/2018----Asia----Iraq
Asia----Pakistan ----Islamabad
4/26/20
3/7/2018----Asia----Sri
4/13/2018----Europe----Russia
8/27/2018----Asia----India----Shahjahanpur, Uttar Pradesh
4/13/2018----Asia----Yemen----
/1/2018
eon
ammu and Kashmir
18----Africa
404
nka
3/7/2018----Africa----Ethiopia
8/15/2

THE STATE OF INTERNET SHUTDOWNS AROUND THE WORLD

THE 2018 #KEEPITON REPORT

#KeepItOn

#KeepItOn

The #KeepItOn campaign unites and organizes the global effort to end internet shutdowns. The coalition is growing rapidly, and so far 191 organizations from 68 countries around the world, ranging from research centers to rights and advocacy groups, detection networks, foundations, and media organizations, have joined the movement.

This report is a publication of Access Now for the #KeepItOn coalition and was written by Berhan Taye with the collaboration of Access Now's team. The author would like to specially thank Peter Micek, Melody Patry, Donna Wentworth, Gustaf Björksten, Akash Singh, and Sage Cheng for their contributions.

Overview

The 2018 internet shutdown trends

"When the shooting and looting happened in Jijiga, we wanted to get more information about what was happening, we wanted to share with the world that we have been victims. We were not able do that because they cut off the internet. We couldn't leave our house, we can hear gun shots and people screaming. We had to call people in Addis Ababa 600 km away to find out what was happening in our city."

— Anonymous, Ethiopia, April 2018

196

Documented shutdowns in 2018

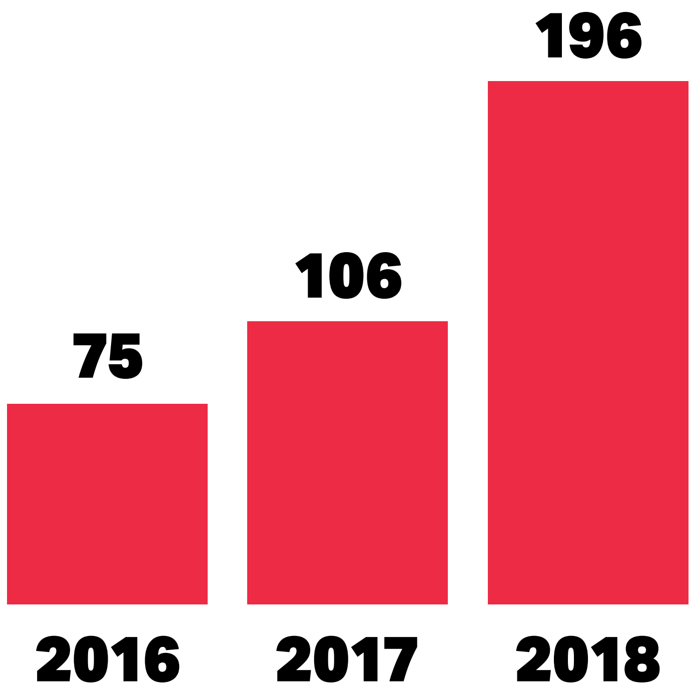
25

Countries

Most affected regions

Asia
Africa

The number of internet shutdowns worldwide is on the rise

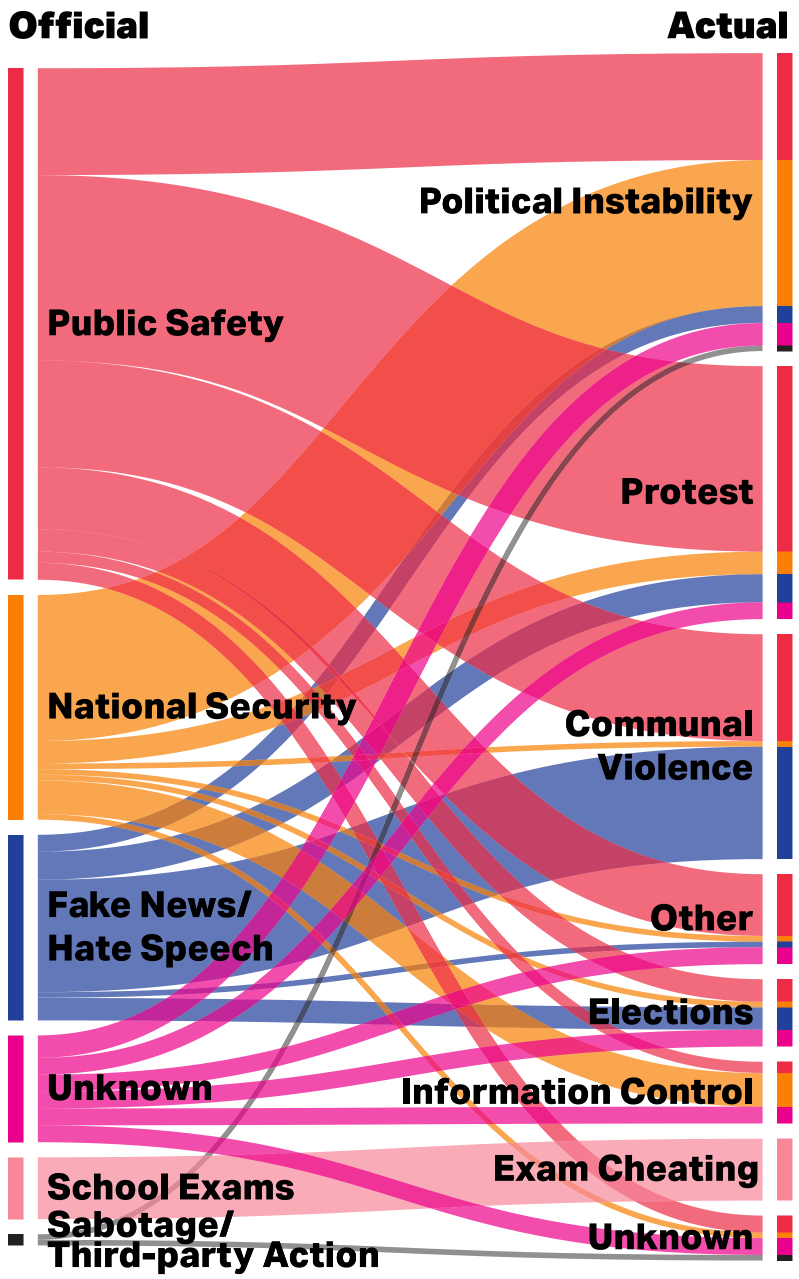


More people are pushing back

191
#KeepItOn coalition members

68
countries worldwide

Official justifications vs. actual causes of internet shutdowns in 2018



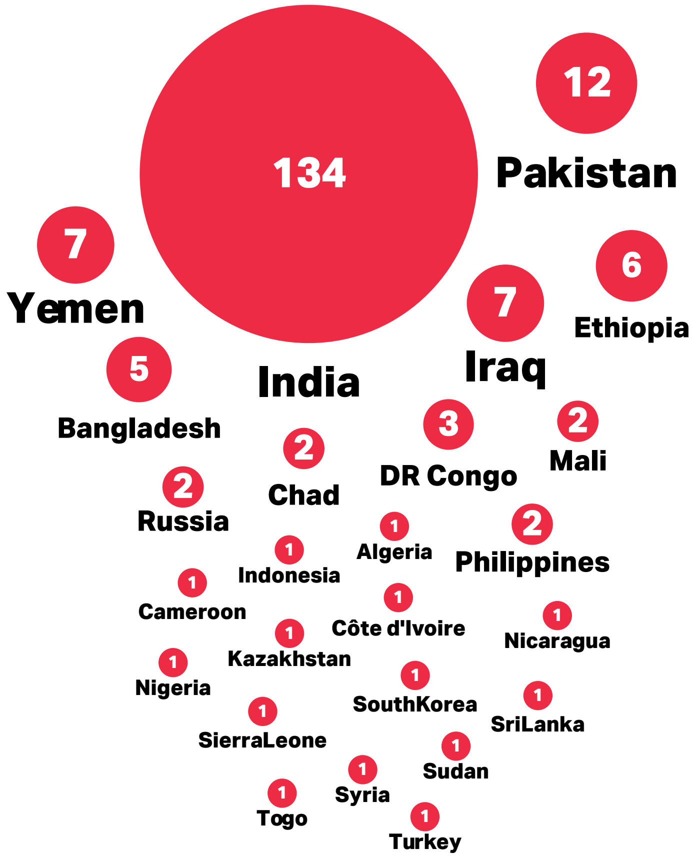
* Data from the Shutdown Tracker Optimization Project (STOP) 2016-2018

Table of Contents

1. Introduction: internet shutdowns in 2018

In 2018, the global #KeepItOn coalition [1] documented more than 196[2] internet shutdowns around the world. Just as it has been since 2015, India was responsible for the majority: 67% of the world's documented shutdowns took place in India in 2018, with 134 incidents. The remaining 33% took place in a diverse range of countries: Algeria, Bangladesh, Cameroon, Chad, Côte d'Ivoire, Democratic Republic Congo, Ethiopia, Indonesia, Iraq, Kazakhstan, Mali, Nicaragua, Nigeria, Pakistan, Philippines, and Russia.

