Bangladesh: September 2029 - August 2020

Belarus: August - December 2020

Ethiopia: June - August 2020

Myanmar: June 2019 - Ongoing

India: August 2019 - January 2020

Yemen: July 2020 -

SHATTERED DREAMS AND LOST OPPORTUNITIES

A year in the fight to #KeepItOn

#KeepItOn

A note on our data

This #KeepItOn report looks at incidents of internet shutdowns in 2020. While we try to be comprehensive, 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 unnoticed or unreported, and numbers are likely to change if and when new information becomes available. For further reading, please visit https://accessnow.org/keepiton-2020-data-methodology.

March 2021

#KeepItOn

The #KeepItOn campaign unites and organizes the global effort to end internet shutdowns. The coalition is growing rapidly, and so far 243 organizations from 105 countries around the world have joined the movement, ranging from research centers to rights and advocacy groups, detection networks, foundations, and media organizations.

This report is a publication of Access Now for the #KeepItOn coalition and was written by Berhan Taye in collaboration with the Access Now team.

The author would like to specially thank Rafael Bezerra Nunes, Felicia Anthonio, Sage Cheng, Peter Micek, Natalia Krapiva, Donna Wentworth, Carolyn Tackett, Raman Jit Singh Chima, Laura O'Brien, Verónica Arroyo, Alexia Skok, Eric Null, Jennifer Brody, Isedua Oribhabor, Marwa Fatafta, Dima Samaro, Bridget Andere, Melody Patry, and Gustaf Björksten for their contributions. She would like to thank Data4Change, the Software Freedom Law Center India (SFLC.in), Yodet, VeSinFiltro, Southeast Asia Freedom of Expression Network (SAFEnet), and other members of the #KeepItOn coalition for providing valuable information about case studies, reviewing data and sources, and contributing to the report.

Table of contents

I. Internet shutdowns in 2020: a global overview 2
- Regional and country-specific details 4
- The impact of internet shutdowns in the year of COVID-19 6
    1. Lost opportunities and dreams 6
    2. Information saves lives, now more than ever 6

II. Trends in 2020 7
- Dissecting an internet shutdown 8
    1. Throttling 8
    2. Mobile and broadband internet and service shutdowns 9
- How did they justify the shutdown? 10
- What triggers a shutdown? 12
    - Fighting “fake news” or “illegal content” at any cost 14
- Human rights violations and violence during shutdowns 15
- Crackdown on the use of VPNs 16

III. Internet shutdowns during elections and protests 17
- Elections and shutdowns 17
- Protests and network disruption 18

IV. New countries added to the shame list 19
- Cuba 19
- Tanzania 20
- Kenya 21

V. Who stood out in 2020? 21
- Yemen: ICT infrastructure a war bargaining chip 21
- Belarus: 121 days of internet shutdowns 22
- 355 days of internet shutdowns in Rohingya refugee camps in Bangladesh 23
- Myanmar: 19 months and counting 24
- India entrenches use of shutdowns to suppress protests, cuts off Jammu and Kashmir 26
- The threat of an internet shutdown in the United States 28
- International organizations standing against shutdowns 28

VI. Enabling and profiting from censorship: the case of Sandvine and Allot 29

VII. Challenging internet shutdowns on legal grounds: the case of Togo and Indonesia 31
- Challenges and opportunities 32
    1. #KeepItOn challenges and opportunities **32**
    2. Lessons learnt 33

I. Internet shutdowns in 2020: [redacted] a global overview [redacted]

Even as the COVID-19 pandemic swept through the world and those with access to the internet depended on it to continue with their education, communicate with loved ones, and continue to earn a living, Access Now and the #KeepItOn Coalition documented **at least 155 internet shutdown[1] incidents around the world in 29 countries**.[2] When compared to 2018 and 2019, this is a lower number of shutdowns. However, the smaller number of shutdowns is not an indication of the lessened impact of a shutdown or an overall increase in digital rights.

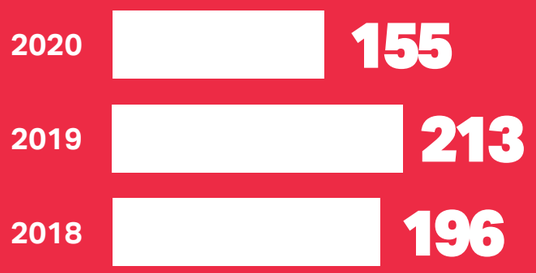
For a world that was and continues to be under lockdown or at least some forms of movement restriction, 155 intentional communication disruptions came at a high cost to the fundamental human rights of people around the world. Countries like Bangladesh, Myanmar, Yemen, Ethiopia, and others entrenched the use of shutdowns even during the COVID-19 pandemic. For instance, Ethiopia's national internet blackout affected more than 100 million people for more than two weeks during the height of the pandemic in the country. Rohingya refugees in Bangladesh implored the government of Bangladesh to turn on the internet as COVID-19 spread through the refugee camps, but they were ignored.[3] In 2019 and 2020, Myanmar perpetrated

1 An internet shutdown is "an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." An internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. Access Now (n.d.) Retrieved Jan 22, 2021, from https://www.accessnow.org/keepiton-faq/.

2 The methodology for confirming, counting, and classifying a shutdown event can be found at: Access Now (2020). *Shutdown Tracker Optimization Project (STOP) CodeBook*. Retrieved Feb 10, 2021 from https://accessnow.org/keepiton-2020-data-methodology.

3 Rohingya Students Network - RNS. (@NetworkRsn) (2020) May 15, 2020, Retrieved Jan 22, 2021 from https://twitter.com/NetworkRsn/status/1261285024478883841.

Documented internet shutdowns by year



Number of countries that shut down the internet

29 in 2020
- Africa: 10
- MENA: 8
- Asia Pacific: 6
- LatAm and the Caribbean: 3
- Europe: 2

33 in 2019
- Africa: 12
- Asia Pacific: 9
- MENA: 8
- LatAm and the Caribbean: 2
- Europe: 2

25 in 2018
- Africa: 10
- Asia Pacific: 8
- MENA: 5
- LatAm and the Caribbean: 1
- Europe: 1

* It is important the international community does not prematurely celebrate the lower number of shutdowns in 2020. Although it would take extensive research to investigate the underlying factors, it is possible this decline can be attributed to the peculiar realities of the year.

Impact of shutdowns in the COVID-19 pandemic

100 million

people were in a national internet blackout for more than two weeks in Ethiopia during the height of the COVID-19 pandemic in the country.

355+ days

of shattered and throttled internet and telecommunications affected nearly one million residents of the Rohingya refugee camps in Cox's Bazar, Bangladesh.

19 months

of mobile network restrictions impeded people from getting critical health information across nine townships in Myanmar's Rakhine and Chin states.

Every two weeks

people in Jammu and Kashmir endured yet another extension or new mobile network shutdown ordered by. the administration throughout the year of 2020.

one of the world's longest internet shutdowns, affecting some of the world's most vulnerable people. The Burmese government proceeded to expand mobile internet throttling across the nine townships in Rakhine and Chin states even as the pandemic spread, restricting residents of these townships from access to critical and life-saving information.[4] These restrictions were only lifted[5] after a military coup attempt in February 2021,[6] when factions of the Arakan National Party came out in support of the coup;[7] meanwhile, the military has continued to impose shutdowns elsewhere.[8] In Jammu and Kashmir, the administration, which is directly supervised by India's federal government as a union territory, issued internet shutdown orders every two weeks in 2020 despite concerns from doctors, journalist associations, and other residents on the additional challenges it posed to COVID response.[9]

4 Enlightened Myanmar Research Foundation (2020, September). *Rapid Situational Analysis of Covid-19 in Rakhine and Chin States*. Retrieved Jan 26, 2021, from https://www.emref.org/sites/emref.org/files/publication-docs/emref_rapid_situational_analysis_in_rakhine_and_chin_stateeng.pdf.

