹⁹</p>
	<p>In 2023, IODA conducted applied research on the technical and political signatures of shutdowns to help those monitoring disruptions better distinguish between a government-ordered internet shutdown and other outages.³⁰⁰ This research sets a foundation for more effective monitoring and potential predictive analytics. IODA also improved the usefulness of its outage data by grading and color-coding shutdowns according to severity, now visible on its country and region outage maps.³⁰¹ Finally, the project developed new functionality to help researchers analyze shutdown signals and share IODA outage data and visualizations, improving people's capacity to verify, confirm, and advocate against shutdowns.</p>
<p>Circumvention Tools</p>	<p>Responding to the increasing crackdown on the use of virtual private networks (VPNs) and circumvention tools around the world, the Tor Project improved its censorship-resistant infrastructure by expanding its toolkit. The project introduced the Webtunnel and Conjure, tools to make it more difficult for censors to spy on website traffic or block "phantom" proxies without incurring significant collateral damage. They also updated the Tor Browser to make it easier for people to connect to bridges and keep their connection to the Tor network hidden. In addition to making its tools more user-friendly, Tor has closely collaborated with people and communities impacted by shutdowns and censorship to collect and share real-time, localized information on how to bypass censorship, translating the content into languages including Arabic, Swahili, and Chinese to enhance rapid response.³⁰²</p>

²⁹⁸ OONI (2023). New OONI Explorer features for investigating censorship through open data. <https://ooni.org/post/2023-new-explorer-features/>; see also OONI (2023). *OONI Outreach Kit*. <https://ooni.org/support/ooni-outreach-kit/>

²⁹⁹ Cloudflare (2023). *Traffic anomalies and notifications with Cloudflare radar*. <https://blog.cloudflare.com/traffic-anomalies-notifications-radar>

³⁰⁰ IODA (2023). *First Interdisciplinary, Longitudinal Study of Internet Shutdowns and Outages*. <https://ioda.inetintel.cc.gatech.edu/reports/interdisciplinary-longitudinal-study-of-shutdowns-and-outages/>

³⁰¹ IODA (2023). *IODA update: Design Standards + Outage Severity Map*. <https://ioda.inetintel.cc.gatech.edu/reports/ioda-update-designstandards-outagemap/>

³⁰² The Tor Project (2023). *2023: Year in Review: Tor Project*. <https://blog.torproject.org/2023-year-in-review/>

Legal Advocacy

Civil society continues to find success challenging the legality of shutdowns imposed by governments across the globe.

In 2023, Media Defence, together with local organizations, won a case against the government of Guinea at the Economic Community of West African States (ECOWAS) Community Court of Justice for imposing internet shutdowns in the country during protests in 2020 and 2021.³⁰³ This is the third time the ECOWAS Court has ruled against states imposing internet shutdowns and declared the disruptions unlawful, following successful challenges to shutdowns in Togo in 2020 and Nigeria in 2022.³⁰⁴ There are also pending cases against the government of Senegal at the ECOWAS Court, following Senegal's decision to shut down mobile internet access on several occasions in 2023 to quell protests.³⁰⁵

Cases filed by the Coalition against Internet Shutdowns in Kazakhstan are pending against three telcos in the district courts of Almaty, challenging the January 2022 shutdowns in the country.³⁰⁶

In addition, courts in India and Pakistan have denounced the use of shutdowns and, in some instances, demanded an end to ongoing disruptions.³⁰⁷

Although these legal challenges and rulings have not brought an end to the use of shutdowns, they reinforce the norm that shutdowns violate international law, and serve as important legal precedents for Access Now, the #KeepItOn coalition, and our partners to continue pushing back against shutdowns in courts.

Coalition Resources and Capacity Building

Since its launch in 2022, the **Advocacy Assembly Shutdown Academy** has supported the global fight against shutdowns by empowering people with the skills, tools, and resources to join the battle.³⁰⁸ The academy launched 10 courses on shutdowns and created a mentorship program to train people and communities impacted by or interested in learning about internet shutdowns.³⁰⁹ They made courses available in English, French, Spanish, Arabic, Persian, Portuguese, and Swahili.

