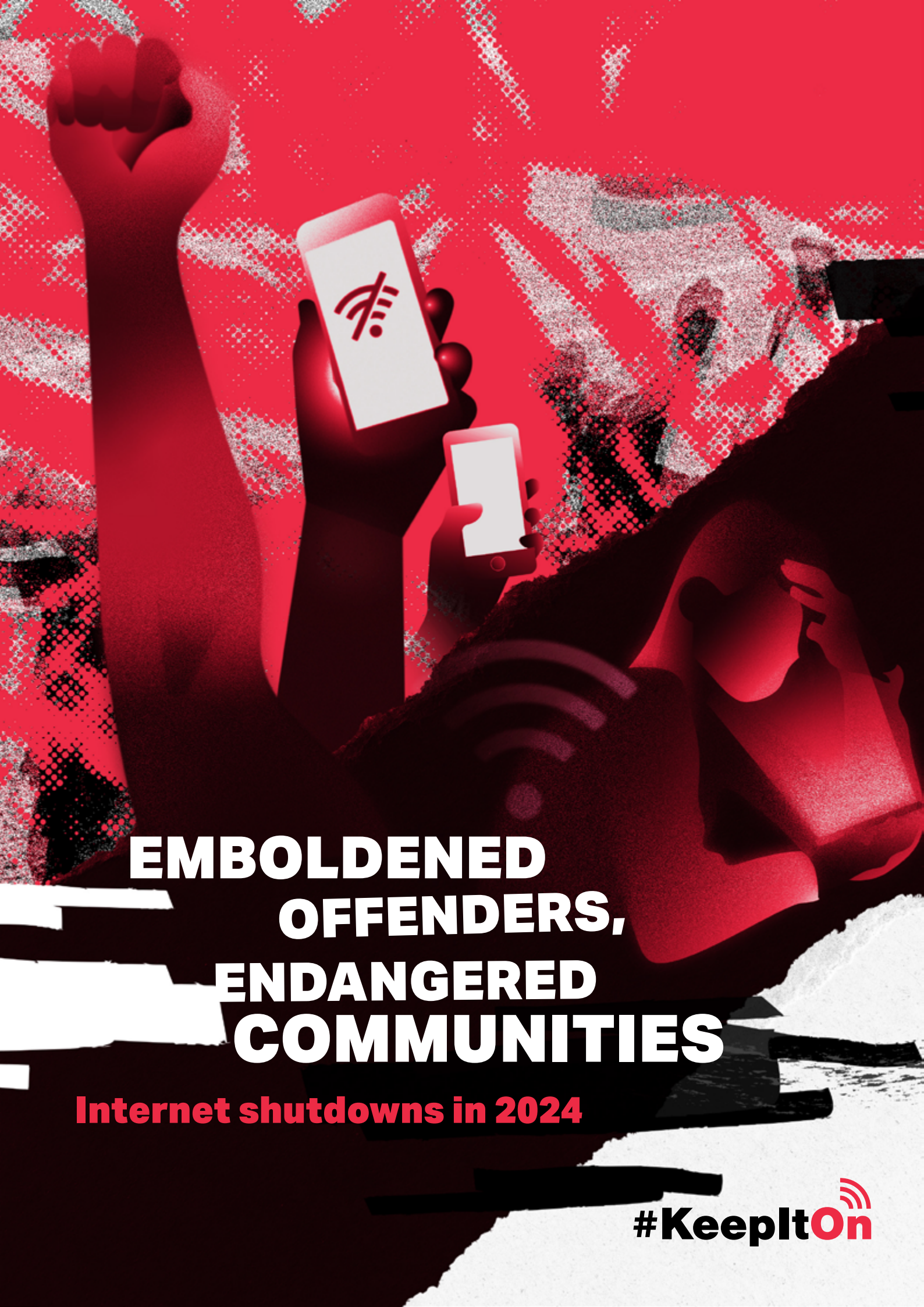


EMBOLDENED OFFENDERS, ENDANGERED COMMUNITIES

Internet shutdowns in 2024

#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 345 members from 106 countries around the world, ranging from civil society and human rights 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 Ángela Alarcón, Bridget Andere, Darika Bamrungchok, Raman Jit Singh Chima, Giulio Coppi, Marianne Díaz Hernández, Marwa Fatafta, Natalia Krapiva, Méabh Maguire, Namrata Maheshwari, Peter Micek, Kassem Mnejja, Wai Phyo Myint, Shruti Narayan, Laura O'Brien, Milica Pandzic, Alexia Skok, Donna Wentworth and Anastasiya Zhyrmont for their contributions. We would also like to thank Athan, Cloudflare, Digitally Right, Internet Outage Detection and Analysis (IODA), Internet Society, Kentik, Miaan Group, Myanmar Internet Project, Open Observatory of Network Interference (OONI), Software Freedom Law Centre India (SFLC.in), Yodet, 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.

A note on our data

This #KeepItOn report looks at incidents of internet shutdowns documented by Access Now and the #KeepItOn coalition in 2024. While we try to build a comprehensive dataset, 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. Our dataset can be accessed at 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.

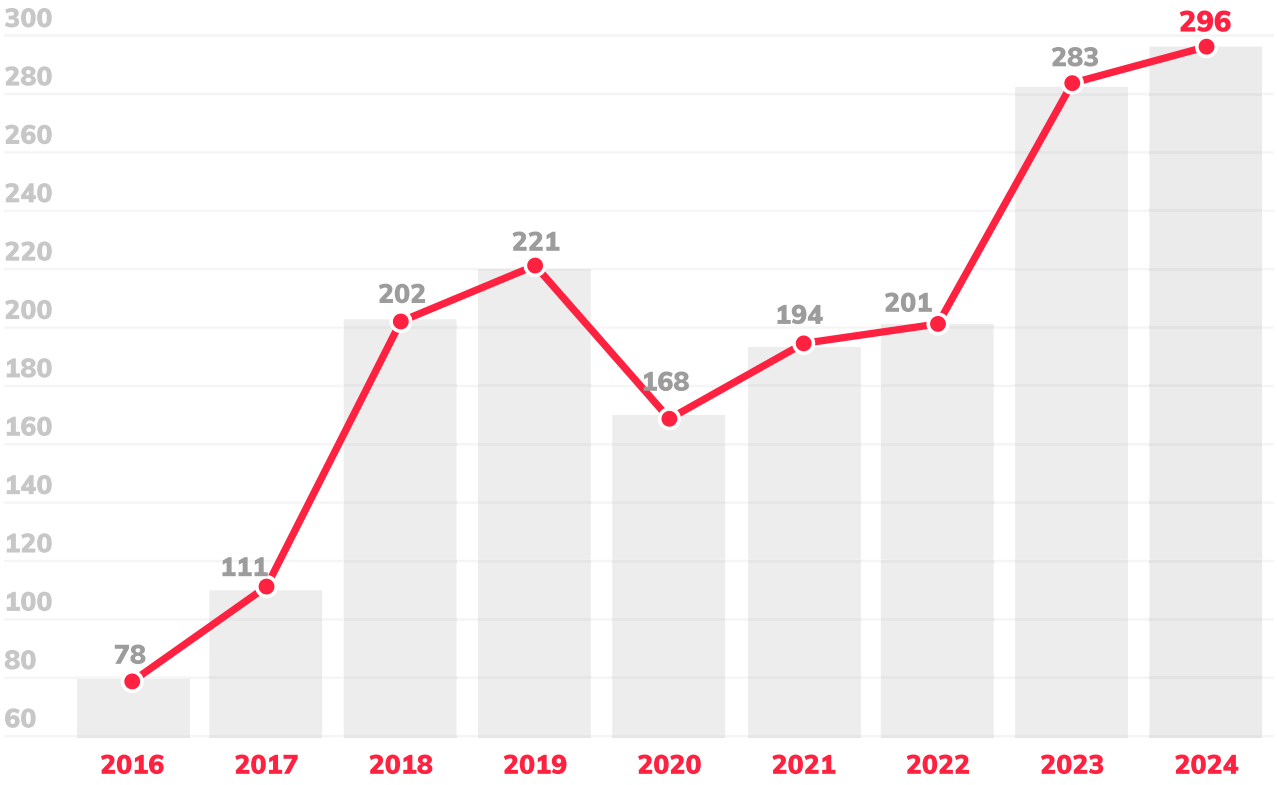
February 2025

Table of contents

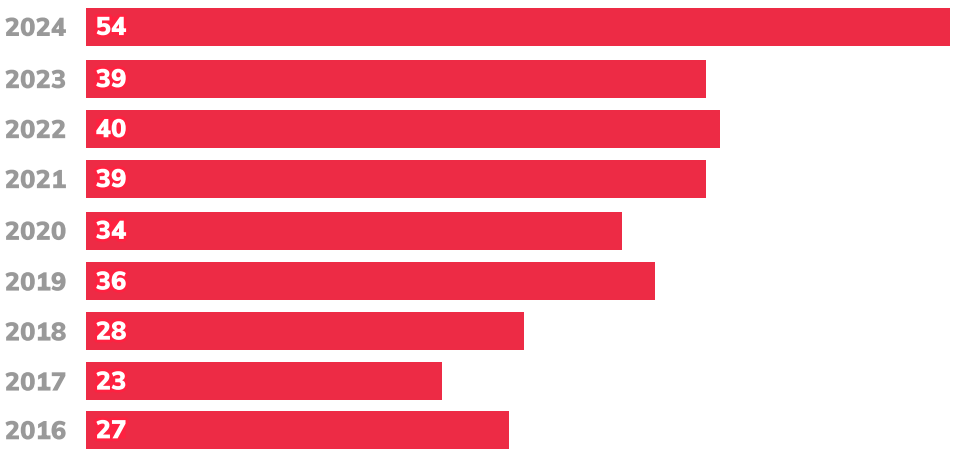
I. Internet shutdowns in 2024: a global overview

Internet shutdowns are never justified. Since 2016, the **#KeepItOn** coalition has documented shutdowns' clear harms, and helped to solidify international consensus that shutdowns are incompatible with human rights.[1] Despite these gains, perpetrators of internet shutdowns around the world continue to leverage this tactic to silence and isolate with impunity. The past year was no exception, with a steadily expanding group of offenders maintaining long-term shutdowns year over year, a cohort of notorious repeat offenders cutting access when people are most vulnerable, and a wave of new offenders setting dangerous new records.

Total number of shutdowns by year



Number of countries where shutdowns occurred by year



1 *See* Access Now. *#KeepItOn Campaign*. https://www.accessnow.org/campaign/keepiton/; UN Office for Digital and Emerging Technologies (2024). *Global Digital Compact*. https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf

In 2024, Access Now and the #KeepItOn coalition documented **296** shutdowns in **54** countries. This continues a sharp uptick in the number of total shutdowns after what was already a devastating, record-setting year in 2023 (**283**).[2] It also marks an alarming **35%** increase in the number of countries where people suffered internet shutdowns over the previous high in 2022 (**40**), including **seven** countries where governments joined the offender list for the first time. Breaking the record from prior years, we saw **47** shutdowns continue from 2024 into 2025, with **35** active shutdowns ongoing for more than a year as 2024 came to a close.[3]

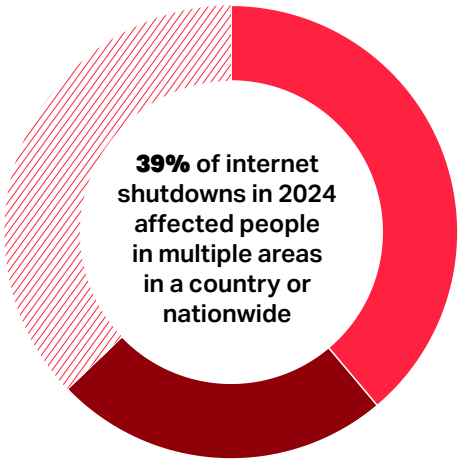
The **four** offenders with the highest total number of shutdowns accounted for **209** cases, or **71%** of the global total. In Myanmar, at least six perpetrators, led predominantly by the regime, imposed **85** shutdowns across the country, reflecting the unprecedented scale at which shutdowns have been deployed since the outbreak of civil war in 2021. Following closely behind was India with **84** shutdowns, which for the first time since 2018 was not the leading offender but still imposed an unacceptably high number of shutdowns as the world's largest democracy. Pakistan imposed **21** shutdowns, the highest ever for the country, and Russia imposed **19** shutdowns, including seven in Ukraine during its continued full-scale invasion.