5 On February 3, 2021, in the days following a coup attempt by the Myanmar military, full internet access was restored in the eight townships in Rakhine and Chin states. Telenor (2021). *Network restored in eight townships in Myanmar*. Retrieved Feb 9, 2021, from https://www.telenor.com/network-restored-in-eight-townships-in-myanmar/.

6 BBC (2021, February 1). *Myanmar coup: Aung San Suu Kyi detained as military seizes control*. Retrieved Feb 10, 2021, from https://www.bbc.com/news/world-asia-55882489.

7 BNI Multimedia group (2021, February 8). *ANP says it will cooperate with coup leaders to resolve Arakan cris*. Retrieved Feb 11, 2021, from https://www.bnionline.net/en/news/anp-says-it-will-cooperate-coup-leaders-resolve-arakan-crises; The Irrawaddy (2021, February 5). *Anti-NLD Ethnic Politicians Picked by Military Regime for Governing Council*. Retrieved Feb 11, 2021, from https://www.irrawaddy.com/news/burma/anti-nld-ethnic-politicians-picked-military-regime-governing-council.html.

8 BBC (2021, February 1). *Myanmar coup: Internet shutdown as crowds protest against military*, Retrieved Feb 10, 2021, from https://www.bbc.com/news/world-asia-55960284.

9 Adi Radhakrishnan (2020 April). COVID-19: Restricted Internet Impacts on Health in Kashmir. Retrieved Feb 10, 2021, from https://www.hhrjournal.org/2020/04/covid-19-restricted-internet-impacts-on-health-in-kashmir/.

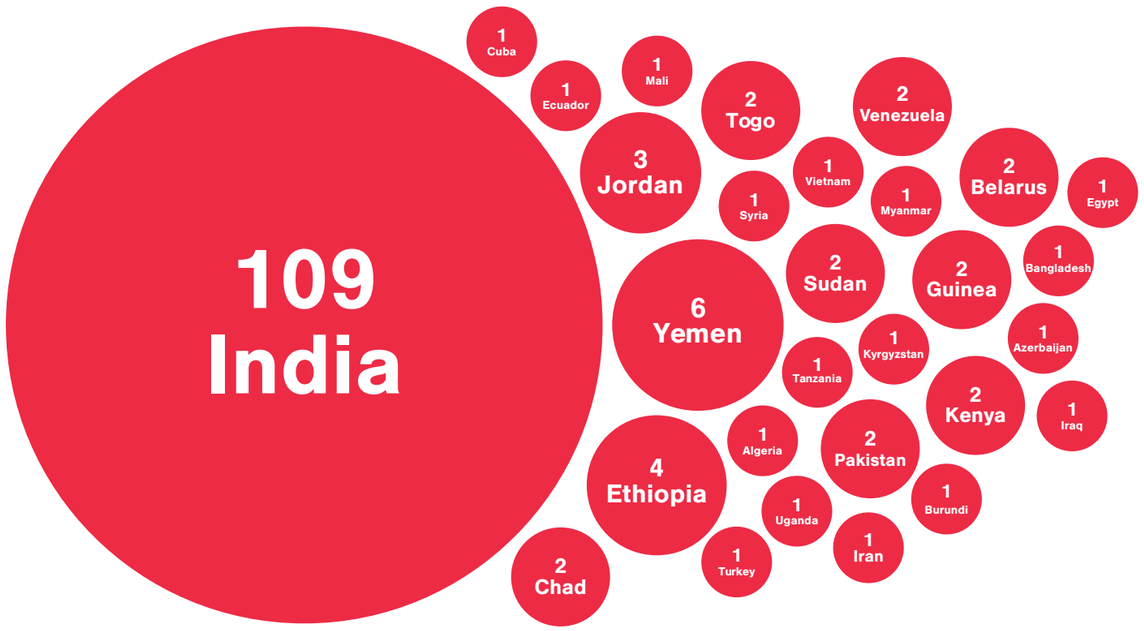
During this deadly pandemic, as billions turned to the internet to go to school, work, and communicate, new countries that have never shut down the internet before, like Tanzania, Cuba, and others, joined the internet shutdown shame list. Other countries, like Belarus, Ethiopia, and Tanzania, continued to interfere with or cut access to the internet during critical political moments such as elections and protests. In Vietnam, the government throttled Facebook, making it nearly impossible for people to access the platform.

Facebook also succumbed to demands by the authorities to take down content the government deemed illegal, putting profit before human rights in order to stay in the market.[10] In the United States, former U.S. President Donald Trump threatened to ban TikTok and WeChat if the companies did not meet his demands.[11] In Yemen, warring parties persisted in using internet infrastructure as a bargain chip for the protracted conflict in the country.