2018 number of internet shutdowns by country



1.1 What is an internet shutdown?

An internet shutdown can be 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."[3] They include blocks of social media platforms, and are also referred to as "blackouts," "kill switches," or "network disruptions."

In Access Now's work documenting shutdowns in 2018 and in this report, we identify the key trends that defined shutdowns and show the nature and official rationales for shutdowns in the year. Perpetrators of internet shutdowns historically use similar justifications for ordering shutdowns, but these justifications rarely match what observers can conclude is the real motivation. This year the official rationales have included combating "fake news" (properly called disinformation and misinformation), hate speech, and related violence, securing public safety and national security, precautionary measures, and preventing cheating during exams, among others.

Whether they are ordered in Ethiopia, Chad, Venezuela, or India, and whether they are justified as a measure to fight "fake news" and hate speech or to stop cheating during exams, the facts remain the same: internet shutdowns violate human rights, put people in danger, and harm the economy. Internet shutdowns curtail freedom of expression, cut access to information, and can inhibit people from assembling and associating peacefully, online and off. In addition, during shutdowns, many victims are unable to reach their families, get accurate information to stay safe, or reach emergency services. Shutdowns disrupt businesses, schools, and ordinary lives, often exacting a significant financial cost[4]. The United Nations and other intergovernmental bodies have passed a series of important resolutions[5] to condemn shutdowns and caution states against imposing them.

> **Notably, in a variety of cases, governments never publicly acknowledge that they are responsible for a shutdown.**

Shutdowns are ordered under a variety of state structures. Typically, the orders come from authorities in local governments, state/regional governments, the judiciary, and executive bodies of governments. The entity that orders a shutdown can impact the scope and effect of the shutdown. The geographic reach of a shutdown could extend beyond a country's borders, or be as localized as a few cellular towers on a protest route. Some countries have legislation that facilitates and legitimizes shutdowns, while others issue arbitrary orders that are not necessarily grounded in or supported by law.

In ordering shutdowns, government authorities employ a range of tactics to support specific goals in a particular context. A government might use bandwidth throttling to slow internet access, or alternate between shutting down mobile internet and cutting broadband service internet together, or it may block specific apps and services, such as social media or messaging services. Notably, in a variety of cases, governments never publicly acknowledge that they are responsible for a shutdown. That shifts the burden of proof to the victims, making it harder to push back or seek redress for harm done. That is all the more troubling because there appears to be a correlation between suspension of the internet and human rights violations that take place in the dark.

The good news is that the increased global spotlight on internet shutdowns appears to making an impact. Even though there were more documented shutdowns in 2018 than we recorded in previous years, there were also more documented court challenges to stop them. Public interest lawyers, activists, ordinary citizens, and civil society groups have been forcing telcos, communications regulators, and others to defend network disruptions in court, asserting the rights to access to information and freedom of expression. At the same time, members of the global #KeepitOn coalition have been working together to help victims gather technical evidence of shutdowns and in some cases, also helping them to circumvent the shutdowns.

Importantly, the community that dedicates its invaluable time to fighting shutdowns continues to grow and diversify. There are now civil society coalition members from more than 68 countries working to keep the internet on, all across the globe.

2. Governments continue to normalize shutdowns

2.1 Governments rarely acknowledge shutdowns

Out of the more than 200 incidents of shutdowns reported in 2018, only 77 were acknowledged by the government or entities that ordered the shutdowns.

2.2 When they do, they use umbrella terms to justify shutdowns despite details and nuances of what actually happened

When governments shut down the internet, whether through a memo, directive, or just a phone call, authorities will sometimes provide the public with some form of public rationale or justification. The most common justifications cited in 2018, as shown below: public safety, "fake news" (which as we have noted, is properly called disinformation or misinformation) or hate speech and related violence, national security, and school exams.

[1] #Keepiton, Access Now, 2019, https://www.accessnow.org/keepiton/

[2] The number of shutdowns in 2018 is estimated to be more than 196. This number indicates only the incidents we have been able to verify and confirm through our partners on the ground and via the media. It is highly likely that the number of shutdowns is much higher than what we have documented.

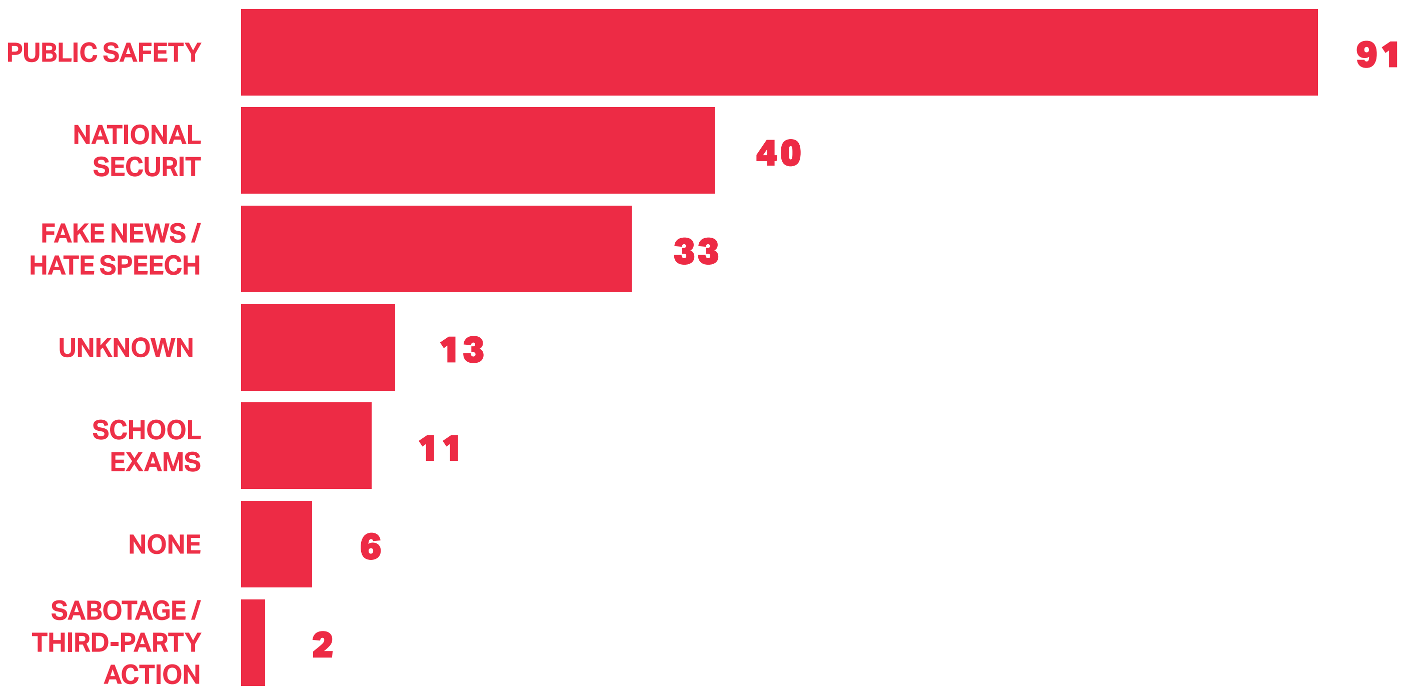
[3] This definition was developed at RightsCon Brussels in 2016 in collaboration with a diverse set of stakeholders including technologists, policy makers, activists, and others. Read more: https://www.accessnow.org/no-internet-shutdowns-lets-keepiton/