³⁰³ *Supra* note 89.

³⁰⁴ Access Now (2022). *ECOWAS Court upholds digital rights, rules 2017 internet shutdowns in Togo illegal*. <https://www.accessnow.org/press-release/internet-shutdowns-in-togo-illegal/>; Access Now (2022). *ECOWAS Court victory: Twitter ban in Nigeria declared unlawful*. <https://www.accessnow.org/press-release/ecowas-court-nigeria-unlawful-twitter-ban/>

³⁰⁵ Media Defence (2023). *Media Defence and SLS's Rule of Law Impact Lab File Case Before ECOWAS Court Challenging Senegal Internet shutdowns*. <https://www.mediadefence.org/news/senegals-internet-shutdowns/>

³⁰⁶ Access Now (2022). *Timeline: Kazakhstan internet shutdowns aim to crush protests, hide state violence*. <https://www.accessnow.org/kazakhstan-internet-shutdowns-protests-almaty-timeline-whats-happening/>; Eurasian Digital Foundation (2023). *Coalition against Internet shutdowns in Kazakhstan filed claims*. <https://shutdown.kz/works/claims-against-telecom/>

³⁰⁷ The Times of India (2024). *Manipur Internet Ban News: Manipur high court steps in to partially restore internet connectivity*. <https://timesofindia.indiatimes.com/city/imphal/manipur-high-court-steps-in-to-partially-restore-internet-connectivity/articleshow/105031873.cms>; see also Live Law (2023). *Manipur High Court Orders State To Lift Internet Ban On Leased Line Connections; Fiber Internet To Be Restored On Case-To-Case Basis*. <https://www.livelaw.in/high-court/manipur-high-court/manipur-high-court-internet-ban-lift-restrictions-safeguards-ftth-connections-232273>; SAMAA TV (2024). *SHC again orders immediate restoration of internet services, social media*. <https://www.samaa.tv/2087310116-shc-again-orders-immediate-restoration-of-internet-services-social-media>

³⁰⁸ Advocacy Assembly (2023). *Advocacy Assembly's Shutdown Academy 2023 in Review*. <https://advocacyassembly.org/en/news/247>

³⁰⁹ Advocacy Assembly (2023). *Ten Courses to Demystify and Combat Internet Shutdowns*. <https://advocacyassembly.org/en/news/243>

VI. Recommendations for stakeholders

The findings of this report underscore that all stakeholders must act urgently to halt the growing weaponization of internet shutdowns and work together to address their devastating impact on human rights.

In 2023, people were targeted with an unprecedented number of conflict-related shutdowns. The international community has not responded consistently from one conflict to another, and has generally failed to sustain efforts to help people who have been deliberately cut off from the world and are in dire need of emergency and humanitarian assistance. **To address the use of shutdowns in conflict-affected areas, we call on all stakeholders to take the following actions:**³¹⁰

► Parties to these conflicts should:

- Immediately cease the indiscriminate targeting of civilian objects, including medical, energy, and telecommunications infrastructure; more broadly, halt the indiscriminate use of explosive weapons in populated areas; and abstain from these practices going forward;³¹¹
- Ensure that the civilian population has access to accessible, reliable, open, and secure telecommunications infrastructure, enabling them to receive early warnings, communicate with humanitarian services and their loved ones, and otherwise exercise their fundamental human rights;
- Lift any blockades on and boost access to fuel, electricity, and other vital resources for civilian purposes, including powering essential infrastructure such as civilian cell towers; and
- Allow freedom of movement and safe passage to service providers working to repair damaged or malfunctioning telecommunications infrastructure.

► States should:

- Create, sustain, and protect digital mediation and cyber peacebuilding efforts, investing in civil society capacity to help reduce disruptions and ensure lasting resolutions;³¹²
- Ensure no military aid or other forms of assistance are used to enable digital repression, targeting of civilian infrastructure, or other humanitarian or human rights abuses;
- Strengthen language across UN resolutions to prioritize open, secure, stable, interoperable, and affordable telecommunications and internet connectivity as an essential service and foundation to ensure the continuation of critical services; and
- Take action individually and collectively, including through networks such as the Freedom Online Coalition (FOC), to urgently call out specific perpetrators of conflict-related shutdowns.