The landscape for monitoring and pushing back on internet shutdowns has grown increasingly complex, introducing new challenges for attribution, accountability, and prevention. Additionally, internet shutdowns are in many cases becoming a cross-border issue. In 2024, people in **13** countries experienced **25** shutdowns implemented by a combination of eight perpetrators outside of their borders. Perpetrators have also shown more sophistication in their mechanisms for imposing and obfuscating shutdowns and thwarting circumvention attempts, including using techniques like jamming devices (**5**), cyberattacks (**5**), forced seizures and disabling of Low Earth Orbit (LEO) satellite internet terminals (**2**), and tampering of subsea cable landing stations (**1**). The role of the private sector also continues to evolve, as providers of alternative connectivity solutions like satellite internet gain influence over people's ability to connect,[4] and the companies that run social media platforms adopt content governance practices that may lead more governments to block or otherwise interfere with access to these platforms. Staggering numbers of shutdowns were imposed during conflict, protests, exams, and elections around the world, and **72** were linked to grave human rights abuses.[5]

As perpetrators break more records for shutdowns around the world, our calls to #KeepItOn must get stronger. Behind each of the **1,754** shutdowns since 2016 is a story of people and communities cut off from the world and each other, often during political upheaval, unrest, violence, and war. As evidenced by what we see in the 2024 data, the significant increase in internet shutdowns in 2023 was no fluke. In combination with censorship, surveillance, VPN bans, cable cuts, and other tools of digital authoritarianism, the increasing number of shutdowns reflects a world where internet access is consistently weaponized, restricted, and precarious.

One internet shutdown is one too many.

Geo-scopes of internet shutdowns in 2024



- **39%** (115) of shutdowns affected locations in more than one state, province, or region
- **37%** (110) of shutdowns only affected one city, county, or village
- **24%** (71) of shutdowns affected more than one city in the same state, province, or region

2 Access Now (2024). *Shrinking democracy, growing violence: Internet shutdowns in 2023.* https://www.accessnow.org/keepiton-2023-report.

3 Access Now (2023). *Weapons of control, shields of impunity: Internet shutdowns in 2022*. https://www.accessnow.org/keepiton-2022-report.

4 Access Now (2025). *Holding space for human rights: Improving the governance of satellite internet connectivity*. https://www.accessnow.org/wp-content/uploads/2025/02/Holding-Space-for-Human-Rights-a-bid-for-better-governance-of-satellite-internet-connectivity.pdf

5 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. These abuses must occur within the geographic area and time period of a verified shutdown to be counted as coinciding with a shutdown.

Where people experienced shutdowns in 2024

Myanmar: 85*
India: 84
Pakistan: 21
Russia: 13*
Ukraine: 7*
Palestine: 6*
Bangladesh: 5
Iraq: 5
Jordan: 4
Sudan: 4
Tanzania: 4*

Iran: 3
Senegal: 3
Syria: 3*
Türkiye: 3

Azerbaijan: 2
Chad: 2*
China: 2
El Salvador: 2
Ethiopia: 2
Kenya: 2
Mauritania: 2
Mozambique: 2
Oman: 2
Uganda: 2*
Venezuela: 2
Yemen: 2

Afghanistan: 1
Algeria: 1
Bahrain: 1*
Belarus: 1
Brazil: 1
Burundi: 1*
Comoros: 1
Cuba: 1
Equatorial Guinea: 1
Guinea: 1
Guinea-Bissau: 1
Indonesia: 1
Israel: 1*
Kazakhstan: 1
Kyrgyzstan: 1
Laos: 1*
Lebanon: 1
Malaysia: 1
Mauritius: 1
Nepal: 1
New Caledonia: 1
Nigeria: 1
Qatar: 1
Rwanda: 1*
Saudi Arabia: 1
Turkmenistan: 1
United Arab Emirates: 1

*Noting places where some shutdowns were imposed by parties outside the location. For more details on these cases, *see* **"Cross-border shutdowns"** on **pages 14-15.**

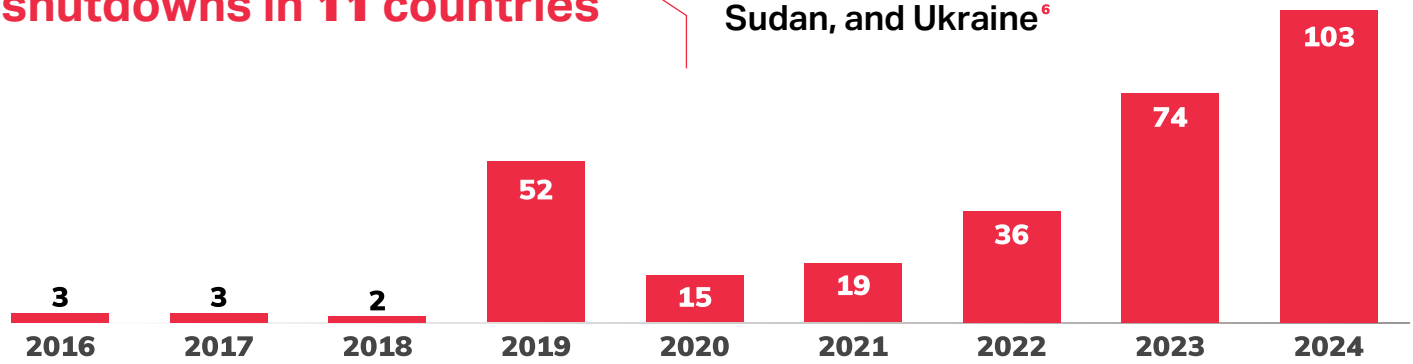
II. Triggers for internet shutdowns in 2024

Triggers of internet shutdowns refer to incidents and contexts during which authorities are more likely to impose internet shutdowns. Year after year, conflict, protests, elections, and exams have been the most consistent contexts in which authorities have imposed shutdowns.

Shutdowns during conflict

103 conflict-related shutdowns in 11 countries

Bahrain, Chad, Ethiopia, India, Israel, Myanmar, Pakistan, Palestine, Russia, Sudan, and Ukraine[6]



Following a violent year of war-related shutdowns in 2023,[7] conflict remained the leading trigger in 2024 and reached a new peak for the number of episodes recorded in a single year. Authorities used a wide range of tactics to shut down the internet during conflict, including but not limited to cutting fiber optic cables,[8] taking over internet service provider (ISP) offices,[9] jamming devices,[10] deploying cyberattacks to sabotage providers,[11] destroying power and telecommunications infrastructure,[12] and disabling or seizure of terminals for LEO satellite internet.[13] Regardless of the method, warring parties deliberately turned to internet shutdowns not only during fighting over controlled territory,[14] but also while laying siege or in situations of occupation, often as a collective punishment or to terrorize the population.[15] Through shutdowns military leaders enable war crimes and atrocities.[16]

6 Note: While there were no active conflicts ongoing in Bahrain and Chad in 2024, people in both countries experienced shutdowns as a result of a hacking group's cyberattacks in response to Bahrain's involvement in the ongoing conflict in Yemen and Chad's support for a party to Sudan's civil war, respectively. *See*: Africa Cybersecurity Magazine (2024). *Chad's largest telecommunications provider hit by cyberattack by Anonymous Sudan.* https://cybersecuritymag.africa/le-plus-grand-fournisseur-de-telecommunications-au-tchad-victime-de-cyberattaque-par-anonymous; The Hack Wire (2024). *Bahrain Telecom Hit by DDoS Attack from Anonymous Sudan.* https://www.thehackerwire.com/bahrain-telecom-hit-by-ddos-attack-from-anonymous-sudan/

7 *See supra note 2.* Access Now (2024).

8 The Nation (2024). *NBTC, police dismantle massive illegal cable network.* https://www.nationthailand.com/blogs/news/general/40043830

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

10 Ayeyarwaddy Times (2024). *Due to the installation of a bomb near the Pathein Regional Military Council office, phone and internet lines are frequently cut off in the nearby neighborhood.* https://ayartimes.com/?p=30643; Samaa (2024). *Mobile, internet services suspended across Pakistan for Muharram.* https://www.samaa.tv/2087317874-mobile-internet-services-suspended-across-pakistan-for-muharram

11 *See supra note 6.* Africa Cybersecurity Magazine (2024).

12 7amleh – The Arab Center for the Advancement of Social Media (2024). *7amleh Issues New Report on the Impact of War on Gaza's Telecommunications Infrastructure.* https://7amleh.org/2024/10/29/impact-of-war-on-gaza-s-telecommunications-infrastructure-en; RFA (2024). *TNLA cuts phone and internet lines after airstrike in Mogok.* https://www.rfa.org/burmese/news/tnla-cut-off-phone-internet-mogok-11142024221229.html.

13 The Hindu (2024). *Agencies probe seizure of Starlink devices in Manipur.* https://www.thehindu.com/news/national/agencies-probe-seizure-of-starlink-devices-in-manipur/article68996996.ece,

14 *See supra note 9.* Access Now (2024).

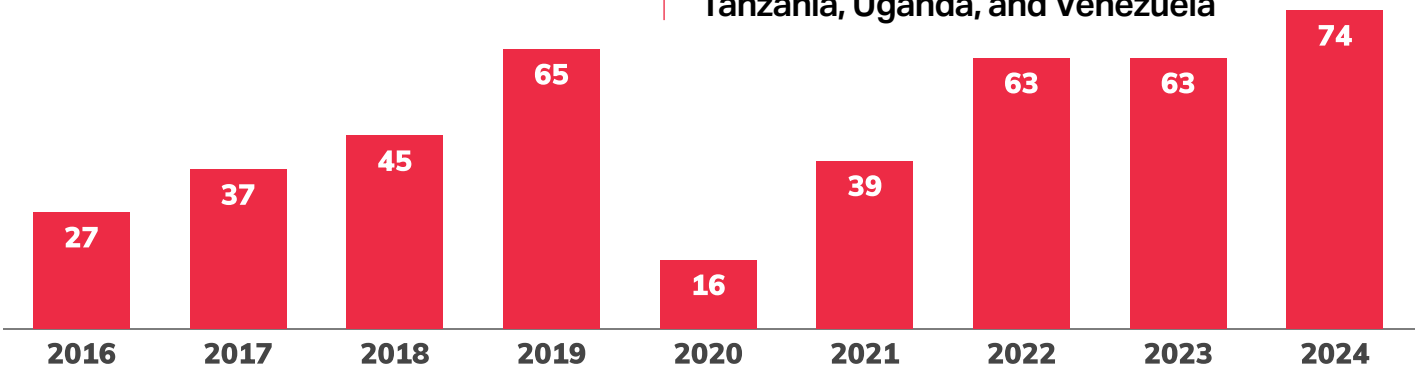
15 Reuters Institute and University of Oxford (2024). *Palestinians struggle to connect and get news amid digital shutdowns in Gaza: "Without the internet everything stops."* https://reutersinstitute.politics.ox.ac.uk/news/palestinians-struggle-connect-and-get-news-amid-digital-shutdowns-gaza-without-internet; NBC News (2023). *Israel promises a 'complete siege' of the Gaza Strip. What could that look like?* https://www.nbcnews.com/news/world/israel-promises-complete-siege-gaza-strip-look-rcna119552

16 Access Now (2023). *Evading accountability through internet shutdowns: trends in Africa and the Middle East.* https://www.accessnow.org/wp-content/uploads/2023/03/Evading-accountability-through-internet-shutdowns.pdf

Shutdowns during protests and instability

74 shutdowns in 24 countries during protests

Bangladesh, Burundi, Chad, Comoros, Cuba, Equatorial Guinea, Guinea-Bissau, France (in New Caledonia), India, Iran, Jordan, Kenya, Kazakhstan, Mauritania, Mozambique, Nigeria, Pakistan, Russia, Rwanda, Senegal, Syria, Tanzania, Uganda, and Venezuela



The world saw a surge of anti-government protests in 2024, with 166 cases documented across 76 countries according to the Carnegie Endowment's Global Protest Tracker.[17] From Senegal to Pakistan, Venezuela to Mozambique, authorities wielded internet shutdowns to quell protests, stifle dissent, disrupt independence movements, and suppress fundamental rights. Large-scale protests challenging undemocratic policies,[18] fraudulent election outcomes,[19] economic hardships,[20] and corruption[21] were met with **74** shutdowns across **24** countries, the highest number of protest-related shutdowns in a single year in our records to date.