[4] West, D. *Internet shutdowns cost countries $2.4 billion last year*, Brookings, 2016. Available at: https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

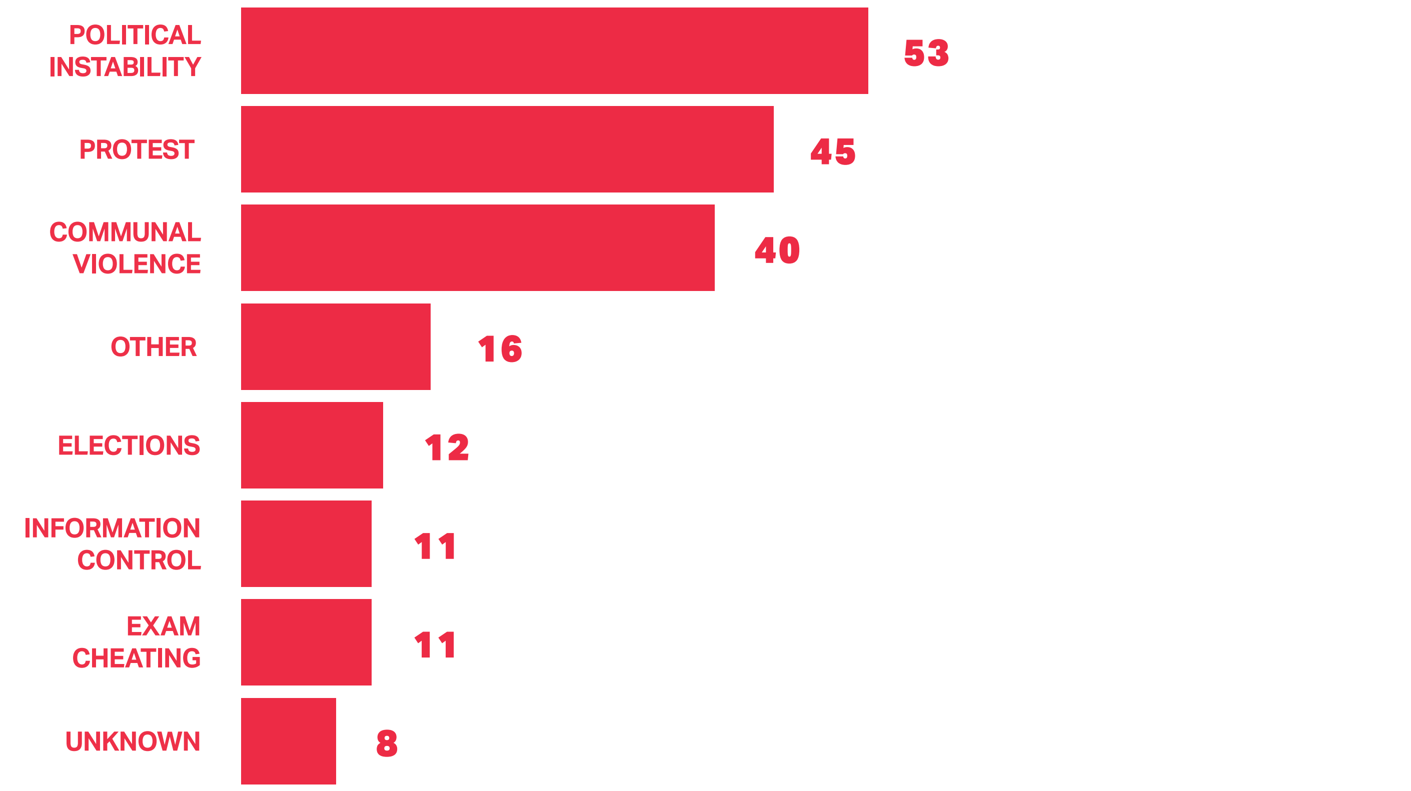
[5] See page 14.

Observation can reveal more information for determining the impetus for internet shutdowns in 2018: they took place in response to protests, militant or terrorist activity (mostly in the Kashmir region in India), elections, during communal violence, to assert information control (including during periods of political instability), on religious holidays and anniversaries, and during school exams.

Common official justifications used by governments that ordered shutdowns

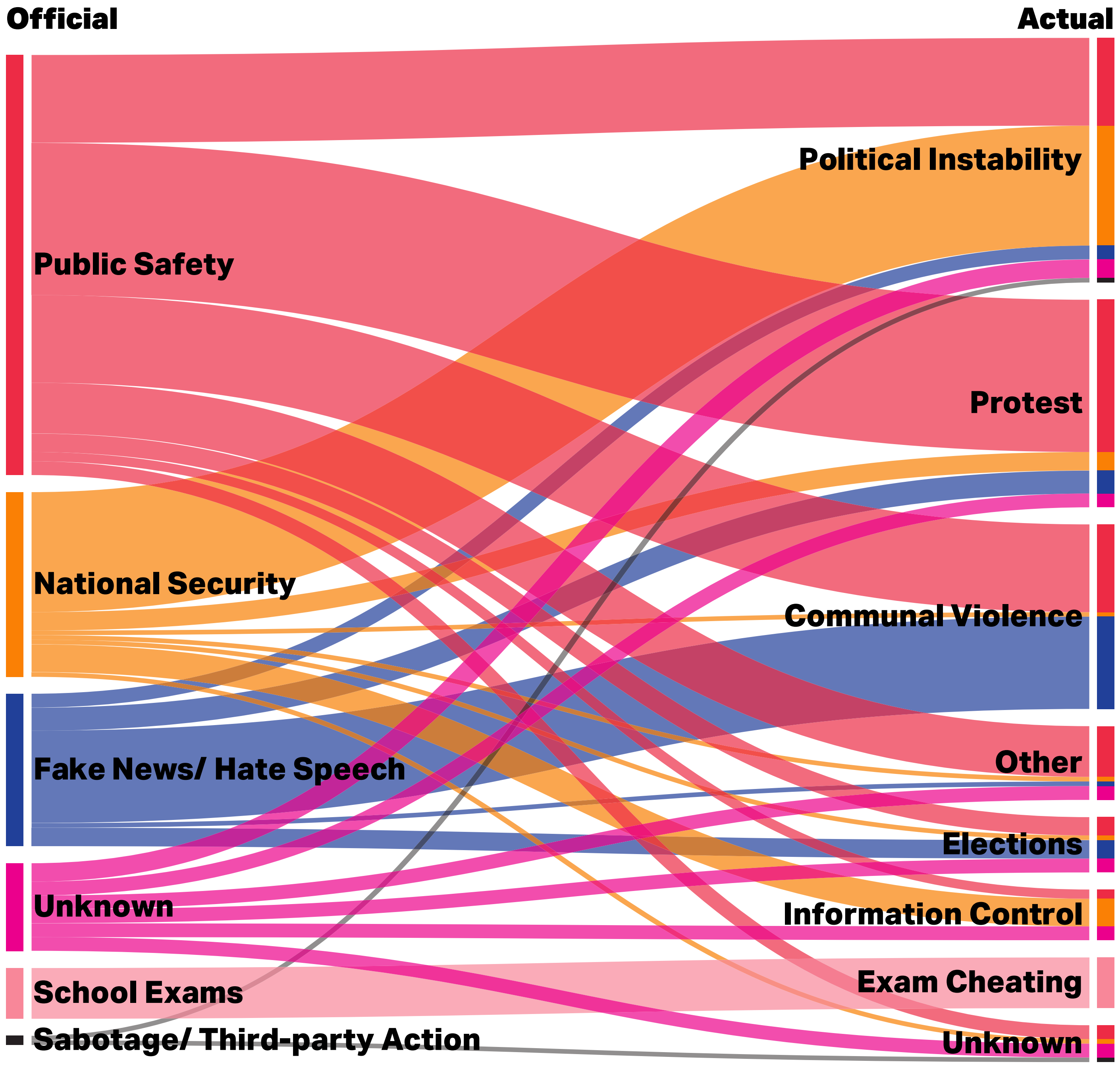


Common actual causes that triggered or influenced internet shutdowns



It is rare for government justifications to match the cause of shutdowns as reported by the media, civil society organizations, and activists. As the image below illustrates, when governments shut down the internet citing "public safety," it is often evident to observers that, in reality, authorities may fear protests and cut off access to the internet to limit people's ability to organize and express themselves, whether online or off. The data reveal that when authorities cite "fake news," rumors, or hate speech, they are often responding to a range of issues including protests, elections, communal violence, and militant activity, among others. Using these threats as scapegoats, it appears that governments are leveraging shutdowns to shape the political narrative and control the flow of information.