► Private actors should:

- Adopt policies and practices that identify, assess, and address the heightened human rights risks inherent in conflict-affected and high-risk areas, including in connectivity management, data integrity, and content governance, and even before a conflict occurs;³¹³
- Clearly communicate to users any limitations, restrictions, or changes to service they may experience and provide regular updates on system status;
- Preserve adequate documentation of any orders received to disrupt civilian telecommunications services or communications platforms, in particular where it may provide supporting evidence in trial against authorities for international crimes; and

³¹⁰ Targeted recommendations for individual conflict zones are available for Gaza, Ukraine, and Myanmar: *supra* note 236; *supra* note 10; *supra* note 149.

³¹¹ See ICRC (2024). *ICRC president: "We are witnessing a global and collective failure to protect civilians in armed conflicts"*. <https://www.icrc.org/en/document/global-and-collective-failure-to-protect-civilians-in-armed-conflict>.

³¹² See *supra* note 236.

³¹³ See Access Now (2023). *Tech and conflict: a guide for responsible business conduct*. <https://www.accessnow.org/guide/tech-and-conflict-a-guide-for-responsible-business-conduct/>; *supra* note 37.

- For investors and financial institutions linked to businesses operating in the impacted area, hold these businesses accountable for full transparency on their business conduct and the above requirements.

► **International actors should:**

- Provide technical resources, support, and assistance in rebuilding damaged communications infrastructure in a manner that is resistant and resilient to disruption;
- Ensure the timely and continued provision of shutdowns-resilient telecommunications equipment, personnel, and standards through bodies like the International Telecommunication Union (ITU), Global System for Mobile Communications (GSMA), and Emergency Telecommunications Cluster (ETC), not only for the humanitarian community but for the entire affected population;
- Recognize and fund solutions for alternative access to the internet and other communication channels as critical tools for protecting lives and fundamental human rights, and establish and commit resources for coordinated action plans to provide people in high-risk areas with alternative access to telecommunication services;³¹⁴
- Seek accountability through the International Court of Justice (ICJ), International Criminal Court (ICC), and other relevant courts, and ensure jurists consider the role of internet shutdowns and other digital rights violations in the investigation of international crimes; and
- Ensure that UN-led investigations into ongoing conflicts include adequate reporting on digital rights violations, including internet shutdowns.

Internet shutdowns continue to pose a persistent threat to communities at risk around the world in moments when access to information is vital, from elections to protests to natural disasters. In all contexts, we call on stakeholders to take up the following recommendations:

📣 **All states should:**

- Adopt legislation that clearly prohibits disruptions to ICT networks and digital communication platforms, in accordance with international human rights standards;
- Unequivocally reject any proposals to ban digital platforms people rely on to exercise free expression, free assembly, and other fundamental rights;³¹⁵
- When addressing issues such as public safety or the spread of harmful content online, refrain from resorting to disproportionate tactics like internet shutdowns that further exacerbate harm, and instead consult with civil society and other stakeholders to develop effective and rights-respecting policy solutions;
- Leverage all appropriate diplomatic channels to sustain continuous, consistent pressure on authorities globally to lift ongoing shutdowns and to discourage additional offenses going forward; and
- Push tech and telecom companies to uphold human rights and hold them accountable when they fail to provide effective remedy for violations.

📣 **Authorities currently imposing internet shutdowns should:**

- Immediately and unequivocally remove all restrictions to accessing ICT services and online communications platforms.

📣 **In particular, the top repeating and emerging offenders named above in this report should:**

³¹⁴ See *supra* note 10. Access Now (2023); *supra* note 149.