Authorities in France,[22] Equatorial Guinea,[23] and Pakistan[24] used shutdowns in their attempts to quell self-determination protests and silence marginalized groups, such as the Indigenous Kanak population of New Caledonia, the Annobónese of Equatorial Guinea (including environmental activists), and the Baloch people of Pakistan. Despite oppression and targeted shutdowns, activism among these groups and many others remained steadfast. Although authorities in **60** countries have imposed shutdowns during protests since 2016, this tactic does not appear to suppress mobilization[25] and may only amplify violence.[26]

Shutdown stories *See page 16*
Read the testimony from those affected by shutdowns during protests.

17 Carnegie Endowment for International Peace (2025). *Global Protest Tracker.* https://carnegieendowment.org/features/global-protest-tracker?lang=en

18 Amnesty International (2024). *What is happening at the quota-reform protests in Bangladesh?.* https://www.amnesty.org/en/latest/news/2024/07/what-is-happening-at-the-quota-reform-protests-in-bangladesh/

19 Access Now (2024). *Maduro must #KeepItOn in times of protest and unrest.* https://www.accessnow.org/press-release/maduro-keepiton-during-protest-and-unrest/

20 Reuters (2024). *Nigeria's president calls for end to protests against economic hardship.* https://www.reuters.com/world/africa/nigerias-president-calls-end-protests-against-economic-hardship-2024-08-04/

21 Al Jazeera (2024). *'Kenya is not asleep anymore': Why young protesters are not backing down.*https://www.aljazeera.com/features/2024/7/24/kenya-is-not-asleep-anymore-why-young-protesters-are-not-backing-down

22 Access Now (2024). *First-time culprit: France blocks TikTok in New Caledonia.* https://www.accessnow.org/france-blocks-tiktok-new-caledonia/

23 Access Now (2024). *#KeepItOn: Equatorial Guinea authorities must end internet shutdown and other human rights abuses in Annobón.* https://www.accessnow.org/press-release/keepiton-equatorial-guinea-authorities-end-internet-shutdown-in-annobon/

24 The Tribune (2025). *Internet shutdown attempts to silence voices ahead of Baloch Genocide Remembrance Day: Mahrang Baloch.* https://www.tribuneindia.com/news/world/internet-shutdown-attempts-to-silence-voices-ahead-of-baloch-genocide-remembrance-day-mahrang-baloch/

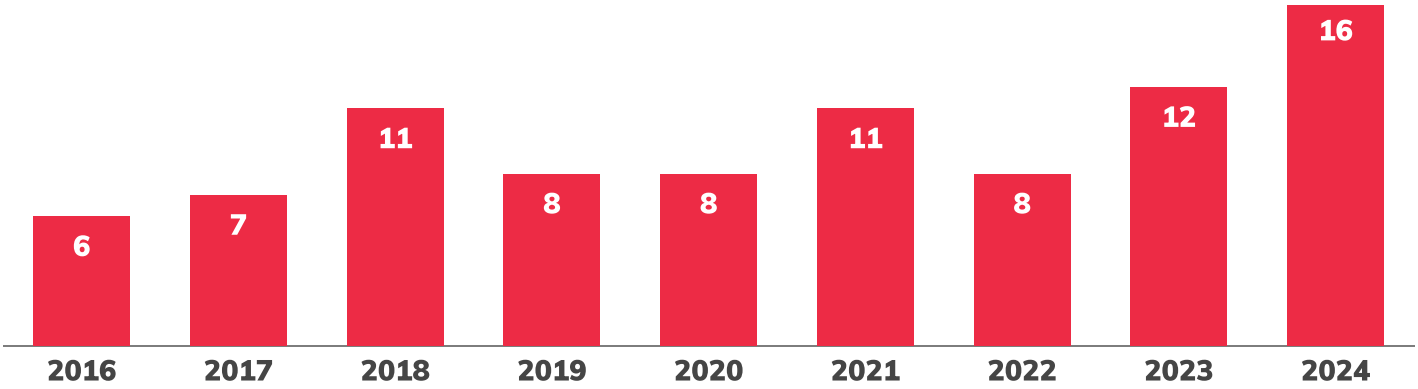
25 BBC (2023). *Pakistan shut down the internet - but that didn't stop the protests.* https://www.bbc.com/news/world-asia-65541769

26 Access Now (2024). *Violence & internet shutdowns in 2023: the worst year on record.* https://www.accessnow.org/press-release/keepiton-internet-shutdowns-2023/; *See also,* Hertie School (2024). *Anita Gohdes discusses her new book on Digital Repression.* https://www.hertie-school.org/en/news/allcontent/detail/content/anita-gohdes-discusses-her-new-book-on-digital-repression-on-elliott-schools-pomeps-podcast. ("… Gohdes noted that internet shutdowns typically accompany military offensives, contradicting theories that shutdowns prevent violence…").

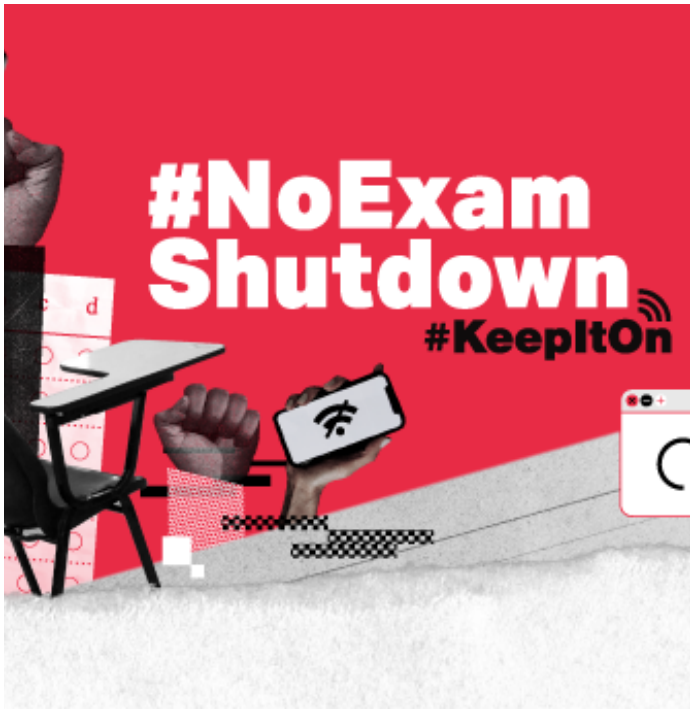
Shutdowns during exams

16 shutdowns in 7 countries to "prevent exam cheating"

Algeria, Jordan, Kenya, India, Iraq, Mauritania, and Syria



In 2024, we recorded **16** exam-related shutdowns in **seven** countries (Algeria, India, Iraq, Jordan, Kenya, Mauritania, and Syria), the highest annual total for this type of shutdown in our records. Authorities in the Middle East and North Africa (MENA) region were the lead perpetrators globally,[27] accounting for **10** such shutdowns across **five** countries, despite repeated calls for #NoExamShutdown.[28] Iraqi authorities imposed recurring two-hour long shutdowns during **five** exam periods across the country. Jordan blocked access to messaging apps during the 2024 Tawjihi exams, backsliding after a year of reprieve in 2023.[29] Elsewhere, Kenya once again blocked Telegram for **three** weeks in November during national secondary school exams,[30] and India matched their 2018 record, imposing **five** exam-related shutdowns during government job placement exams.[31] There were also promising developments, however. Iran[32] and Sudan[33] refrained from exam-related shutdowns in 2024, despite their past history of imposing such shutdowns.[34] Notably, the ongoing conflict in Sudan prevented the majority of high school students — estimated at 400,000 in 2024[35] — from taking exams in the first place, as the journey to examination centers posed serious safety risks.



27 Access Now (2024). *Why #NoExamShutdown should be every country's class motto.* https://www.accessnow.org/why-noexamshutdown-should-be-the-motto/

28 Access Now (2023). *#NoExamShutdown campaign page.* https://www.accessnow.org/campaign/no-exam-shutdown/

29 *See supra note 27.* Access Now (2024).

30 Access Now (2024). *#KeepItOn: authorities in Kenya must restore access to Telegram and protect people's rights.* https://www.accessnow.org/press-release/authorities-in-kenya-must-restore-access-to-telegram/

31 Internet Society (2024). *Internet shutdowns.* https://pulse.internetsociety.org/shutdowns/internet-services-suspended-in-jharkhand-india-21-september-2024

32 *See supra note 27.* Access Now (2024).

33 Ministry of Culture and Information (2024) on X. https://x.com/gov_moci/status/1872894493499719776?t=J3lh4KMyL5C6X2GdBORn7w&s=19

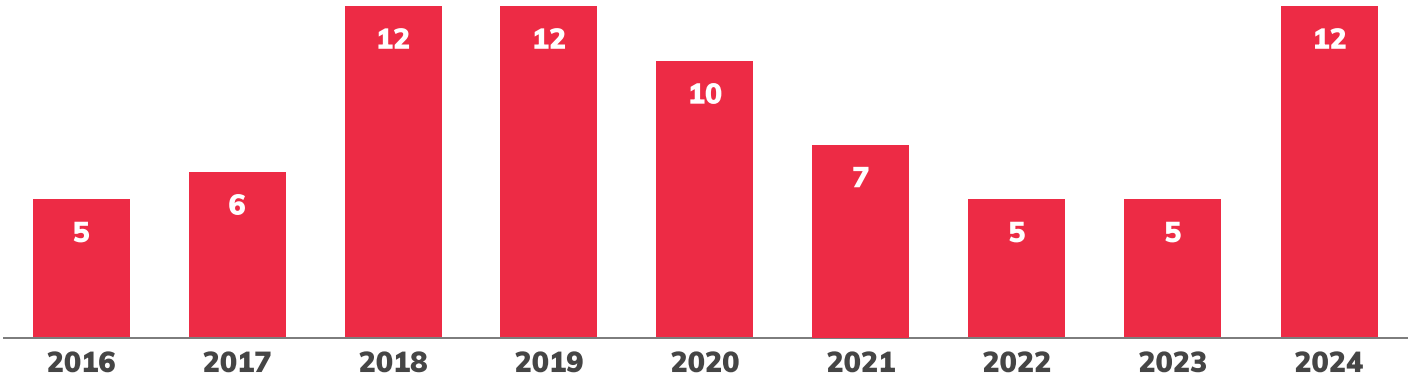
34 Cloudflare (2021). *Sudan's exam-related Internet shutdowns.* https://blog.cloudflare.com/sudans-exam-related-internet-shutdowns/

35 Sudan Tribune (2024). *400,000 Sudanese students miss high school exams due to conflict.* https://sudantribune.com/article295760/

Shutdowns during elections

12 election-related shutdowns in 8 countries

Azerbaijan, Comoros, India, Mauritania, Mozambique, Pakistan, Uganda, and Venezuela



The year 2024 was deemed a "year of democracy,"[36] as elections took place in at least 64 countries to determine representatives for nearly half of the world's population.[37] We recorded **12** election-related shutdowns in **eight** countries after a years-long decrease, documenting the highest yearly total of such shutdowns since 2019. In Uganda, a Facebook block implemented during elections in 2021 was still in place in 2024, and as of early 2025, remains ongoing. The other **seven** countries that imposed election-related shutdowns (Azerbaijan, Comoros, India, Mauritania, Mozambique, Pakistan, and Venezuela) were among **23** that we had flagged as high-risk for the 2024 #KeepItOn Election Watch[38] campaign.