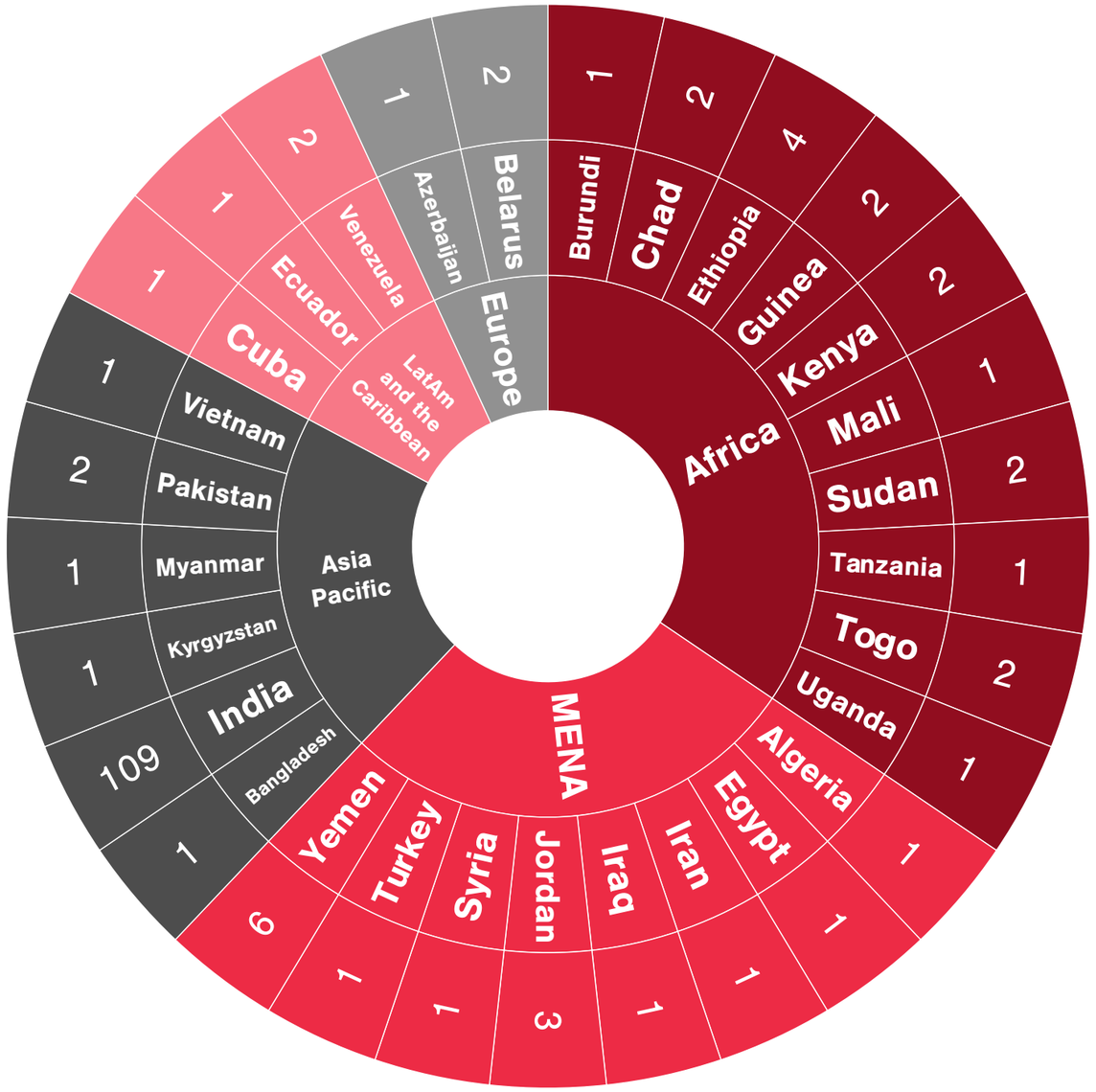
Regional and country-specific details

Number of internet shutdowns by country in 2020

Like it did in previous years, India once again topped the list of internet shutdowns with at least 109 in 2020, followed by Yemen with at least six shutdowns, Ethiopia with four, and Jordan three. India, Yemen, and Ethiopia had been among the worst disruptors of the internet in 2019.[12]



Internet shutdowns by region in 2020



- Ten countries in Africa shut down the internet 18 times.
- Eight countries in the Middle East and North Africa (MENA) shut down the internet 15 times. Yemen makes up almost half of the documented shutdowns in this region.
- Six countries in Asia Pacific shut down the internet 115 times. India alone shut down the internet at least 109 times.
- Three countries in Latin America and the Caribbean (LatAm and the Caribbean) shut down the internet four times.
- Two countries in Europe shut down the internet in 2020.

10 Vu, Khanh (2019, January 8). *Vietnam says Facebook violated controversial cybersecurity law*. Reuters. Retrieved Jan 22, 2021 from https://www.reuters.com/article/us-vietnam-facebook/vietnam-says-facebook-violated-controversial-cybersecurity-law-idUSKCN1P30AJ.

11 Access Now (2020, September 18). *Trump executive orders targeting China-linked apps fail to protect privacy, harm human rights*. Retrieved Jan 27, 2021, from https://www.accessnow.org/trump-executive-orders-targeting-china-linked-apps-fail-to-protect-privacy-harm-human-rights/.

12 Access Now (2020). *Targeted, cut off, and left in the dark: The #KeepItOn report on internet shutdowns in 2019*. Retrieved Jan 22, 2021 from https://www.accessnow.org/keepiton-2019-report.

The impact of internet shutdowns in the year of COVID-19

Internet shutdowns disrupt lives and livelihoods, damage human rights, and hurt public health and safety. The negative impact of shutdowns is deepened during COVID-19.[13] Those who have had access to the internet during the pandemic have depended on it to get the most recent and often life-saving information. Not only are those connected better able to protect themselves and stay safe, most have used the internet to work, continue their education, teach their children from home, communicate with their loved ones, get medical help information, seek employment, and so on. Those without internet access or deliberately cut off do not have these resources, and are living in fear.

1. Lost opportunities and dreams

The choice to shut down the internet during a global pandemic had a compounded effect on the most vulnerable around the world. For example, before getting cut off, the Rohingya in Myanmar could take classes online. With the shutdown and lockdown in effect, they were left without a vital pathway to get educated. In the words of one resident, "I cannot go to school in another place because I am a Muslim. The internet is the place where I can study advanced education."[14] When the shutdown came into effect, many Rohingya talked about having to pause their education, "missed opportunities," and in some cases, being "unable to dream" about their future.[15]

2. Information saves lives, now more than ever

All deliberate disruptions of the internet are an attack on human rights, but when a government imposes a blanket shutdown, where people are completely cut off from the internet, it has a deeper impact. This type of shutdown is all the more damaging during the COVID-19 pandemic. When people are cut off from the internet, they are prevented from accessing often life-saving information to protect themselves and their families. While those who are able to get online grapple with misleading information about the pandemic, its remedies, origins, and other information, ensuring open access to the internet and other media channels is critical to help people get accurate information to combat this misinformation and disinformation. In short, access to information saves lives, now more than ever.

Unfortunately, even as false information about COVID-19 spread, some governments moved to disrupt the free flow of information. In the early days of the pandemic in April 2020, as Pakistan confirmed more than 2,000 cases of COVID-19, an ongoing internet shutdown kept the residents of the former Federally Administered Tribal Area (FATA) dangerously uninformed.[16] Since June of 2016, authorities had kept more than 3.7 million people living in the FATA region deliberately in the dark.

In the Rakhine and Chin states of Myanmar, while some people who had access to the internet said they could get COVID-19-related information using radio, television, the internet, and other channels,

13 Taye, Berhan, and Felicia Anthonio (2020, March 17). *#KeepItOn: internet shutdowns during COVID-19 will help spread the virus!* Access Now. Retrieved Jan 26, 2021, from https://www.accessnow.org/keepiton-internet-shutdowns-during-covid-19-will-help-spread-the-virus/; and Human Rights Watch (2020, March 31). *End Internet Shutdowns to Manage COVID-19*. Retrieved Jan 26, 2021, from https://www.hrw.org/news/2020/03/31/end-internet-shutdowns-manage-covid-19.

14 The Peace and Development Initiative – Kintha; and Rohingya Youth Association et. al. (2021, January). *Lockdown and Shutdown Exposing the Impacts of Recent Network Disruptions in Myanmar and Bangladesh*. Retrieved Jan 22, 2021 from https://clinic.cyber.harvard.edu/files/2021/01/Lockdowns-and-Shutdowns.pdf.