³¹⁵ See *supra* note 76; Access Now (2023). *Slipping down the authoritarian hole: Nepal must lift the TikTok ban*. <https://www.accessnow.org/press-release/nepal-tiktok-ban/>; Vox (2024). *Banning TikTok would be both ineffective and harmful*. <https://www.vox.com/technology/24100104/banning-tiktok-us-senate-ineffective-and-harmful-bill>

- Engage in a process of open, meaningful consultation with civil society and other stakeholders to establish alternative strategies and strengthen safeguards for human rights;
- Implement effective independent oversight mechanisms to protect human rights and begin the process of rebuilding trust between authorities and communities who have experienced repeated harm from internet shutdowns and other abuses; and
- Establish and uphold clear mechanisms for remedy and redress for victims of past human rights violations.

📣 To countries that have previously implemented shutdowns but have since discontinued the practice, we applaud your change of course and encourage you to:

- Make public commitments to #KeepItOn going forward, including through adoption of binding policies to prevent the use of internet shutdowns at all levels; and
- Document and share learnings about the importance of leaving the practice behind and promoting reliable, affordable, open, and secure internet access.

📣 Private sector actors should:

- Address internet shutdowns in human rights policies, anticipate risks through due-diligence processes, and adopt mitigation and transparency measures;
- Explore all lawful measures to challenge the implementation of disruptions, and ensure the maximum level of transparency in management of such events;
- Include a commitment to preventing and mitigating adverse human rights impacts in

the context of internet shutdowns in public human rights policy statements, and establish operational policies and procedures adequately prepared for responding to shutdown requests, even in high-pressure situations;

- Preserve and facilitate the transmission of crucial evidence of potential human rights violations, including any attacks impacting personnel;
- Comply with the UN Guiding Principles on Business and Human Rights and OECD Guidelines to avoid causing or contributing to human rights violations when responding to requests to shut down the internet;³¹⁶
- Ensure full understanding of the human rights impact of all sanctions compliance decisions, and avoid over-compliance, which may inadvertently undermine the rights of the most vulnerable users;³¹⁷
- Share detailed information with civil society and other accountability partners when facing threatened or actual disruptions to services, including reasons provided by authorities;
- For social media and other communications platforms, take heed of the connection between content governance failures and increasing platform blocks, and strengthen policies and practices accordingly with guidance from civil society and impacted communities;³¹⁸
- Support collective efforts to prevent, document, and circumvent shutdowns by sharing traffic measurement and other relevant data with the #KeepItOn coalition and other stakeholders; and
- Facilitate the export, transfer, and activation of secure connectivity technologies, including alternatives to traditional telecommunications infrastructure, such as mesh networking or satellite internet, as safe and appropriate and in coordination with local actors.

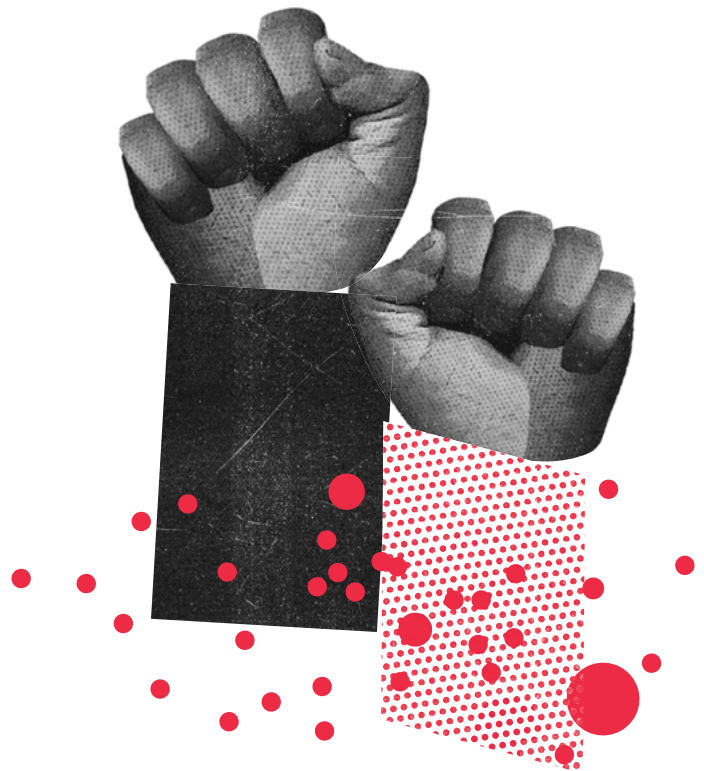
³¹⁶ OHCHR (2011). *UN Guiding Principles on Business and Human Rights*. https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf; OECD (2001). *The OECD Guidelines for Multinational Enterprises*. <https://www.oecd.org/investment/mne/1903291.pdf>; Access Now (2023). *Tech and conflict: a guide for responsible business conduct*. <https://www.accessnow.org/guide/tech-and-conflict-a-guide-for-responsible-business-conduct/>; Access Now (2012). *Telco Action Plan*. https://www.accessnow.org/wp-content/uploads/archive/docs/Telco_Action_Plan.pdf