Despite these troubling developments for human rights and democracy, there were also signs of progress and important milestones of support for the fight to #KeepItOn. In January 2024, authorities in Bangladesh publicly committed[39] to ensuring unfettered access to the internet throughout the election, and followed through, although they later regressed, imposing a punishing string of shutdowns during protests.[40] In March, following joint advocacy with our coalition partner, Paradigm Initiative,[41] the African Commission on Human and Peoples' Rights adopted a landmark resolution[42] urging member states to refrain from imposing internet shutdowns during elections. And in November, authorities in Mauritius ordered a 10-day, sweeping social media ban ahead of their election, but after facing intense pressure from local civil society and community groups, rescinded the order the following day.[43]

Shutdown stories ➨*See page 16*
Read the testimonies from people suffering shutdowns during political unrest.

36 Global Coalition for Tech Justice (2024). *#YearOfDemocracy: Protect people and elections, not Big Tech.* https://yearofdemocracy.org/

37 Time (2023). *The Ultimate Election Year: All the Elections Around the World in 2024.* https://time.com/6550920/world-elections-2024/

38 Access Now (2024). *2024 elections and internet shutdowns watch.* https://www.accessnow.org/campaign/2024-elections-and-internet-shutdowns-watch/

39 The Daily Star (2024). *Internet and mobile network to be fully operational on election day: EC Secy.* https://www.thedailystar.net/tech-startup/news/internet-and-mobile-network-be-fully-operational-election-day-ec-secy-3508161

40 AP (2024). *Internet is still down in Bangladesh despite apparent calm following deadly protests.* https://apnews.com/article/bangladesh-campus-violence-quota-hasina-3f9a3903487e89f1a0bc0d596d91b89b

41 Paradigm Initiative (2024). *Paradigm Initiative Welcomes ACHPR Resolution 580 on Internet Shutdowns and Elections in Africa.* https://paradigmhq.org/paradigm-initiative-welcomes-achpr-resolution-580-on-internet-shutdowns-and-elections-in-africa/

42 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/en/adopted-resolutions/580-internet-shutdowns-elections-africa-achprres580-lxxvii

43 Access Now (2024). *#KeepItOn Mauritius: global coalition urges first-time offender to end crackdown on social media.* https://www.accessnow.org/press-release/keepiton-mauritius-end-crackdown-on-social-media/

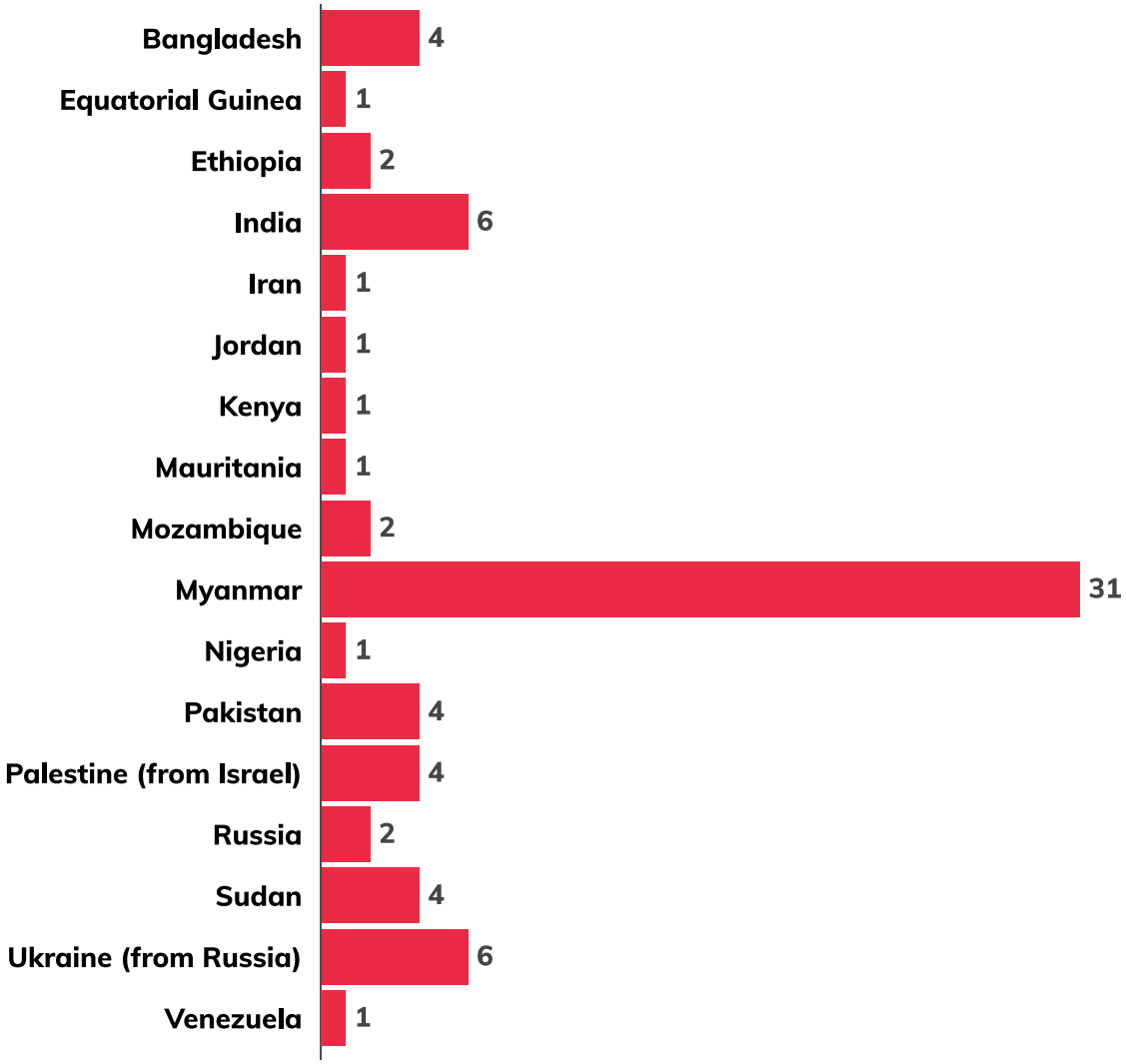
#KeepItOn

III. New and continuing trends in 2024

Shutdowns shrouding grave human rights abuses and violence

In the continuation of a devastating and horrific multi-year trend, shutdowns were rampant during times of violence in 2024. Authorities imposed shutdowns to quell protests or to cover up their own abuses, stoking fear and uncertainty and cutting off access to life-saving information, deepening the impact of the violence.[44] We documented a record-high **72** shutdowns coinciding with grave human rights abuses,[45] such as murder, torture, rape, or apparent war crimes and atrocities,[46] in **17** countries. Shrouded by internet shutdowns, governments, militaries, and police or security forces in these countries killed protesters,[47] targeted civilians through airstrikes on villages, hospitals, and schools,[48] and blockaded cities from receiving humanitarian aid.[49]

Shutdowns coinciding with grave human rights abuses



44 Human Rights Watch (2024). *Mozambique: Post-Election Internet Restrictions Hinder Rights.* https://www.hrw.org/news/2024/11/06/mozambique-post-election-internet-restrictions-hinder-rights

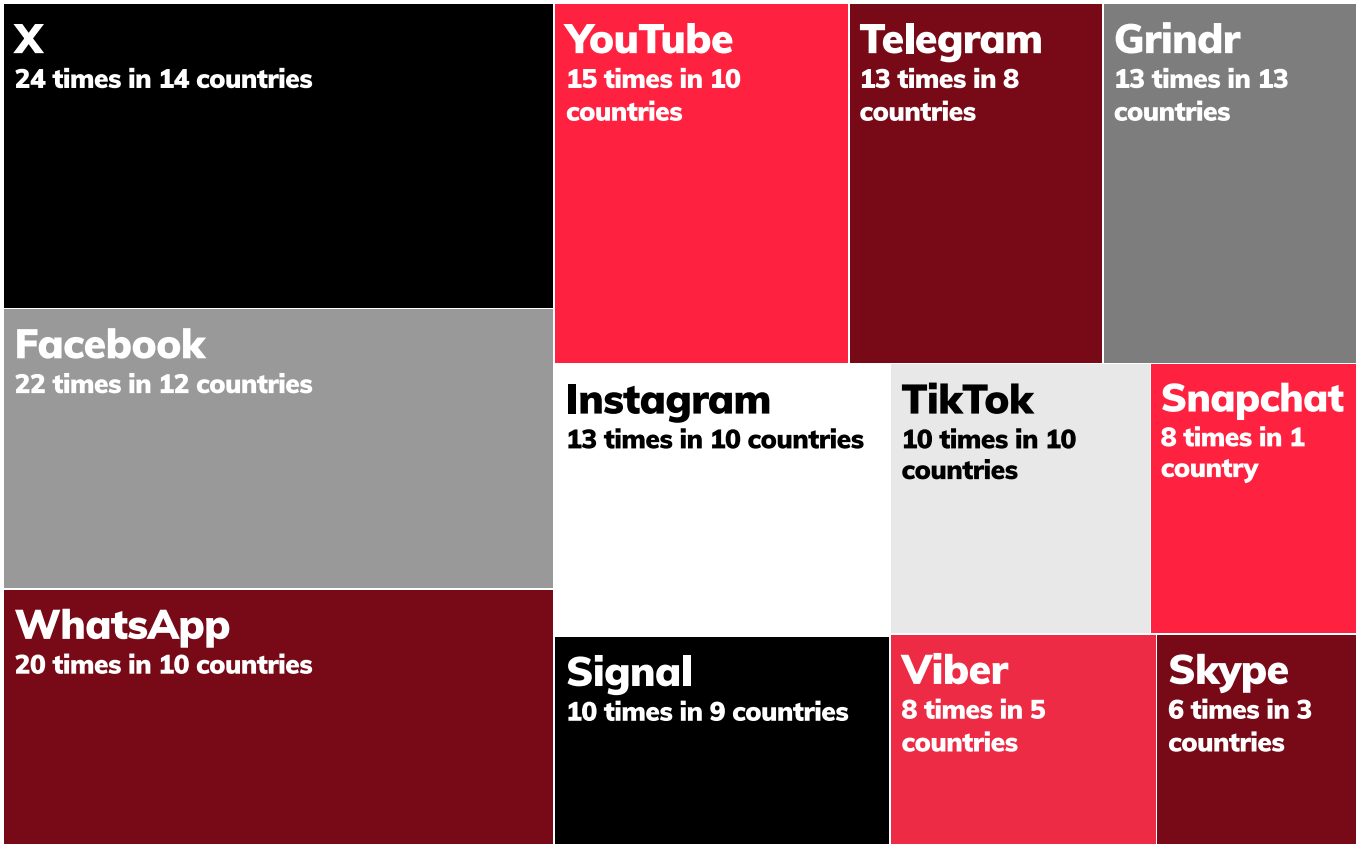
45 *Supra note 5.*

46 *See,* e.g., Access Now (2024). *MENA in 2023: internet shutdowns soar amid unprecedented violence and war.* https://www.accessnow.org/press-release/mena-keepiton-internet-shutdowns-2023-en/