Justifications vs. actual causes



2.3 Increased shutdowns to "fight 'fake news,' hate speech, and related violence"

Many governments shut down the internet as a response to violence related to the spread of misinformation and disinformation. In 2018, Ethiopia, India, Nigeria, and Sri Lanka imposed internet shutdowns, citing as the rationale the spread of information on social media believed to incite communal violence. Out of 35 such cases in 2018, authorities in India were responsible for cutting access to the internet 31 times in attempts to stop communal violence.

In this category of shutdown, there are notable cases in Sri Lanka and India.

CASE STUDY: SRI LANKA

In the town of Ambatenna in Sri Lanka, mobs armed with "sticks, stones, and petrol bombs" burned down and vandalized homes and businesses in the Muslim community. The attackers, reportedly from a Sinhalese Buddhist community, targeted the Muslim minority. They used Facebook, WhatsApp, and Viber to spread rumors about Muslims and instigate the attacks. Authorities in Sri Lanka, seeking to end the violence, blocked access to Facebook, WhatsApp, and other social media platforms for more than a week.

CASE STUDY: INDIA

India also repeatedly disrupted access to the internet and mobile services in an attempt to curb communal violence after false information was circulated. In these contexts, an altercation between different communities can take on a life of its own on social media, resulting in the targeted attack of one community by another. For instance, authorities shut down internet services twice in two North Eastern regions of India in an attempt to stop the rumors of child-lifting gangs[6] that led to a series of lynchings, with more than 30 deaths. It is important to note that the spread of false information and triggering of violence poses critical challenges to governments and citizens. Research indicates that social media blocking like the ones exhibited in India can suddenly change "a predictable situation into one that is highly volatile, violent, and chaotic."[7] Moreover, shutting down the internet is an inherently disproportionate response. It often leaves vulnerable people without access to information that could potentially save their lives.

3. Governments continue using shutdowns in response to critical events

3.1 Elections

Elections are the pillar of a democratic society and are often an indicator of the civic and economic rights of citizens. The free flow of information and expression during electoral periods builds public trust and facilitates transparent and fair elections. The internet is an essential enabler of access to information and expression. Governments have nevertheless become increasingly prone to tampering with the integrity of the internet before, during, and after elections. For instance, Bangladesh and the Democratic Republic of Congo shut down the internet during and after elections (respectively), under the rationale that disgruntled groups might disseminate fake results. In both Bangladesh and the DRC, the election results were ultimately contested. In the DRC, there were so many reports of rigging that the United States levied sanctions[8] against the election authorities.

[6] Singh, B. (2019). *With rumours spreading fast, Tripura suspends mobile services for the next 48 hours*. The Economic Times. Available at: https://economictimes.indiatimes.com/news/politics-and-nation/with-rumours-spreading-fast-tripura-suspends-mobile-services-for-the-next-48-hours/articleshow/64782782.cms?from=mdr

[7] Rydzak, J. "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India." Available at SSRN: https://ssrn.com/abstract=3330413

[8] Reuters. (2019). *U.S. sanctions Congo election officials, says they obstructed vote*. Available at: https://in.reuters.com/article/congo-election-usa-sanctions-idINKCN1R22IZ

CASE STUDY: DEMOCRATIC REPUBLIC OF CONGO

Just after voting ended on December 30, 2018, authorities in the Democratic Republic of Congo shut down the internet and disabled SMS texting, "fearing" the spread of false election results. The internet and SMS shutdown lasted for more than 20 days and during this shutdown, the media reported election fraud[9] that went almost unnoticed. It appeared that the opposition leader, Martin Fayulu, had won the election by decisive margins; however, the election authority awarded victory to Flexi Tshisekedi, even as many independent groups, including the Catholic Church and members of the media, highlighted mismanagement of the elections and potential rigging[10] in favor of the candidate approved by the former President Joseph Kabila.

3.2 Protests

Protests, like other significant political events, are often a spur for internet shutdowns. Notable protests that triggered internet shutdowns in 2018 took place in Nicaragua, Sudan, and the Democratic Republic of Congo.

CASE STUDY: NICARAGUA

Nicaragua's spontaneous protests have left more than 280 people dead and more than 2,000 injured,[11] and amidst these crucial movements, the government cut internet connection in major regions including Jinotega, Matagalpa, Leon, and Masaya, among others.[12] Although these shutdowns lasted for just about a day, reports indicate that the shutdowns were coordinated with attacks by government forces against civilians that left many casualties.[13

Just a few days before the New Year, Sudan was rocked by protests. As the protests engulfed the country, Sudanese authorities blocked access to social media sites including Facebook, WhatsApp, and Twitter. The first round of shutdowns lasted eight days (December 20-28, 2018) and then continued, on and off, until February 2019.

The Democratic Republic of Congo is one of the most frequent culprits imposing internet shutdowns, especially during social unrest. For instance, DRC shut down the internet three times in 2018, and two of the shutdown incidents we documented took place during protests. The first round was in January 2018 and lasted for about three days, and the next came a month later, in February 2018, when people took to the streets to denounce President Kabila's decision to postpone elections for another year.

3.3 Cheating during school exams

Algeria, Bangladesh, India, Iraq, and Syria frequently carry out internet shutdowns during school exams, and in the case of India, during police constable entrance exams. The justification for this kind of shutdown is to prevent cheating. Some countries impose a curfew-style internet blackout, where the internet is turned off all across the country during exams, then turned back on when exams end.

It is understandable that the advent of social media and smartphones have made exam administration and cheating complicated and difficult to thwart. However, cutting internet access is a disproportionate response, especially if it disconnects the whole country and impacts everyone, outside proper legal basis. Moreover, in our observation of shutdown incidents over the past four years, we have seen that the countries that shut down the internet for exams are more likely to cut access during protests, elections, and for information control. For instance, Iraq shut down the internet more than seven times in 2018. Out of these seven incidents, only three were attributed to exams. The remaining four were ordered in elections, protests, and other occasions in attempts to control the flow of information. For this reason, one shutdown often acts as a catalyst for more shutdowns, and we call for greater scrutiny to this phenomenon of exam-based disruptions.

[9] France24. (2019). DR Congo presidential vote plagued by fraud, media investigation finds. Available at: https://www.france24.com/en/20190117-dr-congo-election-fraud-kabila-fayula-tshisekedi

[10] Reuters. (2019). *How Kabila's election strategy unravelled in Congo.* Available at: https://af.reuters.com/article/africaTech/idAFKCN1PD0GJ-OZATP

[11] Aljazeera.com. (2019). *Nicaragua unrest: What you should know.* Available at: https://www.aljazeera.com/news/2018/05/nicaragua-protests-180530130717018.html

[12] [13] NetBlocks. (2019). *Regional internet disruptions in Nicaragua amid protests.* Available at: https://netblocks.org/reports/nicaragua-regional-internet-disruptions-amid-protests-gdAmMvA9