15 Ibid.

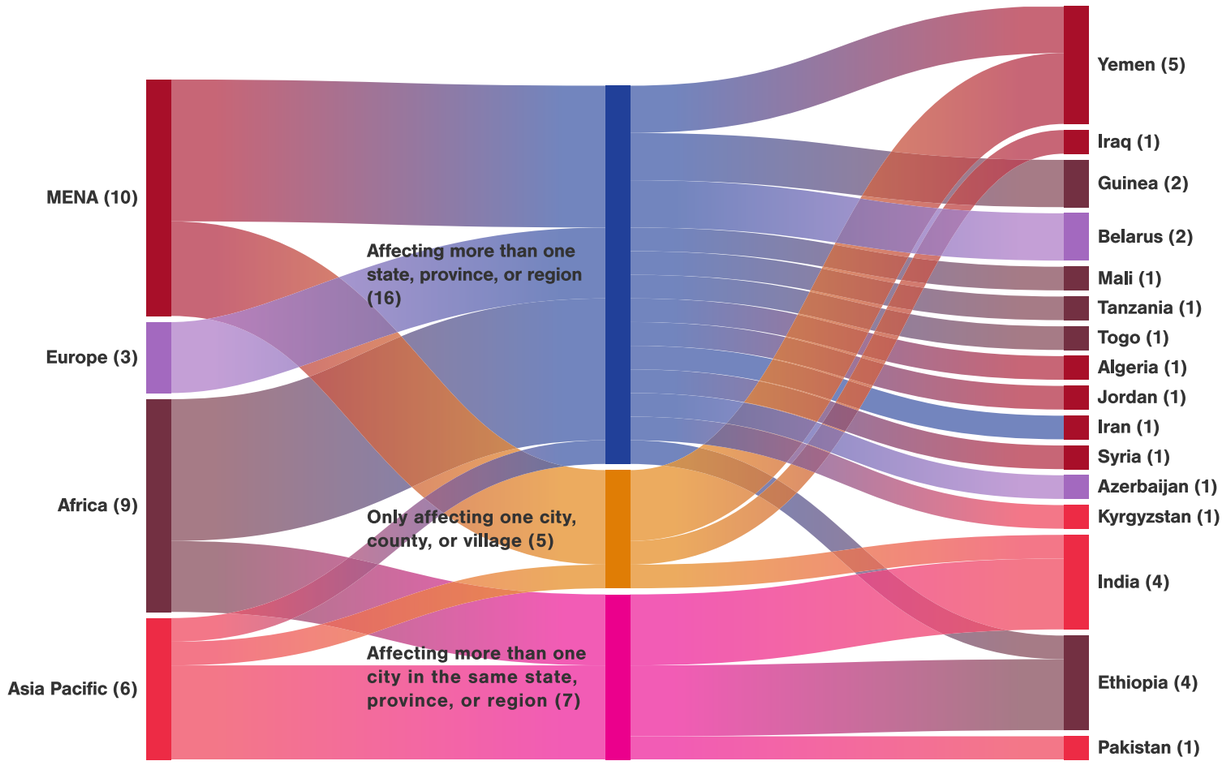
16 Kamran, Hija (2020, April 1). *An Internet Shutdown Is Keeping Coronavirus Information From Millions in Pakistan*. Slate Magazine. Retrieved Jan 26, 2021 from https://slate.com/technology/2020/04/coronavirus-covid19-pakistan-internet-shutdown-fata.html.

others living in areas cut off through prolonged and targeted internet shutdowns had more difficulty. For instance, Kyauktaw residents struggled to get this information because an intentional shutdown forced them to rely on pamphlets, which are expensive and difficult to distribute during the pandemic.[17] In Maramagyi, the lack of internet access and national lockdowns had a compounded effect. Residents had to use phones to pass along COVID-19-related information.[18]

II. Trends in 2020

In 2020, there were 28 complete internet blackouts that plunged people, often the most marginalized, into digital darkness, as authorities disabled both broadband and mobile connectivity. Governments in Yemen, Ethiopia, India, Belarus, Guinea, Algeria, Pakistan, Jordan, Azerbaijan, Iraq, Kyrgyzstan, Mali, Syria, Tanzania, Iran, and Jordan entirely cut off at least one city. Ethiopia imposed at least four complete internet outages in 2020. One of the four was a nationwide internet shutdown that lasted for more than two weeks and affected more than 100 million people,[19] while the rest were regional shutdowns that were more restricted in scope.

Scope of impact of complete internet blackouts in 2020



17 *See supra* note 4.

18 *See supra* note 4.

19 Access Now (2020, July 16). *Back in the dark: Ethiopia shuts down internet once again.* Retrieved Jan 26, 2021, from https://www.accessnow.org/back-in-the-dark-ethiopia-shuts-down-internet-once-again/.

Dissecting an internet shutdown

Not all shutdowns are the same, nor are they undertaken in the same manner. Analyzing the different types of shutdown can shed light on the tactics governments are using, and help us understand why they carry out particular acts of censorship — under what circumstances and for what purpose. In our work at Access Now with the #KeepItOn coalition, we have learned through documenting, investigating, and fighting internet shutdowns that they are typically an extension and escalation of traditional forms of censorship. Governments often deploy them to further silence and infringe on the human rights of particular populations, entrenching existing patterns of censorship. For example, in countries where governments deliberately shut down the internet, we often see that press freedom is under attack, journalists are harassed or arrested, websites are blocked, and political rights are restricted. By shutting down the internet, these countries not only ramp up censorship and hurt free expression and access to information, however; they also interfere with a broad range of other human rights.

1. Throttling

Governments and internet providers that intentionally disrupt the internet throttle (or slow down) internet traffic, cut off internet access entirely, or combine these tactics. A provider can throttle all internet traffic, affecting both broadband and mobile internet, or only slow down access to specific sites, apps, or segments of traffic. Out of the 155 internet shutdowns in 2020, six incidents were bandwidth throttling.[20] For instance, beginning in August 2020, Myanmar had been throttling mobile data in Rakhine and Chin states, and this continued through the end of the year. As we note above, full access was only restored after the military coup attempt in 2021,[21] during which the military has strategically imposed full internet shutdowns and blocked social media platforms elsewhere.[22] Bangladesh has throttled mobile data in refugee camps where Rohingya refugees reside for more than 355 days. Other countries, like Vietnam and Uganda, throttled social media platforms like Facebook, making it almost impossible to use these apps or share images and videos. It appears that in 2020, governments used throttling to inflict longer restrictions on the free flow of information, while avoiding the burden and cost of a complete shutdown.

Authorities in both Bangladesh and Myanmar combined throttling with other tactics that exacerbated the effect of the shutdown. In Myanmar, the Posts and Telecommunications Department (PTD) issued a directive in 2020 to restrict the purchase of Subscriber Identity Module (SIM) cards to two per operator, and required all SIM-card holders to re-register with a valid identification document.[23] Those who did not have access to the internet because of a deliberate shutdown were not able to re-register because they could not upload their identification documents online to complete the registration.[24] This meant that, due to the shutdown and ill-conceived and discriminatory SIM card directive, people in the townships affected by the throttling were being denied other telecommunication services, including voice connectivity and Short Message Service (SMS). It was already a difficult situation: due to the pandemic and lockdown, numerous SIM card vendors were closed, making it harder to

20 Bandwidth throttling is the intentional slowing of an internet service or a type of internet traffic.

21 Telenor (2021). *Network restored in eight townships in Myanmar*. Retrieved Feb 9, 2021, from https://www.telenor.com/network-restored-in-eight-townships-in-myanmar/.

22 *See supra* note 8.

23 Free Expression Myanmar (2020, April 29). *Deactivating SIM cards during Covid-19 violates rights*. Retrieved Jan 26, 2021 from http://freeexpressionmyanmar.org/deactivating-sim-cards-during-covid-19-violates-rights-covid-19/.