47 Al Jazeera (2024). *Bangladesh student protests over jobs escalate, telecoms disrupted.* https://www.aljazeera.com/news/2024/7/19/bangladesh-student-protests-over-jobs-escalate-telecoms-disrupted

48 The Irrawaddy (2024). *Myanmar Junta Destroys 35 More Hospitals, Clinics in Two Months: NUG.* https://www.irrawaddy.com/news/burma/myanmar-junta-destroys-35-more-hospitals-clinics-in-two-months-nug.html

49 Al Jazeera (2024). *Updates: Israel continues to block Gaza aid; heavy rains flood tent camps.* https://www.aljazeera.com/news/liveblog/2024/12/31/live-seventh-palestinian-freezes-to-death-in-gaza-amid-israeli-siege



The widespread use of platform blocks

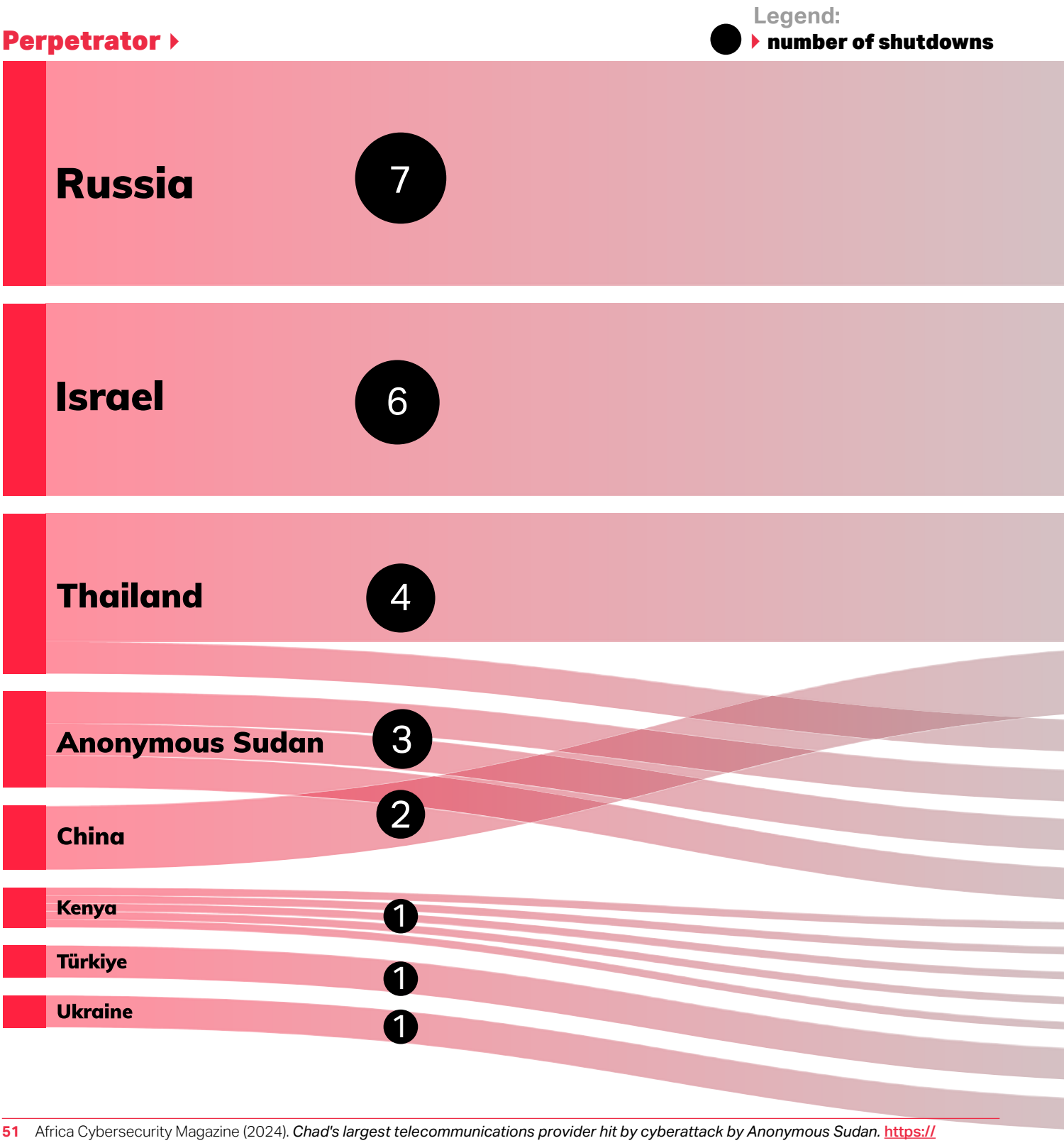
The blocking of communications platforms surged in 2024, with **71** blocks in **35** countries, an increase from **53** blocks in **25** countries in 2023 and exceeding the previous record high of **57** blocks in **28** countries in 2019. Authorities imposed this type of shutdown to control the flow of information on popular platforms and target specific populations. There is a misconception that such sh utdowns minimize impacts or represent a more acceptable form of censorship than cutting off the internet entirely, but blocking platforms that are a central means for people and communities to access information and communicate is just as harmful as blanket internet shutdowns. Our records show that new offenders or those that have imposed fewer shutdowns often use platform blocks, and 2024 was no exception. **Four** of the **seven** new offenders in 2024 (El Salvador, Malaysia, Mauritius, and France in New Caledonia) imposed platform blocks exclusively, while countries with less frequent shutdowns (Kyrgyzstan, Mozambique) blocked platforms for the first time. These offenders contributed to the significant increase in platform blocks in 2024, as did a group of repeat offenders (Bangladesh, India, Jordan, Myanmar, Pakistan, Russia, Tanzania, Türkiye, and Venezuela) that combined shorter-term blocks with new indefinite blocks.[50]

X was the most blocked platform around the world in 2024, with **24** blocks in **14** countries, the highest number for the platform since 2019, when it was blocked **33** times. TikTok was blocked **10** times in **10** countries in 2024 compared to **six** times in **six** countries in 2023, with **three** countries maintaining active blocks from 2024 into 2025 (India, Jordan, and Kyrgyzstan). Finally, of the **52** total platforms blocked in some combination across **71** shutdown instances, Signal saw the highest spike in 2024, with **10** blocks in **nine** countries (Algeria, Bangladesh, China, Iran, Myanmar, Pakistan, Russia, Venezuela, and Yemen) compared to **two** blocks in **two** countries in 2023 (China, Iran). Every blocking of Signal, with the exception of the **two** in Bangladesh and one each in Algeria and Yemen, was ongoing into 2025.

50 The total number of platform blocks include ongoing blocks over multiple years, which are counted once for each year they're in place, as well as blocks that start and end within the same calendar year. *See* Access Now's Shutdown Tracker Optimization Project (STOP) FAQ, Question #4. https://www.accessnow.org/guide/shutdown-tracker-optimization-project/#faq

Cross-border shutdowns

In 2024, there were 25 cross-border shutdowns implemented by **eight** offenders, impacting people in **13** countries. We also saw a private actor group, Anonymous Sudan, publicly claim responsibility for cyberattacks aimed at disrupting connectivity, targeting aggressors or supporters of ongoing wars or conflict.[51] The spread of cross-border shutdowns in recent years to new conflict zones, colonized territories, or neighboring countries is deeply troubling and complicates efforts to achieve accountability and redress.

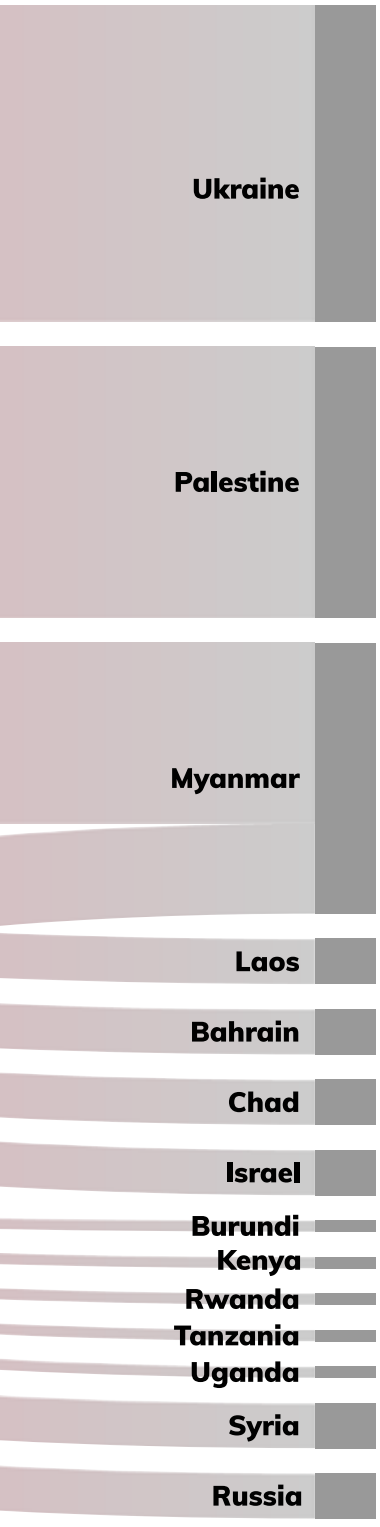


51 Africa Cybersecurity Magazine (2024). *Chad's largest telecommunications provider hit by cyberattack by Anonymous Sudan.* https://cybersecuritymag.africa/le-plus-grand-fournisseur-de-telecommunications-au-tchad-victime-de-cyberattaque-par-anonymous

Event(s) and context:

1. **Russia** continued its illegal full-scale invasion of Ukraine and in 2024 launched a cyberattack on Ukrainian ISPs, as well as deploying at least six sets of missile strikes targeting energy infrastructure, all of which led to significant internet disruptions across Ukraine.[52]
2. **Israel** continued its onslaught on Gaza in 2024, including imposing internet shutdowns in areas where the Israeli Defense Forces (IDF) were focusing military action. The shutdowns, which have been documented since October 2023,[53] persisted throughout 2024, forcing people across Gaza offline, and coinciding with numerous documented atrocities and war crimes,[54] including mass displacement, military targeting of shelters and hospitals, cutting off humanitarian aid, and constant bombardments of civilians.[55]
3. **Thailand:** During the active conflict in Myanmar, Thai authorities ordered internet service and phone lines serving people in Myanmar to be disconnected. These actions were intended to curb cybercrime, but affected local residents, disconnecting those relying on Thai networks, including vulnerable populations trafficked to work in scam call centers.[56]
4. **Anonymous Sudan:** The hacker group took credit for three separate cyberattacks that caused shutdowns in three countries. These attacks were in protest of Bahrain's participation in a coalition opposing the Houthi in Yemen,[57] Chad's support of the Rapid Support Forces (RSF) in Sudan, and Israel's war on Gaza,[58] respectively.
5. **China:** Perpetrators cut off electricity, internet, and phone lines from Chinese providers into Myanmar, first disrupting service for the city of Laukkai and later all border crossings for Kachin and Shan states. People in these areas of Myanmar had relied on internet from Chinese providers to stay connected despite heavy fighting and the persistent shutdowns of junta-controlled networks.
6. **Kenya:** During heightened protests in Kenya, Kenya and four other countries lost connectivity for over seven hours. While telecommunication companies Safaricom and Airtel claimed the outage was as a result of damaged undersea cables,[59] the timing of the shutdown and relatively swift restoration of services suggests the disruption may have been a deliberate attempt by authorities to quell protests.[60]
7. **Türkiye:** Turkish authorities cut off internet access in parts of northern Syria during protests against Turkish policies.[61]
8. **Ukraine:** Ukrainian hackers carried out a cyberattack on Russian state media, including television, radio broadcasting, and the internet.[62]