4. Who from the government orders shutdowns? Who's affected?

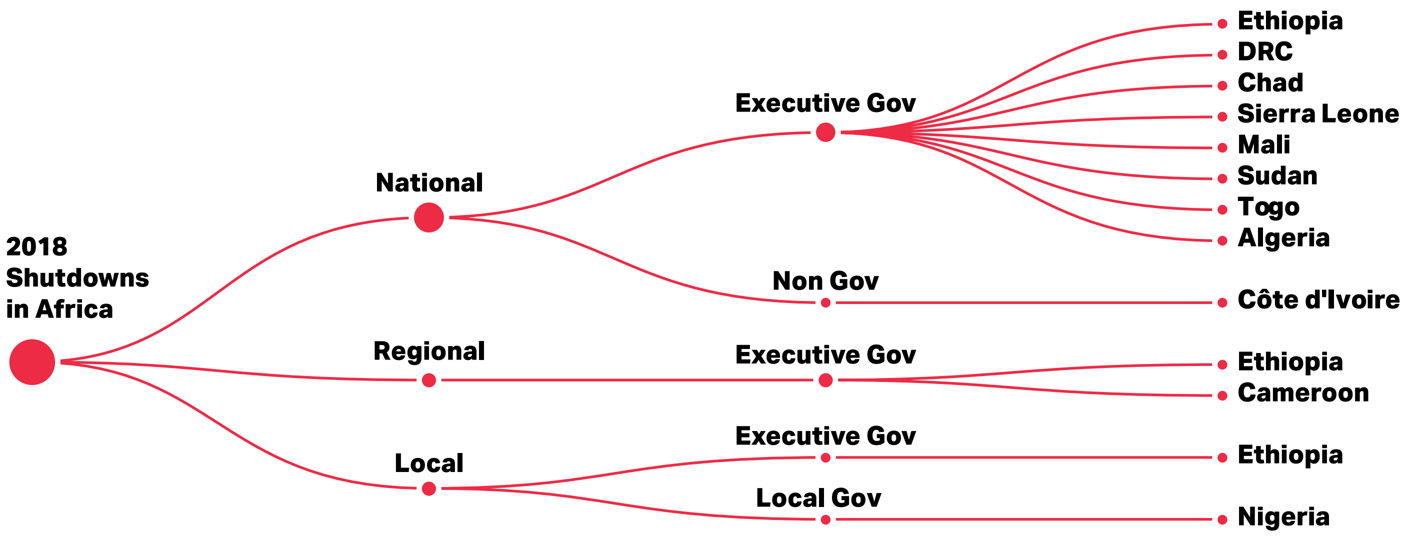
4.1 Shutdown orders and scope

In many African countries that shut down the internet, the shutdown orders come from the helm of power. Of the 21 countries that shut down the internet in the African continent, it is only in Nigeria's Jos North and Jos South that the local government was responsible for ordering shutdowns; elsewhere, these orders were issued via the executive or by central governments. With the exception of Ethiopia, the African countries that suspended the internet in 2018 typically have an authority that regulates the telecommunications sector, yet in many cases the communications regulator did not make an official statement about the shutdowns or provide a justification. Algeria, which shut down the internet in 2018 for school exams, was the only country that gave any notice before imposing a shutdown, and the only one to give clear information about when, why, and for how long the internet would be cut off.

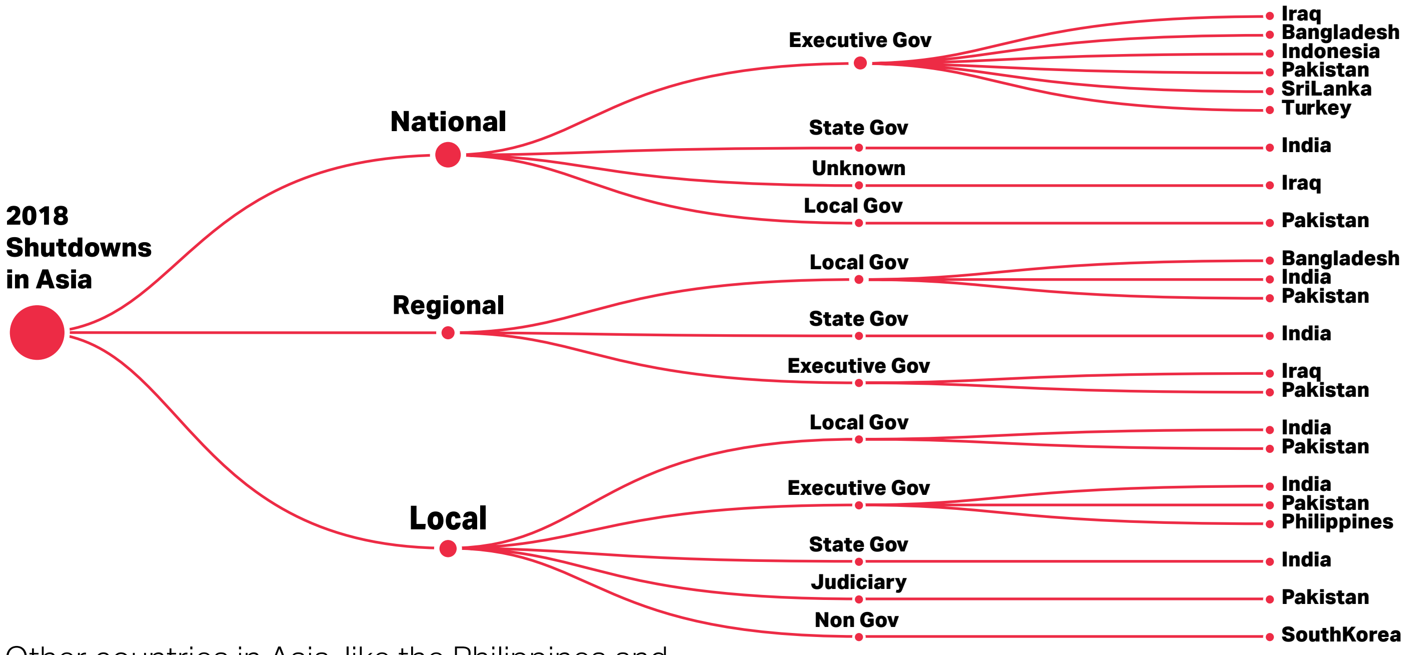
In contrast, in the Asian countries that frequently disrupt the internet, the decision makers are often much more diverse. For instance, in Pakistan, in cases where we were able to identify the decision maker, we saw that multiple actors are frequently involved: the Ministry of Interior, the federal government, the Ministry of Information and Broadcasting, the military, the Islamabad High Court, and others, have each ordered shutdowns. These actors appear to have the power to order different types of disruptions: countrywide shutdowns, regional disruptions that affect more than one city, and localized shutdowns that affect specific neighborhoods.

However, there are exceptions to this "rule." In Bangladesh, documented shutdowns almost always affect more than one city, and 80% of the time affect the entire nation. In addition, they are ordered in most cases by the national government, and the Bangladesh Telecommunication Regulatory Commission (BTRC) often provides clear and transparent communications about, or orders for, shutdowns. In Iraq, shutdowns likewise typically affect more than one city, and 85% of the time, affect one region or more. In contrast to Pakistan, in Iraq the shutdown orders come from the federal government.

Shutdown orders and scope in Africa in 2018



Shutdown orders and scope in Asia in 2018

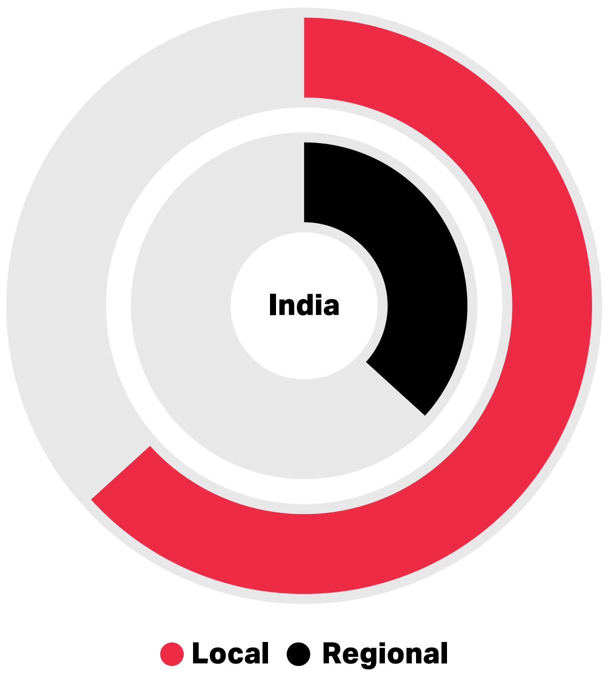


Other countries in Asia, like the Philippines and Sri Lanka, have had shutdowns in 2018 that were ordered by the executive government. While the disruption in the Philippines was localized to certain neighborhoods, Sri Lanka had a nationwide shutdown.

In India, 62% of the shutdowns were restricted to just one city, while 36% affected more than one city, but were restricted to a single state. In 2018, there was only one shutdown that affected more than one state in India.