³¹⁷ Access Now (2023). *When sanctions undermine human rights online*. <https://www.accessnow.org/sanctions-undermining-human-rights/>

³¹⁸ Access Now (2022). *Content governance in times of crisis: how platforms can protect human rights*. <https://www.accessnow.org/publication/new-content-governance-in-crises-declaration/>; see also *supra* note 37.

International organizations should:

- Identify and isolate the core group of repeat offenders, holding them accountable for violating international law using all diplomatic, economic, and legal measures available;
- Strengthen norms through continuing resolutions at all levels of the UN system, including the UN Security Council, as well as international and regional treaty bodies;
- Enforce existing resolutions on internet shutdowns to the greatest extent possible;
- For international courts and treaty bodies, where relevant, include shutdowns in evaluation of cases and allow individual and collective claims for redress; and
- Consider the digital dimension of threats, harm, and violence in developing the Draft articles on Prevention and Punishment of Crimes Against Humanity under discussion at the United Nations General Assembly Sixth Committee.³¹⁹



Civil society should:

- Join the **#KeepItOn** coalition;³²⁰
- Reach out to the **#KeepItOn** coalition for support from the network in your advocacy against internet shutdowns;³²¹
- Continue to collaborate in investigations, including through witness and victim support, and digital evidence collection and preservation, and include the digital dimension of harm when documenting human rights violations;
- Reach out to Access Now's Digital Security Helpline for direct assistance with digital safety or circumventing shutdowns;³²² and
- Consider sharing shutdown impact stories with the **#KeepItOn** coalition to strengthen advocacy against shutdowns.³²³

³¹⁹ International Law Commission (2019). *Draft articles on Prevention and Punishment of Crimes Against Humanity*. https://legal.un.org/ilc/texts/instruments/english/draft_articles/7_7_2019.pdf; General Assembly of the United Nations. Sixth Committee (Legal). <https://www.un.org/en/ga/sixth/>

³²⁰ Access Now. *#KeepItOn: Add Your Organization*. <https://www.accessnow.org/campaign/keepiton/#coalition>

³²¹ See, e.g., Access Now (2021). *Advocating to #KeepItOn during elections: what you can do*. <https://infogram.com/advocating-to-keepiton-during-elections-1h7k230351vkv2x?live>

³²² Access Now. *Digital Security Helpline*. <https://www.accessnow.org/help/>

³²³ Access Now. *#KeepItOn: Share Your Story*. <https://www.accessnow.org/campaign/keepiton/#take-action>



VII. Join us

As our coalition continues to grow and diversify, so will our capacity to turn the tide against the use of internet shutdowns as a tool for violence, authoritarianism, and oppression around the world. If you'd like to join us, we encourage you to reach out. All stakeholders are welcome as we work together to ensure shutdowns become a thing of the past.

CONTACT

For questions and more information, please visit:

<https://www.accessnow.org/keepiton/>

OR REACH OUT TO:

Felicia Anthonio

#KeepItOn Campaign Manager, Access Now

felicia@accessnow.org

Zach Rosson

#KeepItOn Data Analyst, Access Now

zach@accessnow.org

#KeepItOn

SHRINKING DEMOCRACY, GROWING VIOLENCE

Internet shutdowns in 2023



9/14/2021 Myanmar

Gabon

8/26/2023

Suriname

3/9/2023 Ukraine

2/26/2022 Russia