Impacted country or territory



52 United Nations (2024). *Two Years after Russian Federation's Invasion, UN Remains Committed to Ukraine's Sovereignty, Independence, Assistant Secretary-General Tells Security Council.* https://press.un.org/en/2024/sc15588.doc.htm

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

54 OHCHR (2024). *UN Commission finds war crimes and crimes against humanity in Israeli attacks on Gaza health facilities and treatment of detainees, hostages.* https://www.ohchr.org/en/press-releases/2024/10/un-commission-finds-war-crimes-and-crimes-against-humanity-israeli-attacks

55 ReliefWeb (2024). *Israeli Military Escalates Bombing of Civilian Homes in Rafah Amid Threats of Ground Invasion [EN/AR].* https://reliefweb.int/report/occupied-palestinian-territory/israeli-military-escalates-bombing-civilian-homes-rafah-amid-threats-ground-invasion-enar

56 The Diplomat (2024). *Thailand Cuts Off Internet, Mobile Phone Connections to Myanmar Scam Hub.* https://thediplomat.com/2024/05/thailand-cuts-off-internet-mobile-phone-connections-to-myanmar-scam-hub/

57 The Hack Wire (2024). *Bahrain Telecom Hit by DDoS Attack from Anonymous Sudan.* https://www.thehackerwire.com/bahrain-telecom-hit-by-ddos-attack-from-anonymous-sudan/

58 Cloudflare Radar (2024) on X. https://x.com/CloudflareRadar/status/1764710841130131662

59 Nation (2024). *Safaricom CEO explains why there was a network outage on Tuesday.* https://nation.africa/kenya/business/safaricom-ceo-explains-why-there-was-a-network-outage--4670198

60 Access Now (2024). *Authorities in Kenya must immediately restore internet access and #KeepItOn throughout protests and unrest.* https://www.accessnow.org/press-release/kenya-protests-internet-shutdown/

61 Hawar News Agency (2024). *Internet cut by Turkish occupation in Syrian areas enters 7th day.* https://hawarnews.com/en/internet-cut-by-turkish-occupation-in-syrian-areas-enters-7th-day

62 Reuters (2024). *Hacker attack disrupts Russian state media on Putin's birthday.* https://www.reuters.com/technology/cybersecurity/russian-state-media-company-hit-by-unprecedented-cyberattack-kremlin-says-2024-10-07/

IV. Shutdown impact stories from 2024

Access to the internet is woven into the fabric of people's lives in countless ways, and shutdowns denying people that access have far-reaching impacts, including immediate harm to individuals' safety, long-term impacts on communities' economic stability, and so much more. The following stories are direct accounts from individuals who experienced internet shutdowns in 2024, anonymized for their safety.

I rely on the internet for nearly everything in my daily life, especially as I care for my paralyzed husband, who needs constant attention and medical assistance. When the shutdowns happened, I couldn't contact doctors, arrange for nurses, or even get urgent help if something went wrong. My children live abroad, and the money they send me is what keeps us afloat. But without internet access, money transfers are delayed, making it difficult for me to pay for medicine, food, or the nurses who help me care for my husband.

During times of political unrest, the streets become dangerous, and information spreads mostly online. Without internet access, I have no way to stay informed about what's happening. This isolation disrupts everything — our caregiving routines, our finances, and even our sense of safety. I can only plan and organize when the internet returns, leaving our lives at the mercy of these shutdowns.

Retired professor
Venezuela
testimony collected in January 2025

My story began when I was displaced along with my family from the north of Gaza to Rafah. My husband stayed behind in Gaza City. Five months have gone by, my son and I are still stuck in the same place, and my husband is somewhere else.

During the first two weeks of displacement, I could still contact my husband once in a while and make sure he was okay. However, everything changed when the internet went down in Northern Gaza. We lived in a state of fear for more than a month and a half. We had no news of my husband until he managed to regain access to the internet using an Israeli SIM card. He told us about how he was displaced and escaped death.

To this day, we're still in a state of worry because of the constant internet outages. I struggled to do my job as a journalist and eventually stopped working due to the internet shutdown. I faced financial difficulties as the war intensified and prices increased. I never imagined that a blackout in the Gaza Strip would last for months, nor that this suffering would persist without any resolution.

Journalist
Gaza Strip, Palestine
testimony collected in February 2024

YouTube is the main platform where I make a living and search for relevant content in my spare time. Almost every week I google about the state of YouTube blockings in Russia and try to predict the date when the final verdict will be made regarding it by the authorities. Discord is no less a significant loss for me, through it I used to communicate with my colleagues and friends who are in other countries. Other platforms cannot provide me with such quality of communication and comfort. Yes, I am still able to bypass all the blockings, but this only made me hate the censorship body that probably makes money with these blockings.

Content creator
Russia
testimony collected in January 2025

The mother who raised me lives in Annobón in critical health, along with a paralyzed son who is equally ill, not to mention sisters and nephews also in poor health. With the unrest, the military presence, and the abuses, it has been, and continues to be, extremely worrying not being able to communicate with them. It's incredibly disheartening and very frustrating to spend time trying to call. Sometimes, the call seems to go through, but you hear strange voices telling you the phone is being intercepted. It is sad and distressing.

Midwife
Annobón, Equatorial Guinea
testimony collected in October 2024

As an Open Source Intelligence Investigator (OSINT) analyst, the internet is essential to my work. My role involves conducting research, writing articles, and debunking disinformation on social media platforms like X.

On the day of the riots, I was in my office and found myself unable to book an online cab, make online transactions, or even contact my family to let them know I was safe. This was the longest [nationwide] internet shutdown in Pakistan's history. Despite the government's repeated claims that the internet had been restored, on the ground, it was not. Additionally, without any prior notice, the government blocked access to X citing national security reasons, which is crucial for my work.

Although we've tried to use VPNs to access X, the government's recent testing of a firewall purchased from China has made connecting to VPNs increasingly difficult. This has further hampered my ability to carry out my professional responsibilities.

OSINT analyst
Islamabad, Pakistan
testimony collected in August 2024

First-time offenders in 2024

Comoros	Authorities in Comoros imposed an internet shutdown to quell post-election protests after the incumbent President Azali Assoumani was declared the winner of the January 2024 presidential election.[63]
El Salvador	The government of El Salvador blocked access to Telegram on two separate occasions following publication of news articles critical of the authorities.[64]
France	France, a member of the Freedom Online Coalition, a group of countries that supports digital rights and has condemned internet shutdowns, blocked access to TikTok in the territory of New Caledonia.[65] Independence activists led by the Indigenous Kanak people were organizing protests against voting reforms introduced by French authorities.
Guinea-Bissau	On July 27, authorities in Guinea-Bissau disrupted access to the internet and dispersed police to prevent planned demonstrations from taking place across the country.[66]
Malaysia	Internet service providers in Malaysia began blocking access to the Grindr website on April 30, reportedly following orders from the Malaysia Communications and Multimedia Commission (MCMC).[67] Grindr is still blocked on some Malaysian networks at the time of writing this report.[68]
Mauritius	On October 31, Mauritius' Information and Communication Technologies Authority (ICTA) ordered internet service providers in the country to block access to all social media platforms until November 11.[69] However the directive was abruptly withdrawn the following day after condemnation by local and international rights groups.
Thailand	Thai authorities ordered internet service and phone lines serving people in Myanmar to be disconnected, during active conflict. Although authorities claimed these actions were aimed at curbing cybercrime, the shutdown affected local residents, disconnecting those relying on Thai networks, including vulnerable populations trafficked to work in scam call centers.[70]

63 Access Now (2024). *#KeepItOn: Comoros must not black out the internet to quell post-election protests.* https://www.accessnow.org/press-release/comoros-must-not-blackout-the-internet/

64 Access Now (2024). *El Salvador: sociedad civil y periodistas exigen transparencia sobre interrupción de Telegram.* https://www.accessnow.org/press-release/telegram-comunicado-el-salvador/

65 *See supra note 22.* Access Now (2024).

66 VOA Portugese (2024). *Bissau: Police prevent announced demonstrations from taking place.* https://www.voaportugues.com/a/sem-internet-e-com-muitos-pol%C3%ADcias-nas-ruas-bissau-teve-as-manifesta%C3%A7%C3%B5es-anunciadas/7715236.html

67 iMAP (2024). *Internet Censorship Update: Blocking of Grindr.com website.* https://imap.sinarproject.org/news/internet-censorship-update-blocking-of-grindr-com-website

68 OONI Explorer (2024). *OONI Measurement Aggregation Toolkit (MAT).* https://explorer.ooni.org/chart/mat?probe_cc=MY&since=2024-12-30&until=2025-01-31&time_grain=day&axis_x=measurement_start_day&axis_y=probe_asn&test_name=web_connectivity&domain=www.grindr.com

69 Reuters (2024). *Mauritius blocks social media until after election, opposition and civil society groups cry foul.* https://www.reuters.com/world/africa/mauritius-suspends-social-media-until-after-election-communications-regulator-2024-11-01/

70 *Supra note 56.* The Diplomat (2024).

Entrenched and emerging offenders by region

Africa

Equatorial Guinea

On July 20, authorities shut down the internet and phone lines in the island province of Annobón, after residents, including environmental activists, led protests against the government. There were reports of widespread arrests and prosecution of human rights defenders.[71] The shutdown is ongoing as of early 2025.

Ethiopia

Shutdowns in the Tigray and Amhara regions have persisted since November 2020 (Tigray) and August 2023 (Amhara), leaving residents outside of major cities struggling with limited access and throttled speeds. While the government of Ethiopia announced that connectivity has been restored,[72] reports from people in Ethiopia indicate that the restoration has not been complete or meaningful. Connectivity remains well below pre-conflict levels at the time of reporting.

Mozambique

One year following the country's first recorded shutdown in October 2023, authorities violently cracked down[73] on post-election protests and imposed a combination of curfew-style mobile shutdowns and blocks of Facebook and WhatsApp between October 25 and November 14.

Asia Pacific

Myanmar

It is estimated that hundreds of internet shutdowns have been perpetrated in Myanmar since the military coup in February 2021.[74] In 2024, we worked with coalition partners to verify **85** shutdowns; of these, 31 coincided with documented grave human rights abuses.[75] The Myanmar junta imposed 74 shutdowns, at least **17** of which were correlated with airstrikes on villages with civilians. In addition, other parties imposed cross-border shutdowns in Myanmar: China imposed **two** and Thailand **four**, while the exiled National Unity Government (NUG), Myanmar National Democratic Alliance Army (MNDAA), and Ta'ang National Liberation Army (TNLA) imposed **one shutdown each** in areas they controlled. The remaining **two** shutdowns were imposed by unknown parties.

Notably, there were two cases in 2024 where LEO satellite internet services were targeted in Myanmar since people use them extensively when traditional telecommunications networks are cut off.

71 Civicus Monitor (2024). *HRDs arbitrarily arrested, prosecuted; internet shutdown in Annobon province.* https://monitor.civicus.org/explore/hrds-arbitrarily-arrested-prosecuted-internet-shutdown-in-annobon-province/

72 Addis Standard (2024). *News: Internet services resume across Amhara region after near year-long shutdown.* https://addisstandard.com/internet-services-resume-across-amhara-region-after-near-year-long-shutdown/

73 Al Jazeera (2024). *At least 30 reported killed in weeks of post-vote violence in Mozambique.* https://www.aljazeera.com/news/2024/11/8/at-least-30-reported-killed-in-weeks-of-post-vote-violence-in-mozambique

74 Access Now (2023). *Shrinking democracy, growing violence: internet shutdowns in 2023.* https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf

75 OHCHR (2024). *Report on Human Rights situation in Myanmar.* https://www.ohchr.org/en/press-briefing-notes/2024/09/report-human-rights-situation-myanmar

In one instance, the junta raided shops that offer Starlink and IP Star.[76] In another, the NUG instructed townships under resistance control to prevent public use of LEO satellite internet.[77] These are the first instances of this type of shutdown in our records.