Understanding the rules governing shutdowns provides context for what is happening in India. In August 2017, the Government of India issued the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017[14] under the Indian Telegraph Act, 1885. Central and state governments follow these rules to issue shutdown orders. If the central government issues an order, it comes from the Secretary in the Ministry of Home Affairs, and if a state orders it, it comes from the Secretary to the State Government. The Superintendent of Police or an officer of equivalent rank directs the service provider to carry out the order. Prior to the introduction of these rules, the government relied on Section 144 of the Code of Criminal Procedure, under which the District Magistrate had been authorized to issue shutdown orders.

Shutdown scope in India in 2018



[14] Dot.gov.in. (2019). Available at: http://dot.gov.in/sites/default/files/Suspension%20Rules.pdf

4.2 Grounds for shutdowns

Countries like India which have laws that facilitate and legalize shutdowns tend to order more shutdowns. India's current regulations, described in the section above, allow temporary internet shutdowns for "public emergency" or "public safety." Such broad and vague grounds for cutting access can easily lead to misuse or abuse of this shutdown authority, and indeed, year after year, India tops the list globally for the number of disruptions. However, not all states in India order the same number of shutdowns. Some states, specifically Jammu and Kashmir, Rajasthan, Uttar Pradesh, and Maharashtra, together imposed more shutdowns in 2018 than the other 22 states in India. Additionally, the Government of India, specifically the Department of Telecommunication, has expressed concern about the rising number of internet shutdowns state governments are ordering, slamming[15] states for suspending internet services "where public emergency and public safety were not impacted." The federal government urged state governments to "sensitize the concerned officials/agencies against precipitate actions leading to shut down of internet services."

> **In other places, such as Ethiopia, Sudan, and Mali, the government or the telecom service providers only rarely provide information about the orders or directive to shut down the internet, and seldom publicly recognize shutdowns. That puts the burden of proof on the victims of a shutdown to show that the internet has been disconnected intentionally and not by accident.**

Understanding who orders a shutdown is important because in our fight to end internet disruptions and defend human rights, we can tailor our policy and advocacy messages to target the right entity to apply pressure. Some countries have explicit regulations for internet shutdowns, while others order shutdowns without such clarity. In Pakistan, the Ministry of Interior issues directives that define the range, extent, duration, and, at times, the justification for a shutdown. These directives, even when they are used inappropriately, do give those of us challenging shutdowns some transparency and therefore an avenue for pushing back.

In other places, such as Ethiopia, Sudan, and Mali, the government or the telecom service providers only rarely provide information about the orders or directive to shut down the internet, and seldom publicly recognize shutdowns. That puts the burden of proof on the victims of a shutdown to show that the internet has been disconnected intentionally and not by accident. Clearly, just because a telecom or government does not acknowledge a shutdown, it does not mean it did not happen. Civil society organizations are finding innovative ways to bring transparency in these cases. For instance, when Internet Sans Frontières sued telecommunication companies and the communications regulator in Chad,[16] where authorities had blocked access to social media for more than 330 days and continuously throttled bandwidth, the companies disclosed to the court and the public that the order to cut access came from the communications regulator. That was an important step for accountability.

[15] Business Insider. (2019). *Internet shutdowns in India have skyrocketed — but now the Indian government wants that to stop.* Available at: https://www.businessinsider.in/internet-shutdowns-in-india-have-skyrocketed-but-now-the-indian-government-wants-that-to-stop/articleshow/67178243.cms

[16] As of the date this report was published, Chad was still blocking access to social media, so the shutdown has lasted longer than 330 days.

5. Anatomy of shutdowns

5.1 Bandwidth throttling

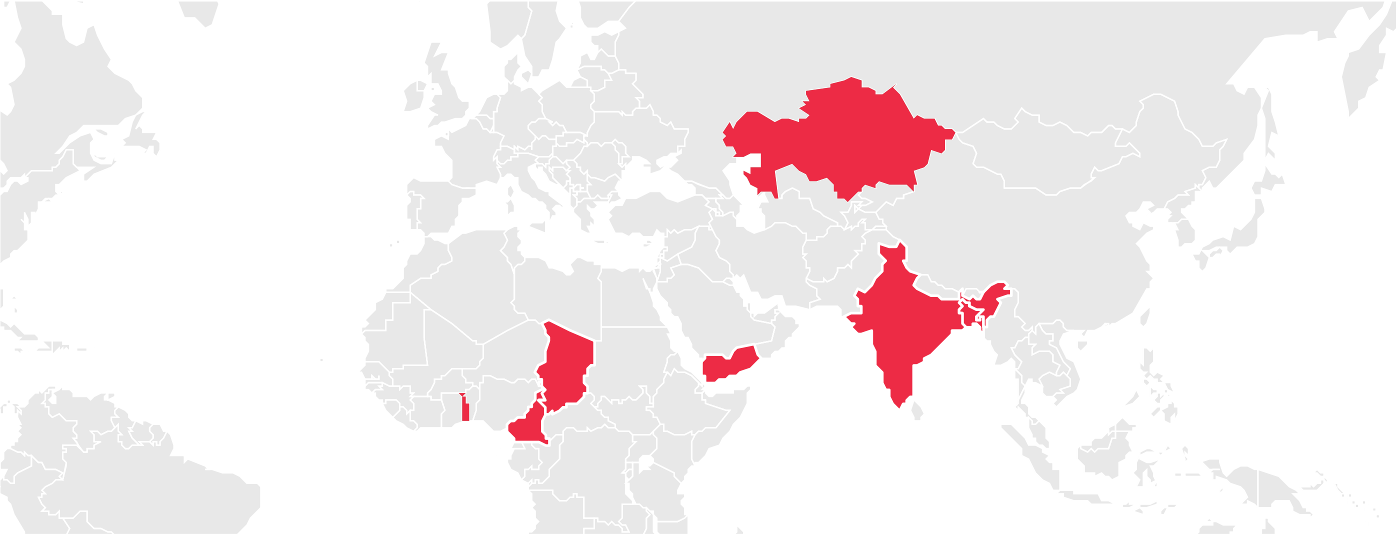
Out of the more than 196 internet shutdowns documented in 2018, about 22 were bandwidth throttling.

Bandwidth throttling is the intentional slowing of an internet service or a type of internet traffic by an internet service provider (ISP). It is employed by ISPs to regulate network traffic and ease bandwidth congestion. When one's internet bandwidth is throttled, it results in poor performance of web content or service for the user.[17]

Throttling in the context of internet shutdowns is understood to mean the intentional slowing of an internet service by an internet service provider. Bangladesh, Cameroon, Chad, India, Kazakhstan, Togo, and Yemen are perpetrators of bandwidth throttling. It is important to note that there was probably more bandwidth throttling in 2018 than we were able to document, since throttling is much harder to verify than other forms of shutdowns. Unless the throttling is exceptionally high and people are unable to upload or see images completely, many will fail to report or even to suspect intentional bandwidth tampering. In many places where shutdowns and throttling happen, access to quality internet connection is limited and the internet connection might not be stable. Therefore, it is often common to confuse throttling with an unstable and congested network.

Technically, one of the more robust ways to determine whether there is a network problem or deliberate throttling is to get a large enough data set that when viewed in its entirety, it can help rule out a network problem. A network delay is usually caused by a temporary "bottleneck" in the network, and having a large enough data set will reveal the bottleneck. Some data will be traveling fast on some routes, while traffic on others will be slower due to the bottleneck. If throttling has been applied to all traffic on the network, slowness will be pervasive, with multiple bottlenecks at every key point necessary to affect traffic on the network as a whole (this is not likely to be an accidental or unintended incident). Even if the technical tests for throttling are simplistic (usually simply recording the time it takes to make a request, and to get a response from a remote server), researchers may not get enough data on the affected network to see what is really going on.

Countries most affected by bandwidth throttling in 2018



[17] Bracci, A & Petronio, L. (2019). *New research shows that, post net neutrality, internet providers are slowing down your streaming*. Available at: https://news.northeastern.edu/2018/09/10/new-research-shows-your-internet-provider-is-in-control/

While the throttling data we have documented is scant compared to information on the other forms of shutdowns, we can see still see some patterns and trends. For instance, in some contexts, there is deliberate throttling of both broadband and mobile internet; while in others, there is deliberate slowing of access to only mobile internet and social media platforms. In contexts where the throttling is official, we have noted that 4G and 3G mobile internet is downgraded to a 2G connection. Normally, a 4G and 3G connection will render 100mb/s and 3.1mb/s of data, respectively, while a 2G connection will only transmit 14.4kb/s. Downgrading mobile internet connections to 2G will effectively make it almost impossible to upload pictures, stream live, and share information quickly.