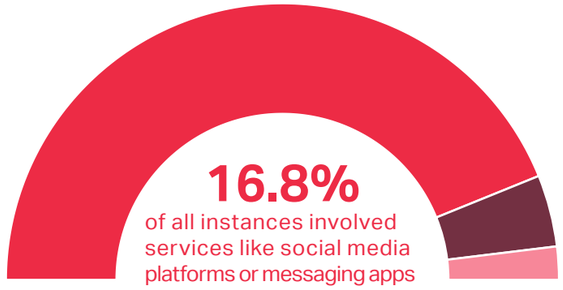
24 Myanmar Times (2020, April 29). *Millions in Myanmar risk having mobile phones cut off after SIM registration deadline*. Retrieved Jan 26, 2021 from https://www.mmtimes.com/news/millions-myanmar-risk-having-mobile-phones-cut-after-sim-registration-deadline.html.

re-register.[25] Moreover, those without identification documents were unable to re-register. As a result, telecom companies were forced to de-register and cut off people using 34 million SIM cards.[26] This situation is not unique to Myanmar. Bangladesh also denied SIM cards to refugees for at least a year.[27]

2. Mobile and broadband internet and service shutdowns

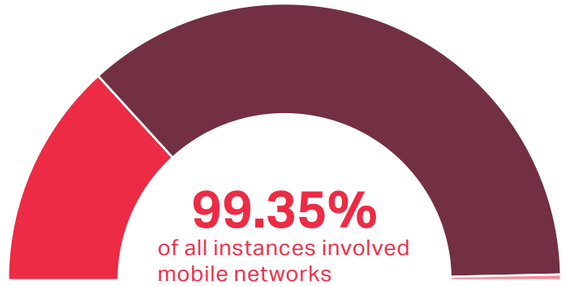
When governments do not slow down the internet, they shut it down. Like they do with throttling, service providers can target shutdowns, cutting access to mobile or fixed-line internet, or blocking access to communications platforms like Facebook, Twitter, WhatsApp, or Telegram. The majority of the shutdowns in 2020 were of this type, and affected people using mobile or broadband internet access or social media apps and other platforms.

Types of network and service restrictions in 2020



- Shutdown: 87.74%
- Shutdown and throttling: 8.39%
- Throttling: 3.87%

Affected networks in 2020



- Broadband and mobile networks: 26.45%
- Mobile networks: 72.90%
- Unknown: 0.65%

It appears that most of the time, governments would rather shut down mobile internet service than fixed-line internet service. In the majority of countries that order network disruptions, the population gets access to the internet primarily via their mobile phones.[28] In most contexts, those who have access to fixed broadband internet are businesses, government institutions, universities, and other establishments.[29] Access to mobile internet is typically much cheaper than broadband internet, making it the more affordable choice for ordinary citizens. When governments shut down broadband internet service and mobile data, in many cases it is fixed-line services that are the first to be restored, while mobile internet is the last.

25 Aung, Naing (2020, October 27). *Telecoms ministry says it has deactivated more than 34 million SIM cards*. Myanmar Now. Retrieved Jan 26, 2021 from https://www.myanmar-now.org/en/news/telecoms-ministry-says-it-has-deactivated-more-than-34-million-sim-cards.

26 Ibid.

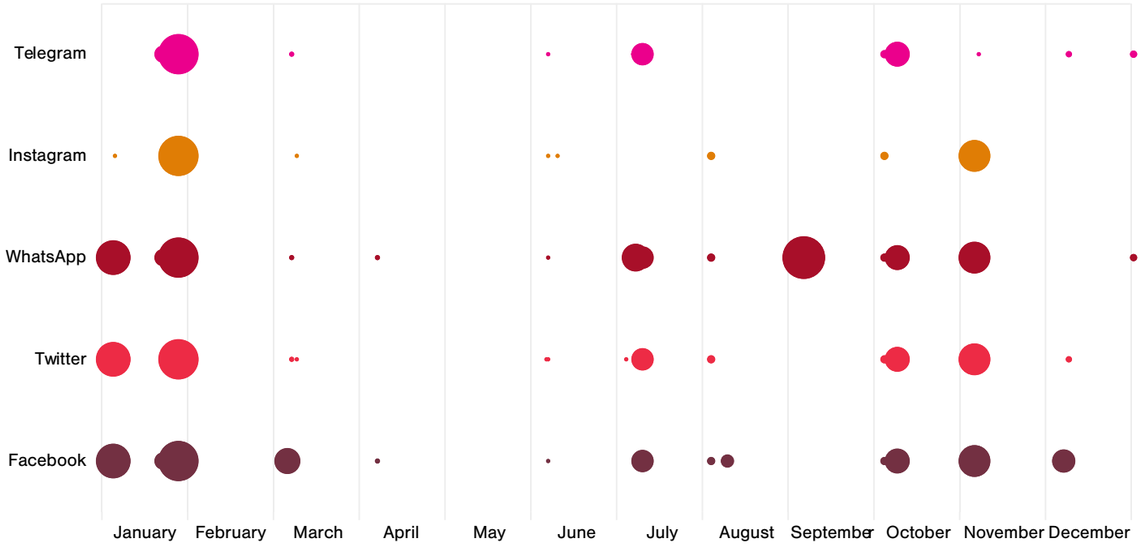
27 Kamruzzaman, Md (2020, August 25). *Bangladesh to restore phone, internet at Rohingya camps*. Anadolu Agency. Retrieved Jan 22, 2021, from https://www.aa.com.tr/en/asia-pacific/bangladesh-to-restore-phone-internet-at-rohingya-camps/1952124.

28 Keelery, Sandhya (2020). *Fixed and mobile broadband internet subscription penetration in India from 2011 to 2017*. Statista. Retrieved Jan 22, 2021, from https://www.statista.com/statistics/482142/fixed-and-mobile-broadband-internet-penetration-india/; and The World Bank. *Mobile cellular subscriptions (per 100 people) - Sub-Saharan Africa, Chad, Tanzania, Guinea, Ethiopia, Togo, South Sudan*. Retrieved Jan 22, 2021, from https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=ZG-TD-TZ-GN-ET-TG-SS.

29 International Telecommunication Union (2020). *Measuring Digital Developments: facts and figures*. Retrieved Jan 22, 2021, from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf.

Following similar patterns in 2018 and 2019, governments continued to shut down social media and communications platforms in 2020. There were at least 26 attempts to deny people access to these platforms in 2020. These shutdowns targeted those using Facebook, Twitter, WhatsApp, Instagram, Telegram, and other platforms.

Social media blocking in 2020
Size of the dot indicates the duration of each block



How did they justify the shutdown?

In 2020, many governments failed to confirm their internet shutdown orders, leaving the affected populations to guess why they imposed this form of arbitrary censorship. Publishing shutdown orders is essential to maintaining the rule of law. If a government does not give notice of why certain behaviors or services are prohibited, the law fails to set precedent. How is one to conform to a rule that's unwritten, and arbitrarily enforced — or fight that rule in court? More lawyers are challenging shutdowns via lawsuits, and published orders help jurists determine who issued the decree, on which grounds, and on whose authority. The public is safer and has more certainty when authorities clarify the duration, scope, and purpose of any restriction on speech, shutdowns included. In some cases, when victims have sued telcos that carry out shutdowns, the telcos have revealed the shutdown orders, providing crucial transparency that governments denied to affected communities.[30] Some governments have attempted to justify shutdown orders by insisting they were to stop the spread of "fake news" or hate speech and incendiary or violence-inciting content. In other cases, they have cited national security, and in a few instances, exam cheating.