Asia Pacific

India

Despite a modest decrease in shutdowns from 2023, India still imposed **84** in 2024, the most disruptions ordered in a democracy that year. People in **16** states and territories experienced a shutdown, with state government officials in Manipur (**21**), Haryana (**12**), and Jammu & Kashmir (**12**) topping the list of offenders in India. Of the **84**, **41** shutdowns were related to protests, and **23** were related to communal violence.

Pakistan

Authorities imposed **21** shutdowns across Pakistan in 2024, the highest annual total ever for the country. This included a combination of nationwide blocks of X, Signal, and Bluesky, a nationwide mobile shutdown on election day (February 8), and numerous local and regional shutdowns during protests and religious holidays. People in the province of Balochistan were impacted by **six** shutdowns, including an ongoing shutdown from 2022 in Panjgur and **two** targeting the Baloch ethnic group during protests that sparked violent police crackdowns.[78]

Bangladesh

Authorities imposed a string of **five** escalating, layered shutdowns in July and August during protests by the student-led quota reform movement. Despite deadly crackdowns,[79] the protest movement led to the resignation of the former Prime Minister and the formation of an interim government.

Eastern Europe and Central Asia

Russia

In addition to **seven** shutdowns imposed on Ukraine during their full-scale invasion, Russia imposed **12** within their own borders through **eight** platform blocks, **two** local or regional shutdowns, and **one** shutdown carried out as they tested their "sovereign internet."[80]

Azerbaijan

Authorities followed a surge of **six** shutdowns from 2022 and 2023 with a shutdown during the February 2024 elections that targeted polling stations,[81] and a blocking of X from October 8-10.

76 BNI Online (2024). *Junta Cracks Down on Myitkyina Establishments Providing Satellite Based Internet Service.* https://www.bnionline.net/en/news/junta-cracks-down-myitkyina-establishments-providing-satellite-based-internet-service

77 Modern Times on Facebook (2024). https://www.facebook.com/story.php?story_fbid=998760372262263&id=100063849292474&mibextid=WC7FNe&rdid=vTl2SyEKZRr5jSrt

78 Al Jazeera (2024). *Why protest by ethnic Baloch has put Pakistan's key port of Gwadar on edge.* https://www.aljazeera.com/news/2024/7/31/why-protest-by-ethnic-baloch-has-put-pakistans-key-port-of-gwadar-on-edge

79 The Daily Star (2024). *At least 93 dead as violence grips the country.* https://www.thedailystar.net/news/bangladesh/news/least-93-dead-violence-grips-the-country-3669636

80 The Record (2024). *Russia disrupts internet access in multiple regions to test 'sovereign internet.'* xzhttps://therecord.media/russia-disrupts-internet-access-in-multiple-regions-runet

81 Meydan.tv (2024). *Internet restrictions during Azerbaijan elections prompt concerns over freedom of communication.* https://www.meydan.tv/en/article/internet-restrictions-during-azerbaijan-elections-prompt-concerns-over-freedom-of-communication/

Eastern Europe and Central Asia

Kyrgyzstan

Authorities blocked TikTok nationwide in April 2024,[82] and as of this writing, it remains blocked. Prior to this, Kyrgyzstan had not had a shutdown since 2020.

Latin America and the Caribbean

Venezuela

Following the presidential election in July 2024 that international monitors deemed neither free nor fair,[83] authorities have met protests with deadly force, scores of arrests and disappearances, and an array of technology-enabled political violence.[84] In a further crackdown on dissent, they blocked numerous platforms on August 8, including Signal and X, and then blocked YouTube on November 23.[85]

Middle East and North Africa

Israel

Israel imposed **six** shutdowns in Gaza in 2024. This includes one continuous shutdown from October 9, 2023, which brought **13** local ISPs offline (**eight** of which never came back online),[86] and five targeted shutdowns in governorates and towns that were the focus of Israeli military bombardments.

Sudan

Warring parties imposed at least **four** shutdowns during the civil war in 2024, all of which coincided with grave human rights abuses.[87] The Rapid Support Forces (RSF) imposed **two** shutdowns by taking over data centers, resulting in nationwide, months-long disruptions. The Sudanese Armed Forces (SAF) imposed **one** shutdown in Darfur in January,[88] and in September, in the midst of heavy fighting, there was another shutdown in Omdurman, with no clear attribution.

Mauritania

Authorities followed the **two** shutdowns in 2023 with another **two** in 2024.[89] In the midst of post-election protests in July, authorities shut down mobile internet for weeks, and then cut off the same networks in August during baccalaureate exams.[90]

82 France 24 (2024). *Kyrgyzstan's TikTok block builds censorship fears.* https://www.france24.com/en/live-news/20240419-kyrgyzstan-s-tiktok-block-builds-censorship-fears

83 VOA (2024). *Concern grows as Venezuela blocks election observers*. https://www.voanews.com/a/concern-grows-as-venezuela-blocks-election-observers/7715124.html

84 Access Now (2024). *Venezuela's many means of surveillance and control.* https://www.accessnow.org/the-many-means-of-surveillance-and-control-in-venezuela/

85 Access Now (2024). *Maduro must #KeepItOn in times of protest and unrest.* https://www.accessnow.org/press-release/maduro-keepiton-during-protest-and-unrest/

86 *Supra note 53*. Access Now (2023).

87 Human Rights Watch (2024). *Sudan: One Year of Atrocities Requires New Global Approach* https://www.hrw.org/news/2024/04/13/sudan-one-year-atrocities-requires-new-global-approach

88 *Supra note 9.* Access Now (2024).

89 Access Now (2024). Authorities in Mauritania must #KeepItOn during presidential inauguration and beyond. https://www.accessnow.org/press-release/mauritania-authorities-keepiton-during-and-after-presidential-inauguration/

90 Access Now (2024) on X. https://x.com/accessnow/status/1823676084505792766

VI. Fighting back in 2024: partnerships, collaborations, community building, and resistance

The record-high number of perpetrators and expanding scope of communities impacted by shutdowns across the globe is a **wake-up call for all stakeholders to redouble their support for the fight to end these blatant acts of repression.** Throughout 2024, **civil society's resilience and commitment to bringing these abuses to light never flagged, as the #KeepItOn coalition deployed** diverse strategies to hold perpetrators accountable.

Over the years, we have fought to establish new global norms against internet shutdowns, resulting in the adoption of key resolutions and frameworks, positive court rulings, and government policy reforms. Governments and regional and international groups have denounced shutdowns, and there is growing public recognition of the dangers they pose, particularly to human rights and democracy. Following are some of the strategies we used in 2024 to advance our collective efforts against shutdowns:

Campaigns:

#KeepItOn Election Watch: Through this initiative, the #KeepItOn coalition mobilizes people and communities to demand an open, inclusive, and secure internet throughout election periods and beyond, engaging through open letters, workshops, and dialogues. In 2024, when over a billion people went to the polls, we tracked and monitored elections in at least 25 countries, warning governments against election shutdowns and calling out those that ignored these warnings and imposed shutdowns in violation of people's fundamental rights.

#NoExamShutdown: Together with our partners SMEX and the Internet Society, we remained steadfast in our fight against exam-related shutdowns in the Middle East and North Africa (MENA) region and beyond. Yet in 2024, authorities continued to disrupt access to the internet during scheduled exams, cutting off entire communities and populations. This underscores the need to expand our strategies and intensify our advocacy in 2025, particularly given the fact that this harmful practice is becoming a global issue, not limited to MENA.

Shutdown Impact Stories Project: Internet shutdowns run counter to efforts to advance digital technology and innovation, particularly in Global Majority countries that are confronting the digital divide. Through this project we share the stories of people directly affected by shutdowns,[91] documenting the negative impact on their rights to education, health, and social, political, and economic independence.

91 Access Now (2016). *Shutdown Stories Archive.* https://www.accessnow.org/tag/shutdown-stories/

Measurement tools:

Thanks to advancements from the measurement community, the #KeepItOn coalition's tracking, detection, verification, and documentation of internet shutdowns has drastically improved. Our detection partners continue to roll out initiatives every year that strengthen our internet shutdown measurement processes.

- **OONI:** In 2024, the Open Observatory of Network Interference (OONI) hosted an in-person partner gathering and launched OONI Run v2 to enhance community-driven censorship testing and rapid response to network disruptions worldwide.[92]

- **Cloudflare:** The IT service management firm Cloudflare increased the accessibility of its tools for tracking shutdowns in 2024, translating[93] its full user interface into 12 major international languages —expanding its reach and boosting the capacity for evidence gathering globally.

Circumvention tools:

The #KeepItOn coalition's partnership with VPN service providers remains crucial to ensure people have access to open, secure, and free VPNs during internet blackouts globally. We have established an open channel with providers of circumvention tools, including TunnelBear, Proton, and Tor Project, to rapidly respond to and support people and communities at risk.

- **Proton:** In March 2024, Proton rolled out a campaign[94] to provide people with free Proton VPN servers in 21 countries that have a history of shutdowns and censorship around elections. They also dedicated resources and developed anti-censorship features to make their VPN accessible and easy to use.

- **TunnelBear:** launched a new anti-censorship technologies support initiative and expanded its bandwidth program[95] to include Azerbaijan, Bangladesh, Mauritius, Mozambique, Pakistan, Senegal, and Venezuela. In addition, they localized their VPN apps into Bengali and Swahili and hope to include more new languages in 2025 to further expand their reach.

Resources and capacity building:

The #KeepItOn coalition continues to prioritize advocacy briefings, capacity building, strategic litigation, and active engagement in national, regional, and international spaces to strengthen our allyship against shutdowns. Over the years, through periodic briefings, we provide updates, deliberate about strategies, and address challenges with members of institutions including the Freedom Online Coalition and its Task Force on Internet Shutdowns (TFIS), the European Union, and government agencies that are instrumental in the fight against shutdowns. We also organize workshops and webinars to foster collaboration and equip grassroots organizations with tools and strategies to #KeepItOn. We have updated our #KeepItOn campaign page[96] and Shutdown Tracker Optimization Project (STOP) methodology,[97] and launched a new dashboard[98] to enhance the accessibility of our resources and data on shutdowns.

92 OONI (2025). *Year in review: OONI in 2024.* https://ooni.org/post/2024-year-in-review/

93 Cloudflare Radar (2024) on X. https://x.com/CloudflareRadar/status/1847276447142166857

94 Proton VPN (2024). *Proton provides free VPN servers in lead up to elections.* https://protonvpn.com/blog/free-servers-before-elections

95 TunnelBear (n.d). *How much data do free users get?* https://help.tunnelbear.com/hc/en-us/articles/360007004411-How-much-data-do-free-users-get

96 *Supra note 1.*

97 Access Now (2024). *Shutdown Tracker Optimization Project.* https://www.accessnow.org/guide/shutdown-tracker-optimization-project/

98 Access Now (2025). *#KeepItOn STOP data.* https://www.accessnow.org/keepiton-data

VII. Recommendations for stakeholders

No single stakeholder can end internet shutdowns alone. Across all contexts, including during conflict, protests, elections, and exam periods, we urge states, private sector actors, donors, international organizations, and civil society to work together to #KeepItOn.

1. Parties to conflict, third-party actors, oversight bodies, and all other stakeholders must ensure by all means necessary that civilians in conflict-affected areas, as well as those fleeing, refugees, and the displaced, maintain reliable access to ICT infrastructure and essential communications platforms.