In addition to being hard to detect, throttling does not take countries "off the grid" entirely, and many suspect that more and more governments will therefore resort to this kind of shutdown as a way to escape accountability. However, whether or not government authorities and providers are open about it, throttling make the internet "effectively unusable," satisfying the definition of an internet shutdown and causing the same kind of damage to human rights, public safety, and the economy.

CASE STUDY: KAZAKHSTAN

Since March of 2018, authorities in Kazakhstan have throttled the internet almost daily for about an hour, whenever Mukhtar Ablyazov, the leader of the opposition group Democratic Choice of Kazakhstan, is streaming on Facebook Live.[18] Once Mr. Ablyazov goes online, users report being unable to view or upload pictures/videos on Facebook Live, YouTube, Twitter, Instagram, Vkontakte, Odnoklassniki, and other social media platforms.[19]

5.2 Broadband internet shutdowns

In 2018, broadband internet shutdowns — that is, cuts to internet access via broadband, such as in a home, office, or business — were accompanied by mobile internet shutdowns. No country shut down access via broadband without also cutting off access to mobile device networks. The spread of cheap smartphones has made mobile internet and networks ubiquitous across many countries and regions, and in the majority of the countries where people experience internet disruptions, they are connecting using smartphones. Therefore, it often has more impact to shut down mobile internet than broadband internet.[20]

5.3 Mobile internet shutdowns

There were at least 63 mobile internet shutdown incidents in 2018. In these cases, we looked at which countries cut access to mobile data but left broadband internet intact. In Africa, Ethiopia shut down mobile internet the most. In Asia, India again heads the list, followed by Pakistan and the Philippines. In Europe, Russia suspended just mobile internet in some regions of the country.

CASE STUDY: INGUSHETIA, RUSSIA

Ingushetia, located in the North Caucasus region and a federal subject of the Russian Federation, experienced mobile internet shutdowns that lasted for two weeks in October 2018. The **government suspended mobile internet**[21] as protests against the new border deal with Ingushetia and Chechnya were announced.

[18] Kumenov, A. (2019). *Kazakhstan is throttling the internet when the president's rival is online.* Available at: https://eurasianet.org/kazakhstan-is-throttling-the-internet-when-the-presidents-rival-is-online
[19] Freedomhouse.org. (2019). *Kazakhstan Country Report | Freedom on the Net 2018.* Available at: https://freedomhouse.org/report/freedom-net/2018/kazakhstan
[20] GSMA. (2018) *2018 Mobile Industry Impact Report: Sustainable Development Goals.* Available at: https://www.gsmaintelligence.com/research/?file=ecf0a523bfb1c9841147a335cac9f6a7&download
[21] №195, Г., Инютин, В. and Новый, В. (2019). Роскомнадзор просят разобраться с ингушской связью. Kommersant.ru. Available at: https://www.kommersant.ru/doc/3779096#id1655735

5.4 "Internet blackouts" or blanket internet shutdowns

More countries are cutting access to the internet entirely, leaving people disconnected for days at a time. In 2018, 14 countries imposed blanket internet shutdowns, also called an "internet blackout." Of these 14 countries, Algeria, the Democratic Republic of Congo, India, and Pakistan also employed other kinds of interference with access to information, blocking social media, throttling the internet, or disabling SMS texting.

CASE STUDY: OROMIA, ETHIOPIA

An internet blackout that took place in Ethiopia in 2018 was not the first time the country had disrupted access to the internet, but the first time it cut access to both mobile and broadband networks for an extended period. Targeting Oromia, the biggest region of the country, **this shutdown lasted**[22] for 40 days and forced many to travel to Addis Ababa or other parts of the country to access the internet.

5.5 Mobile phone call and text message network shutdowns

Cutting mobile phone calls and text messages is not common. In Pakistan, there were two such incidents in 2018. The government and the judiciary each ordered a mobile phone shutdown, and each incident lasted for about five hours. The Democratic Republic of Congo and India also cut phone and SMS texting service in 2018.

5.6 Service-specific (platform) shutdowns

Social media platforms have decentralized who can create and share news and information and reach a large audience. This relatively recent phenomenon has challenged the power governments traditionally have had over the "accepted" narrative. However, as much as these platforms have given citizens the capacity to share information, they can also be leveraged as tools for misinformation and disinformation (notably, also by governments themselves). In 2018, government authorities have responded to the problems arising from the spread of misinformation or disinformation with blunt, disproportionate blocking or throttling of access to social media platforms. There were 14 such documented incidents. In Algeria, Bangladesh, Indonesia, Iraq, Mali, Nigeria, Pakistan, Russia, Sri Lanka, Sudan, Turkey, and Yemen, authorities shut down at least one social media platform in 2018.

For instance, Mali cut access to social media platforms including Facebook, WhatsApp, and Twitter under the pretext of fighting misinformation and disinformation during elections. Iraq, Indonesia, Turkey, and Russia all blocked Telegram.

6. Human rights violations during shutdowns

In addition to directly infringing the right of access to information and freedom of expression, internet shutdowns can hide grave human rights violations. Research has shown that internet shutdowns often occur in conjunction with higher levels of state repression[23], and with an increase in violent protest.[24] In 2018, there were at least 33 incidents

[22] Rahman, A & Shaban, A. (2019). *Unexplained internet blackout in Ethiopia's Oromia region | Africanews.* Available at: https://www.africanews.com/2018/03/21/unexplained-internet-blackout-in-ethiopia-s-oromia-region/

[23] Gohdes, Anita R. "Pulling The Plug Network disruptions and violence in civil conflict". *Journal Of Peace Research*, vol 52, no. 3, 2015, pp. 352-367. *SAGE Publications,* doi:10.1177/0022343314551398. Accessed 7 June 2019.

[24] Rydzak, J. "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India." Available at SSRN: https://ssrn.com/abstract=3330413

of state violence reported during internet shutdowns. It appears that in some cases, governments and law enforcement may cut off access to the internet to unleash violence on citizens with impunity. In Sudan, protesters have become victims to state violence under the "cover" of shutdowns.

CASE STUDY: KAZAKHSTAN

For months on end in 2018, Sudan was rocked by massive protests across the country. A movement that appears to have started in the capital of Khartoum over soaring food prices and high inflation rates gripped the whole country. In response, the Sudanese government blocked social media and perpetrated violence on protesters. Between December 19th and the 30th, more than 60 protesters were killed, and hundreds of peaceful protesters and opposition leaders were arrested.[25] In April 2019, these mass protests forced former President Omar al-Bashir to step down.

7. Challenging shutdowns by global governmental and industry bodies

Institutions across the globe speak out against internet shutdowns. The UN General Assembly has condemned disruptions that violate international human rights law. The African Commission on Human and Peoples' Rights, and the 30 governments in the Freedom Online Coalition (FOC), have addressed shutdowns.

Private firms have made statements against shutdowns through the Global Network Initiative and entities like the GSM Association and Internet Society produce guidance on preventing and mitigating intentional disruptions.

Resolutions, statements, and declarations by intergovernmental bodies regarding internet shutdowns and related disruptions

2018

- **The promotion, protection and enjoyment of human rights on the Internet (Updated)**
UN Human Rights Council, adopted by consensus
- **The promotion and protection of human rights in the context of peaceful protests**
UN Human Rights Council, adopted by consensus
- **Promotion and protection of human rights and fundamental freedoms, including the rights to peaceful assembly and freedom of association**
UN General Assembly, adopted by vote

2017

- **The safety of journalists and the issue of impunity**
UN General Assembly, adopted by consensus

> "Condemns unequivocally measures in violation of international human rights law aiming to or that intentionally prevent or disrupt access to or dissemination of information online and offline, aiming to undermine the work of journalists in informing the public, and calls upon all States to cease and refrain from these measures, which cause irreparable harm to efforts at building inclusive and peaceful knowledge societies and democracies."