In India, the Jammu and Kashmir administration has been forced to publish their internet shutdown demands and the political and legal justification for the disruptions, so it has become easier to document and understand why they are carried out. They previously resisted disclosing this information. It was only after journalists and civil society groups challenged the lack of transparency, bringing the case to India's Supreme

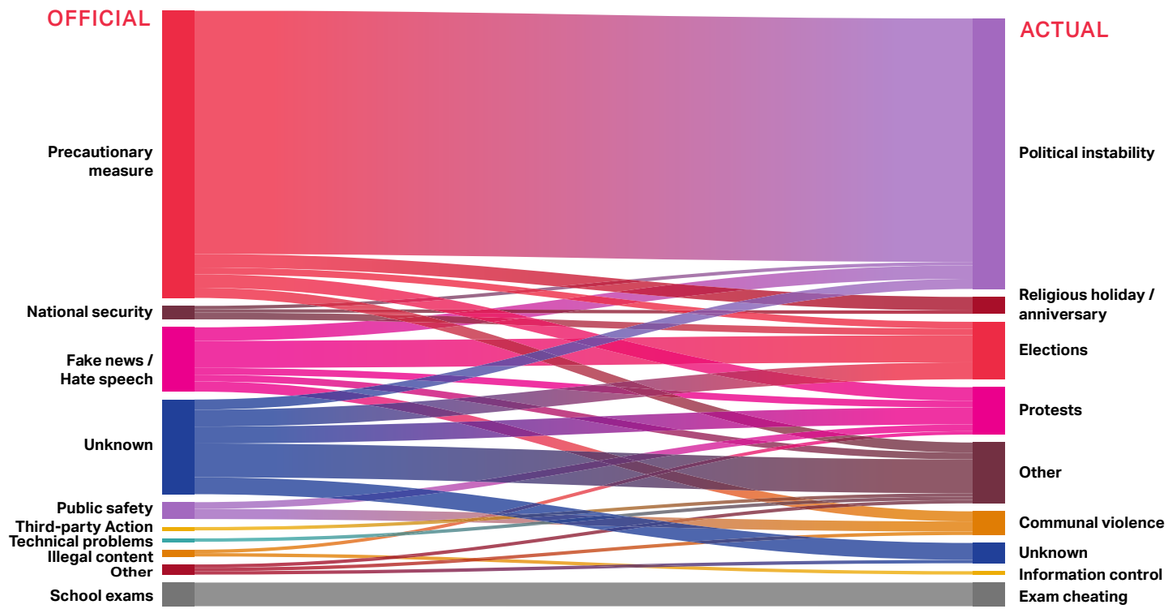
30 Access Now (2019). *The State of Internet Shutdowns Around the World: The 2018 #KeepItOn Report*. Retrieved Jan 22, 2021, from https://accessnow.org/kio-2018-report.

Court, that the government began to publish the orders.[31] Although this is a welcome development, both the union government of India and the Jammu and Kashmir administration have refused to publish previous internet shutdown orders from 2019.[32] Moreover, the union government has informed members of parliament that they do not have data on shutdown orders and have provided confusing answers regarding the hundreds of shutdowns India has carried out.[33] India's government has also refused to centrally collate and publish information on shutdowns going forward, nor will it encourage states to provide similar information. It appears we can only get the true picture of why disruptions are ordered, when — and only when — all states publish their orders and provide legal justifications for these disruptions, or the government finally takes central responsibility for transparency on this issue.

From what we can determine through the published shutdown orders and media reports in 2020, the most common rationale for a shutdown in India during the year was "precautionary measure." The go-to rationale for shutting down the internet was to preemptively fight an "impending security incident" or "stop anti-national elements from sharing false information on social media."

However, governments rarely mean what they say when it comes to internet shutdowns. When officials say they are using shutdowns to fight "fake news" or hate speech, it can mask an attempt to hide or distort information around political instability, obscure police clashes or targeted attacks that take place during communal violence, or stop people from organizing protests.

Official justifications vs. actual causes of internet shutdowns worldwide in 2020
The largest portion of claims of "precautionary measure" during observed "political instability" came from India's shutdowns.



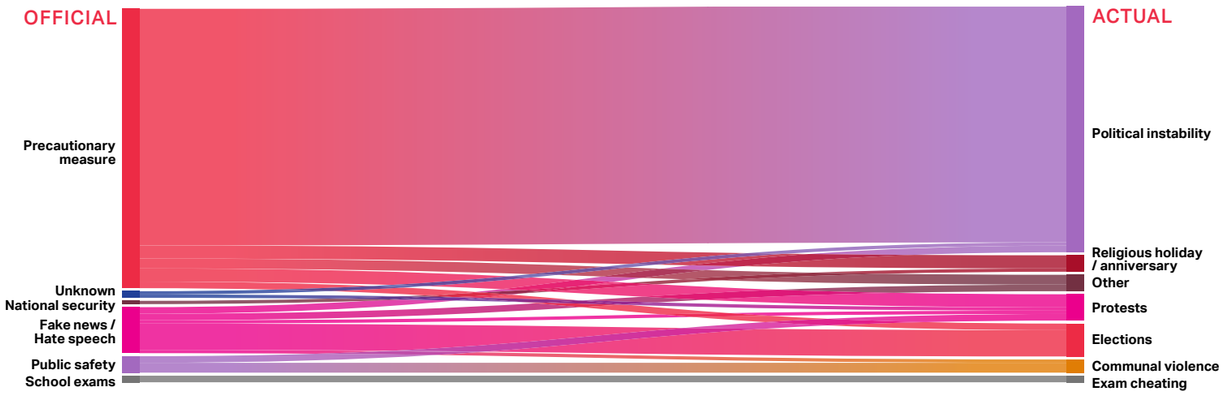
31 Deutsche Welle (2020). *Indian court: Kashmir indefinite internet shutdown illegal*. Retrieved Jan 26, 2021, from https://www.dw.com/en/indian-court-kashmir-indefinite-internet-shutdown-illegal/a-51954255.

32 TheWire.in (2020). *J&K Internet Shutdown Based on 'Dubious' Legal Framework: Report*. Retrieved Feb 10, 2021, from https://thewire.in/government/jammu-and-kashmir-internet-shutdown-jkccs.

33 Chunduru, Aditya (2020, September). *Parliament Watch: Confusing, Indirect Answers From Govt During Week 2*. Medianama. Retrieved Jan 26, 2021, from https://www.medianama.com/2020/09/223-parliament-watch-indirect-answers-week-2/.

In India, which consistently shuts down the internet more than any country in the world, the official justification does not always match the reality on the ground. The government may justify most shutdowns as precautionary, but India has a history of ordering shutdowns targeting political demonstrations, a trend that appears to be accelerating and spreading across all Indian states and union territories. Likewise, a shutdown to fight "fake news" or "hate speech" online may be justified by local or state authorities as an effort to stop communal violence. An altercation between different communities that is amplified on social media can result in targeted attacks on specific communities. In Manipur, for example, the state government shut down the internet for three days in 2020, fearing clashes between two villages over a land dispute.[34] However, while authorities justified the shutdown by observing that "social media has become a useful tool for rumor-mongers and is being used extensively to incite the public," there is little evidence to suggest that cutting access to the internet stops violence in these situations. To the contrary, there is research to show that such blocking in India can suddenly change "a predictable situation into one that's highly volatile, violent, and chaotic." [35]

Official justifications vs. actual causes of India's shutdowns in 2020



What triggers a shutdown?

Continuing the pattern from 2019 and 2018, governments shut down the internet in evident attempts to hide political instability, respond to communal violence, suppress opposition groups, claim purported victory in disputed elections, thwart protests, and stop students from cheating during exams.

One notable trend in 2020 is an increased number of internet shutdowns being deployed in response to ongoing violence — particularly in active conflict zones. We have long pointed out that amid conflict, shutdowns can hide human rights violations or war crimes, thwart journalism, and put people's lives in danger. In Yemen, Syria, and Rakhine and Chin states of Myanmar, which have long been in a protracted conflict,

One notable trend in 2020 is an increased number of internet shutdowns being deployed in response to ongoing violence — particularly in active conflict zones during this year.