For the second consecutive year, conflict was the single largest trigger for internet shutdowns around the world. The staggering number of cases and increasingly complex network of perpetrators in 2024 show yet again that internet shutdowns are spreading in scope and scale, and the impacts are more dreadful for people and communities at risk. The targeting and wanton destruction of civilian connectivity and communication systems is increasingly happening in plain sight, and under the watch of the same states espousing the importance of connectivity and access to information in processes such as the World Summit on the Information Society (WSIS), Internet Governance Forum (IGF), Global Digital Compact (GDC), World Economic Forum (WEF), and beyond.[99]

- **All conflict parties must:**
  - » Reaffirm their commitment to respect human rights and international humanitarian law (IHL) both online and offline, including the limits posed by IHL on activities that disable civilian objects, damage or disrupt civilian data, and interfere with medical as well as humanitarian work;[100]
  - » Immediately cease the indiscriminate destruction of civilian objects, including medical, energy, and telecommunications infrastructure[101] and reaffirm the respect of agreed deconfliction mechanisms; and
  - » Ensure that the civilian population has access to 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.
- Governments and the international community must hold perpetrators of gross human rights abuses and crimes against humanity under the cover of internet shutdowns, as well as their enablers, to account through any and all available avenues of justice.
- All stakeholders must also recognize the plethora of digital harms on affected communities by reaffirming that protections under international legal frameworks fully extend to the digital domain and to civilian telecommunication objects, and embracing and applying the concept of a digital ceasefire.[102]

99 *See, e.g.,* CEPA (2024), *UN Avoids Surrendering the Internet to Russia and China — For Now*, https://cepa.org/article/un-avoids-surrendering-the-internet-to-russia-and-china-for-now, *but see also* 7amleh (2024),Gaza Telecommunications Infrastructure, https://7amleh.org/storage/Advocacy%20Reports/Telecommunications%20Report.pdf

100 ICRC (2024). *Protecting civilians and other protected persons and objects against the potential human cost of ICT activities during armed conflict*. https://rcrcconference.org/app/uploads/2024/10/34IC_R2-ICT-EN.pdf

101 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

102 Access Now (2024). T*oward a digital ceasefire.* https://www.accessnow.org/toward-a-digital-ceasefire/

2. All governments must commit in law and in practice to protect people's freedom of expression, right to access information, and other internet-enabled human rights, and to pursue accountability and redress where those rights have been undermined, including through internet shutdowns.	• In 2024, we saw progressive democracies with relatively strong track records for upholding free expression – including France, Mauritius, and Comoros – regress by implementing internet shutdowns.[103] We urge entrenched and repeat offenders, including authorities in Bangladesh, Equatorial Guinea, India, Myanmar, Pakistan, Russia, Sudan, and Venezuela, to put human rights at the center when addressing concerns or threatening situations during a crisis, rather than shutting down digital communications platforms or the internet, actions that have serious repercussions for human rights.
Countries with a history of internet shutdowns should conduct investigations, pursue accountability, and ensure remedy and redress for those harmed.	• In a promising development, authorities in Bangladesh set up a probe committee in 2024 to investigate the cause of the two-week long internet shutdown during student protests in July.[104] This kind of investigation is crucial to ensure transparency and accountability for such actions, and we urge all governments and stakeholders to follow suit.
3. The Freedom Online Coalition (FOC) should renew and deepen its commitment to preventing internet shutdowns and pursuing accountability when they occur.	It's deeply concerning to see France and Kenya, both members of the FOC, an alliance meant to advocate for internet freedom globally, undermine their own principles by imposing harmful internet shutdowns to quell protests. The FOC's joint statement denouncing protest-related shutdowns in Iran in 2022 was a clear signal that the international community must stand against such actions.[105] • The coalition should adopt stronger and more effective accountability mechanisms for FOC members to prevent such actions in the future. • Likewise, in light of the FOC discontinuing its Task Force on Internet Shutdowns (TFIS) in 2024, the coalition must develop new mechanisms, in collaboration with civil society and the private sector, for continuing its public and private advocacy against shutdowns, and for enabling more member states to step into leadership roles amid uncertain political support for internet freedom at a global level.

103 Access Now (2024). *First-time culprit: France blocks TikTok in New Caledonia.* https://www.accessnow.org/france-blocks-tiktok-new-caledonia/; AP (2024). *Mauritius suspends access to social media ahead of parliamentary elections.* https://apnews.com/article/mauritius-social-media-suspension-elections-pravind-jugnauth-2e4e13fcd2ab37c32f85e4d042726022; and Access Now (2024). *#KeepItOn: Comoros must not black out the internet to quell post-election protests.* https://www.accessnow.org/press-release/comoros-must-not-blackout-the-internet/

104 The Daily Star (2024). *Committee formed to probe internet shutdown.* https://www.thedailystar.net/news/bangladesh/news/committee-formed-probe-internet-shutdown-3674941

105 Freedom Online Coalition (2022). *FOC Joint Statement on Internet Shutdowns in Iran.* https://freedomonlinecoalition.com/wp-content/uploads/2022/10/FOC-Joint-Statement-on-Internet-Shutdowns-in-Iran_October-2022.pdf

4. States and international organizations should continue developing and strengthening norms to ensure the practice of internet shutdowns comes to an end.	In the Pact for the Future and Global Digital Compact, adopted by consensus at the 2024 UN Summit of the Future, world leaders committed to "[r]efrain from internet shutdowns and measures that target internet access."[106] This represents a significant normative win, and a high-level affirmation of a decade of advocacy against internet shutdowns at intergovernmental forums. The UN Secretary-General, Office for Digital and Emerging Technologies (ODET), High Commissioner for Human Rights (OHCHR), International Telecommunication Union (ITU), and other key mandate holders should continue to advance this work both through ongoing norm development and through accountability and implementation.
5. Both communications platforms and governments must uphold their responsibility to maintain unencumbered access to a safe, rights-promoting online ecosystem.	Authorities have continued to wield platform blocks[107] to control the flow of information, often under the pretext of curbing the spread of misinformation and hateful or violent content. However, many of the largest social media platforms have decisively stepped back from their past commitments to limit the spread of harmful content on their platforms,[108] enabling an increase in hate speech and misinformation that governments rightfully want to address. • Tech companies must uphold their responsibilities to reduce human rights harms stemming from the use of their platforms and commit to rights-respecting practices consistently across all contexts, especially for communities in crisis.[109] • At the same time, governments must adhere to international human rights law, work to tackle underlying causes of disinformation, and refrain from imposing platform blocks, which deny people their rights to free speech and access to vital information.[110]

106 United Nations (2024). *Pact for the Future.* https://www.un.org/en/summit-of-the-future/pact-for-the-future

107 Platform blocks are a type of internet shutdown. *See supra note 1*.

108 Free Press (2023). *How Social-Media Rollbacks Endanger Democracy Ahead of the 2024 Elections* https://www.freepress.net/big-tech-backslide-report

109 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/

110 Access Now (2020). *Guide: how to protect human rights in content governance.* https://www.accessnow.org/guide/guide-how-to-protect-human-rights-in-content-governance/; *See also* Access Now (2024). *Access Now condemns the suspension of X in Brazil* https://www.accessnow.org/press-release/access-now-condemns-the-suspension-of-x-in-brazil/

6. Donors and other stakeholders must increasingly invest in the resilience of civil society actors working to end internet shutdowns and the suffering from their impact.	With the escalation of internet shutdowns and the increasing crackdown on civic space globally, especially in places where human rights are under attack, it is vital that advocacy organizations and groups that document and push back against these shutdowns and other digital rights violations are adequately supported. • Donors and funding groups should prioritize support for digital rights groups to ensure that they remain operational and effective. • It remains crucial for donors, funding organizations, and private sector actors to continue to invest in alternative connectivity solutions, circumvention tools, and internet measurement detection tools to ensure that people and communities that face shutdowns have a means to stay connected, access critical information, monitor and document evidence, and report on human rights abuses taking place in their countries and beyond.
7. Collective action remains essential in advocating against the severe impact of internet shutdowns.	• Civil society groups must continue to work together — through joint advocacy, shared resources, capacity building, or coordinated legal strategies — to draw attention to the harms and dangers of internet shutdowns happening in all corners of the world and use available channels to demand accountability.

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.

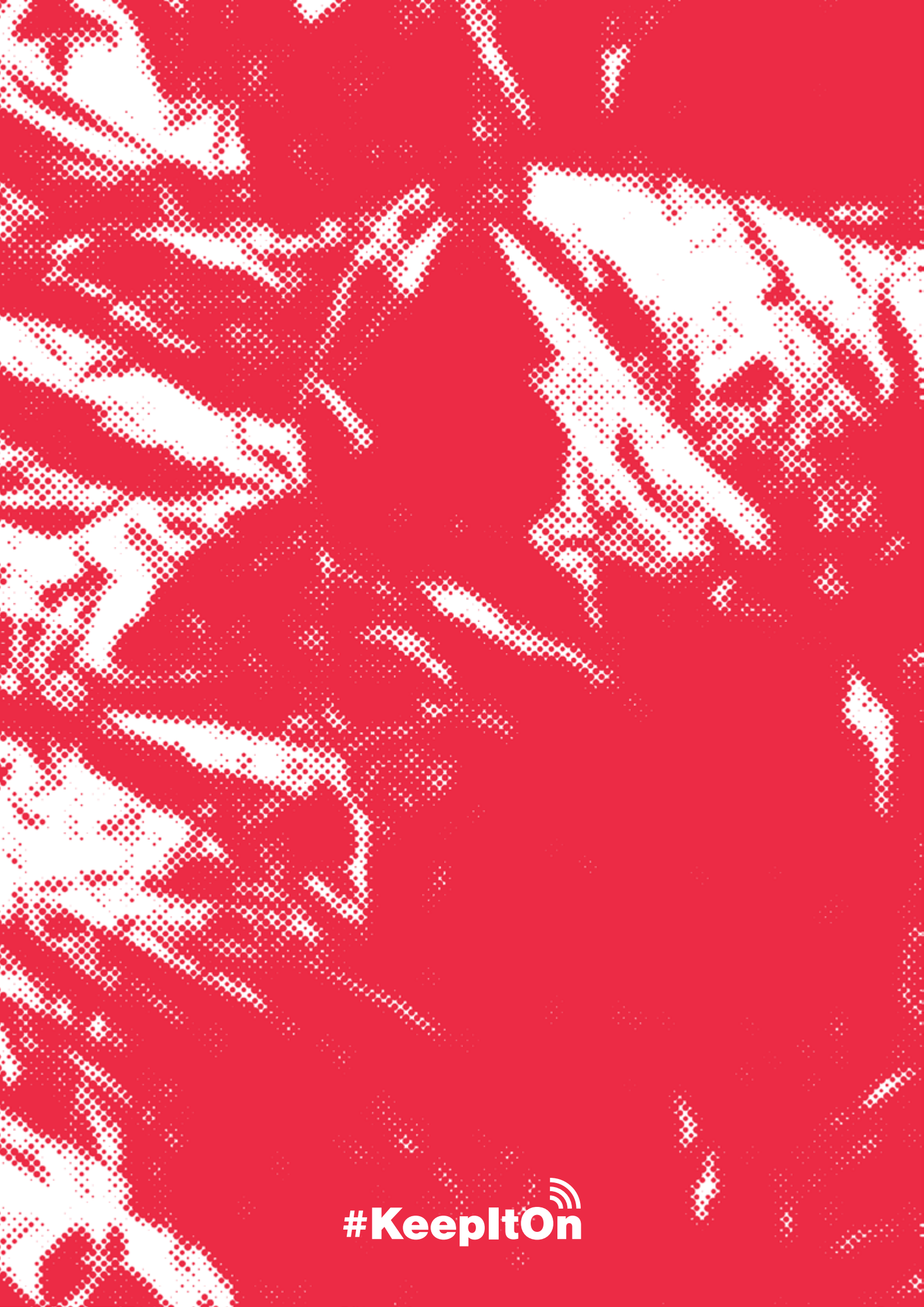
CONTACT

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 and Research Lead, Access Now
zach@accessnow.org


#KeepItOn