- **Joint statement on state sponsored network disruptions**
The Freedom Online Coalition

2016

- **Resolution on the right to freedom of information and expression on the internet in Africa**
African Commission on Human and Peoples' Rights
- **The promotion, protection and enjoyment of human rights on the Internet**
UN Human Rights Council, adopted by consensus

2015

- **Joint declaration on freedom of expression and responses to conflict situations**
Organization for Security and Co-operation in Europe (OSCE)

2011

- **Joint declaration on Freedom of Expression and the internet**
Inter-American Commission on Human Rights, Organization of American States (OAS)

[25] Maclean, R. (2019). *Dozens have been killed by the regime. But Sudan's protesters march on.* the Guardian. Available at: https://www.theguardian.com/world/2018/dec/30/dozens-have-died-but-sudan-protesters-march-on

8. Challenging shutdowns on legal grounds

In 2018, those affected by internet shutdowns have brought the perpetrators to court, notably in Chad, Cameroon, India, Pakistan, and Togo. These challenges were brought with the support of actors including civil society organizations, members of the public, and public interest lawyers.

CASE STUDY: CHAD

Internet Sans Frontières (ISF) brought a case against the two telecom operators,[26] Airtel and Tigo, and the telecommunications regulator for cutting access to social media platforms. ISF did not prevail in the case and the telecommunications regulator did not show up in court,[27] but the challenge nevertheless brought new transparency to this ongoing shutdown. The telecom companies told the court that the order for the shutdown came from the regulator. This provides information to enable additional challenges, advocacy, and pressure in Chad, where the victims of this shutdown are still forced to use virtual private networks (VPNs) to access social media platforms.

CASE STUDY: INDIA

India has the highest number of shutdown incidents in the world, but only a few legal challenges have been filed in opposition. The most recent victory came thanks to a legal challenge brought before the Jodhpur High Court in the State of Rajasthan.[28] Petitioners filed a successful Writ petition arguing that Rajasthan cannot suspend mobile services for a police constable recruitment examination, as it is beyond the scope of the Temporary Suspension of the Telecom Services (Public Emergency and Public Safety) Rules of 2017. This case is an important win because it barred Rajasthan from imposing future mobile internet shutdowns during examinations. In its reply to the court, Rajasthan submitted that its Department of Home Affairs had issued a set of instructions[29] to all the divisional commissioners to cease shutting down the internet during exams.

There were also challenges to internet shutdowns in the Indian Parliament. During the Monsoon Session of the Parliament in 2018, Dr. Husain Dalwai, Member of Parliament in the Rajya Sabha (Upper House), filed a statutory motion[30] for annulment of the aforementioned rules that enable the government to shut down the internet in India. In addition, MPs from both Houses of Parliament asked a number of questions about internet shutdowns, demonstrating understanding of the importance of this issue for Indians.

9. Circumventing and measuring shutdowns in 2018

The #KeepItOn coalition has been working together to verify and document shutdowns, and to help victims circumvent them. Providing direct technical assistance to those affected by shutdowns are Access Now's Digital Security Helpline[31], Code for Africa[32], and other digital security groups.

[26] Ecofin, Agence. *Tchad: Un Collectif D'Avocats Et Internet Sans Frontières Pressent L'Etat Pour Qu'Il Rétablisse L'Accès Aux Réseaux Sociaux*. Agence Ecofin, 2019, Available at: https://www.agenceecofin.com/reseaux-sociaux/2408-59389-tchad-un-collectif-d-avocats-et-internet-sans-frontieres-pressent-l-etat-pour-qu-il-retablisse-l-acces-aux-reseaux-sociaux
[27] *Tchad: La Justice Se Penche Sur Une Plainte Suite Aux Coupures Des Réseaux Sociaux*. RFI Afrique, 2019, Available at: http://www.rfi.fr/afrique/20180920-tchad-justice-penche-une-plainte-suite-coupures-reseaux-sociaux
[28] *Home Department, State Of Rajasthan: No More Internet Shutdowns For Prevention Of Cheating In Examinations*. SFLC.In, 2019, https://sflc.in/home-department-state-rajasthan-no-more-internet-shutdowns-prevention-cheating-examinations
[29] *Additional Affidavit - Translated Copy Of Pages 110-112*. Google Docs, 2019, https://docs.google.com/document/d/1fTyVkRx99kBvRPLuEaWZB2w2XRRChJkN1edD39YRc3E/edit
[30] *Bulletin-II*. Archive.Is, 2019, https://archive.is/cgJ11#selection-143.36-151.2
[31] Digital Security Helpline, Access Now, 2019, https://www.accessnow.org/help/
[32] Code For Africa, Codeforafrica.Org, 2019, https://codeforafrica.org

It's not possible to circumvent blanket internet shutdowns without building alternative sources of internet access, but most communities can circumvent blocking of some services and social media platforms. That is why members of the #KeepItOn coalition work to provide and disseminate customized circumvention tips when a government orders, or is likely to order, a shutdown.

Examples of the circumvention tools shared by #KeepItOn coalition

FREE

PSIPHON
A must-have to circumvent the censorship

AVAILABLE ON

- Android 4.4 and up
- iOS 10.2 and up
- Windows (XP/Vista/7/8/10)

TO DOWNLOAD AND USE
https://psiphon.ca/

FREE

LANTERN
Fast, reliable, and secure access to the open internet

AVAILABLE ON

- Android 4.1 and up
- Windows (XP/SP/3)
- OSX 10.8 and up
- Ubuntu

TO DOWNLOAD AND USE
https://getlantern.org/

FREE 500
DATA/MO

TUNNELBEAR
A VPN that enables private browsing with no logging

AVAILABLE ON

- Android 4.1 and up
- iOS 8 and up
- Windows 7 and up
- MacOS 10.10 and up

Also available as browser extensions
Chrome | Firefox | Opera

TO DOWNLOAD AND USE
https://www.tunnelbear.com/

Monitoring and verifying internet shutdowns is essential for documenting them and pushing back. There are a number of groups in the #KeepItOn coalition that continuously monitor internet traffic, testing for blocking, throttling, and blackouts, so that these attacks on human rights do not go unopposed anywhere around the world. They include Oracle's Dyn Internet Intelligence Map, Internet Outage Detection and Analysis (IODA), the Open Observatory of Network Interference (OONI), and NetBlocks. These and other groups are doing enormously valuable work collecting technical evidence and shedding light on the nature of internet shutdowns, strengthening the effort to stop them. For example, NetBlocks worked to document throttling and social media shutdowns in Chad, which bolstered the legal challenge[33] that provided more transparency to how they're carried out. Similarly, we have used the measurement community's evidence to submit reports to the United Nations and other intergovernmental processes helping us hold states accountable.

Measuring and monitoring tools and resources from the #KeepItOn community

Shutdown Tracker Optimization Project (STOP)
Access Now's contextual tracker of internet shutdown instances around the world

Shutdown Stories Project
Access Now's database of documented personal narratives from people who are impacted by the disruptions of communications and access to information

Who Owns What? The WOW telco database
Access Now's catalog of GSM Association (GSMA) member mobile operators in countries with shutdown issues

Open Observatory of Network Interference (OONI)
A free software, global observation network for detecting censorship, surveillance, and traffic manipulation on the internet

The Cost of Shutdown Tool (COST)
NetBlocks' data-driven online tool that enables users to quickly and easily estimate the economic cost of internet disruptions

internetshutdowns.in
An online tool by Software Freedom Law Centre, India to monitor internet shutdowns in India with a reporting platform

Kill Switch in Pakistan
Bytes for All's active monitor of internet shutdowns in Pakistan

Measurement Lab (M-Lab)
A consortium of research, industry, and public-interest partners dedicated to providing an open, verifiable measurement platform for global network performance, hosting the largest open Internet performance dataset on the planet, and creating visualizations and tools to help people make sense of Internet performance

Internet Outage Detection and Analysis (IODA)
An operational prototype system that monitors the internet in near-real time, developed by Center for Applied Internet Data Analysis (CAIDA)

[33] *Chad: Revelations On The Extent Of Social Media Censorship.* Internet Sans Frontières, 2019, https://internetwithoutborders.org/chad-revelations-on-the-extent-of-the-social-media-censorship/

CONTACT

For questions and more information, please visit https://www.accessnow.org/keepiton/

Or reach out to
Berhan Taye at **berhan@accessnow.org**
Melody Patry at **melody@accessnow.org**
Peter Micek at **peter@accessnow.org**

THE STATE OF INTERNET SHUTDOWNS AROUND THE WORLD

THE 2018 #KEEPITON REPORT

#KeepItOn