34 Ningomba, Bozendra (2020). *Mobile Internet shut after Manipur clash*. The Telegraph India. Retrieved Jan 22, 2021, from https://www.telegraphindia.com/north-east/mobile-internet-shut-after-manipur-clash/cid/1754384.

35 Rydzak, Jan. *Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India*. Retrieved Jan 26, 2021 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413.

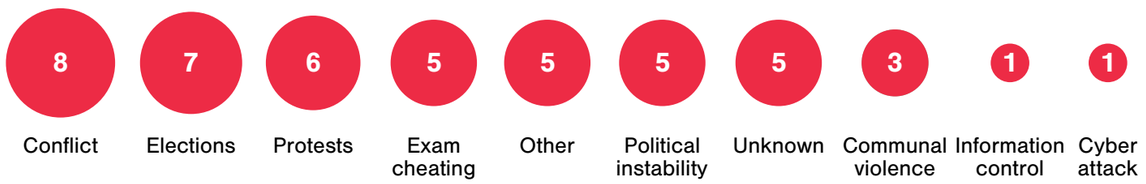
authorities have nevertheless continued to cut access to the internet, and new countries have now joined the list. When war broke out between Armenia and Azerbaijan, for example, Azerbaijan shut down the internet for more than six weeks.[36] In Ethiopia, as the conflict between the Ethiopian Defense Forces and regional forces in Tigray erupted, the internet and mobile network vanished.[37]

Internet shutdowns during armed conflict make it much harder for anyone to capture and document the reality on the ground, including the extent of the fighting and the human toll it is taking. Those responsible for mass atrocities can shroud their actions in digital darkness and dispute civilian narratives, and people who are lucky enough to survive are left in desperate conditions and unable to reach out to the rest of the world. In Ethiopia, Tigrayans living outside the conflict area and in the global diaspora could not check on the safety of their loved ones for months on end,[38] and media coverage and documentation of the mass atrocities and human rights violations committed during the conflict has been delayed.[39] In Azerbaijan, even as the government started throttling internet access, the Minister of Defense set up a Telegram channel to encourage internet users to sign up for updates by state-owned media, in a clear attempt to control the narrative around the dispute.[40] Under these conditions, human rights advocates, activists, journalists, and others find it immensely difficult to monitor and document human rights violations.[41]

The 2020 ranking of the actual causes of internet shutdowns

India

The rest of the world



36 Azerbaijan Internet Watch (2020, September 27). *Country-wide internet disruptions reported in Azerbaijan*. Retrieved Jan 26, 2021, from https://www.az-netwatch.org/news/country-wide-internet-disruptions-reported-in-azerbaijan/.

37 The East African (2020, November 5). *Ethiopia shuts down telephone, internet services in Tigray.* Retrieved Jan 26, 2021, from https://www.theeastafrican.co.ke/tea/rest-of-africa/ethiopia-telephone-internet-services-tigray-2731442.

38 Getachew Temare (@getachew_temare) (2021). Getachew Temare Twitter post. Twitter, 3:10 a.m. January 26, 2021, Retrieved Jan 26, 2021, from https://twitter.com/getachew_temare/status/1353948305496166401.

39 Amnesty International (2020, November 12). *Ethiopia: Investigation reveals evidence that scores of civilians were killed in massacre in Tigray state*. Retrieved Jan 26, 2021, from https://www.amnesty.org/en/latest/news/2020/11/ethiopia-investigation-reveals-evidence-that-scores-of-civilians-were-killed-in-massacre-in-tigray-state/.

40 Arzu Gerybullayeva (2020, November 4). *Azerbaijan, the Internet in times of war*. Balcani Caucaso. Retrieved Jan 26, 2021, from https://www.balcanicaucaso.org/eng/Areas/Azerbaijan/Azerbaijan-the-Internet-in-times-of-war-205919.

41 *See supra* note 30. *See* also, Human Rights Watch (2020, November 25). *Q&A: Conflict in Ethiopia and International Law*. Retrieved Jan 26, 2021, from https://www.hrw.org/news/2020/11/25/qa-conflict-ethiopia-and-international-law# and Beatrice Martini (@Beatrice Martini) (2019). Beatrice Martini Twitter post. Twitter, 5:07 a.m. April 24, 2019, Retrieved Jan 26, 2021, from https://twitter.com/beatricemartini/status/1120962335819149313.

Fighting "fake news" or "illegal content" at any cost

An internet shutdown is an inherently disproportionate interference with the right to free expression, yet in 2020, numerous countries imposed shutdowns on the pretext of combating "fake news," violence-inciting hate speech online, and to respond to other content moderation issues. As we note above, authorities in India shut down the internet repeatedly while citing "rumors spread on social media," including in Manipur, where the state government cut access to the internet for three days in an attempt to prevent clashes between two villages over a land dispute.[42] The official rationale was that social media had become useful for rumor-mongers to incite violence, and unless the use of internet and mobile data was curbed temporarily, "there is a likelihood of deterioration of law and order and communal violence in the state."[43] Yet as we have noted, research suggests that internet shutdowns may encourage, not discourage, violence.[44]

Both democratic and authoritarian regimes raise a legitimate concern over the spread of violence-inciting, misleading, and hateful content online. However, it is not clear how shutting down the internet would address this pernicious problem. When Ethiopia shut down the internet in June 2020, officials argued it was a way to preserve law and order and protect people. But even though the whole country was cut off from the internet, the violence did not disappear. Moreover, the shutdown left in its wake a disputed narrative around what transpired during the complete blackout.[45] Disruptions like this frustrate fact-finding and hinder transparency and accountability.

Dangerously, governments in Nigeria,[46] Singapore,[47] and Hong Kong SAR[48] have proposed or passed legislation to facilitate the blocking of social media platforms, denying internet service to specific internet end users that violate these laws, or shutting down the internet to cut off the public as a whole. While the spread of false and misleading information and violence-inciting expression is an enormous challenge, cutting access to the internet or blocking major communications channels is a disproportionate response with profoundly negative cascading effects.

In countries where social media platforms resist irrational and illegal government demands, authorities are using access to their services as a bargaining chip for compliance. In Vietnam, when Facebook did not take down content the government deemed illegal, authorities throttled the platform for around 50 days until the company gave in. Prior to taking this action, Vietnam had introduced cybersecurity legislation that forces online platforms and others to store data locally, monitor and take down illegal content, and set up local offices in Vietnam.[49] When the law came into force, the government accused Facebook of violating it.[50] One year later, authorities

42 *See supra* note 34.

43 *See supra* note 34.

44 *See supra* note 35.

45 Bearak, Max (2020, July 1). *Ethiopia protests spark Internet shutdown and fears of high death toll after popular singer killed*. Retrieved Jan 22, 2021, from https://www.washingtonpost.com/world/africa/ethiopia-protests-spark-internet-shutdown-and-fears-of-high-death-toll-after-popular-singer-killed/2020/07/01/ff18e5de-bb76-11ea-97c1-6cf116ffe26c_story.html.

46 Amnesty International (2019, December 4). *Nigeria: Bills on hate speech and social media are dangerous attacks on freedom of expression*. Retrieved Jan 22, 2021, from https://www.amnesty.org/en/latest/news/2019/12/nigeria-bills-on-hate-speech-and-social-media-are-dangerous-attacks-on-freedom-of-expression/.

47 Protection from Online Falsehoods and Manipulation Act 2019 (Singapore). Retrieved Jan 22, 2021 from https://sso.agc.gov.sg/Acts-Supp/18-2019.

48 Access Now (2020, July 6). *New Police Powers in Hong Kong Threaten Human Rights Online*. Retrieved Jan 22, 2021 from https://www.accessnow.org/new-police-powers-in-hong-kong-threaten-human-rights-online/.

49 McLaughlin, Timothy (2019, March 16). *Under Vietnam's new cybersecurity law, U.S. tech giants face stricter censorship*. Retrieved Jan 22, 2021, from https://www.washingtonpost.com/world/asia_pacific/under-vietnams-new-cybersecurity-law-us-tech-giants-face-stricter-censorship/2019/03/16/8259cfae-3c24-11e9-a06c-3ec8ed509d15_story.html.

50 *See supra* note 10.

ordered telecommunications companies to block connection to the company's servers in the country.[51]

In countries like Vietnam, platforms have to navigate difficult legal terrain to provide their services. They weigh the benefits of providing services and consequently getting served with arbitrary orders against exiting a market so they will not be used as a tool for oppressive governments. These decisions are difficult, but all platforms have a duty to respect human rights and must always work within the principles of harm reduction. In the case of Vietnam, Facebook's compliance demonstrates that the company is more interested in maintaining its significant market presence than protecting the fundamental rights of the Vietnamese. Facebook's decision to act as an extension of the government's censorship and propaganda machine sets a dangerous precedent. The company should reconsider and take steps to safeguard users' rights.

Human rights violations and violence during shutdowns

Not only do internet shutdowns interfere with the rights to access information, freedom of expression, and other fundamental freedoms, they are used in attempts to hide egregious human rights violations. In 2020, at least 17 incidents of internet shutdowns were accompanied by blatant rights violations. In Ethiopia, Belarus, India, Guinea, and other countries, human rights organizations and civil society groups reported patterns of abuse taking place during a shutdown.

BELARUS

In Belarus, the government not only used internet shutdowns to dissuade protesters from going out into the streets, organizing, and sharing critical information, there were reports of arbitrary arrest, torture, and other human rights violations.[52]

ETHIOPIA

At the onset of the conflict between the federal and regional forces in the Tigray region of Ethiopia, authorities cut off mobile networks, landline phones, and fixed-line internet. As the war engulfed the Tigray region and fighting escalated, civil society, human rights organizations, journalists, and others struggled to investigate and document reports of massive human rights violations.[53] To make matters worse, according to the Ethiopian Human Rights Commission, there were deliberate attempts to stop people from accessing alternative communication channels. In Mai kadra, Tigray zone of Ethiopia, "scores, and likely hundreds, of people were stabbed or hacked to death"[54] during the total communications blackout, Amnesty International and the Ethiopian Human Rights Commission report. As the perpetrators of the violence organized to kill, they also allegedly "collected and destroyed Sudanese

51 Pearson, James (2020, April 21). *Facebook agreed to censor posts after Vietnam slowed traffic*. Reuters. Retrieved Jan 22, 2021, from https://www.reuters.com/article/us-vietnam-facebook-exclusive-idUSKCN2232JX.

52 Amnesty International (2020, August 13). *Belarus: Mounting evidence of a campaign of widespread torture of peaceful protesters*. Retrieved Jan 22, 2021, from https://www.amnesty.org/en/latest/news/2020/08/belarus-mounting-evidence-of-a-campaign-of-widespread-torture-of-peaceful-protesters/; Anthonio, Felicia, and Peter Micek (2020, August 13). *Belarusian election tainted by internet shutdown and state-sponsored violence*. Retrieved Jan 22, 2021, from https://www.accessnow.org/belarusian-election-tainted-by-internet-shutdown-and-state-sponsored-violence/; Human Rights Watch (2021, January 13). *Belarus: Unprecedented Crackdown*. Retrieved Jan 22, 2021, from https://www.hrw.org/news/2021/01/13/belarus-unprecedented-crackdown; and Melnichuk, Tatsiana (2020, August 13). *Belarus elections: Shocked by violence,people lose their fear*. BBC. Retrieved Jan 22, 2021, from https://www.bbc.com/news/world-europe-53762995.

53 BBC (2020, December 5). *Ethiopia's Tigray crisis: Cutting through the information blackout*. Retrieved Jan 22, 2021, from https://www.bbc.com/news/world-africa-55189607.

54 *See supra* note 39.

SIM cards."[55] According to testimonies from survivors of the Tigray massacre, "Ethiopian SIM cards had already stopped working by then, and the motive for confiscating and destroying the Sudanese SIM cards was to prevent any communications or call for help during the attack."[56]

Crackdown on the use of VPNs

Governments often do not stop at shutting down the internet. They go further and make sure citizens do not have alternative channels of communications or a way to circumvent state blocking and censorship. This was a trend in 2019 and it continued in 2020.

Countries including Uganda,[57] Tanzania,[58] and India (within Jammu and Kashmir),[59] have banned the use of Virtual Private Networks (VPNs) and other tools for security, anonymity, and circumvention, such as those from the Tor Project, or they have specifically blocked VPN providers and the Tor site, as Belarus has done since 2015,[60] Many also restrict access to app stores such as Google Play so that citizens can't download VPNs and other tools, and in some cases, threaten arrest if people download and use these apps anyway. The Jammu and Kashmir administration has repeatedly ordered telecom and internet service providers to shut down 2G internet service so people cannot use VPNs.[61] In February 2020, on at least two occasions, the government said it was shutting down 2G mobile internet because of "rumors circulating on social media through misuse of VPNs."[62] In March 2020, the media reported that at least five people were arrested for allegedly using VPNs in Kashmir. In Tanzania, the government introduced new regulations in an attempt to restrict people's access to blocked websites and social media apps, prohibiting use or distribution of tools that let people access censored content and restricting people's capacity to stay anonymous online.[63]

VPNs enable people to exercise their right to access information and free expression, bypassing the arbitrary blocking of websites, online content, and social media platforms. In contexts where the government restricts access to sites and platforms, people cannot freely navigate the internet without a VPN. They are also prevented from surfing the web anonymously and can no longer access, share, or distribute information in private.

55 Due to the proximity to the Sudanese border and difficulty over accessing roaming services over prepaid SIM cards, people use both Ethiopian and Sudanese SIM cards in this region.

56 Ethiopian Human Rights Commission (2020, November 24). *Rapid Investigation into Grave Human Rights Violation in Maikadra Preliminary Findings*. Retrieved from Jan 22, 2021, from https://addisstandard.com/wp-content/uploads/2020/11/Maikadra-Preliminary-Findings-English-Final.pdf.

57 Daily Monitor (2021, January 22). Government threatens to arrest VPN users. Retrieved Jan 26, 2021, from https://www.monitor.co.ug/uganda/news/national/government-threatens-to-arrest-vpn-users-3265618.

58 Taye, Berhan (2020, October 22). Internet censorship in Tanzania: the price of free expression online keeps getting higher. Retrieved Jan 22, 2021, from https://www.accessnow.org/internet-censorship-in-tanzania/.

59 Government of Jammu and Kashmir Home Department (2020, February 13). Government order no: Home 12(TSTS) of 2020. Retrieved Jan 22, 2021, from http://jkhome.nic.in/12(TSTS)of2020_0001.pdf.

60 Lokot, Tanya (2015, February 25). *Belarus Bans Tor and Other Anonymizers. Global Voices Advox*. Retrieved from Jan 26, 2021 from https://advox.globalvoices.org/2015/02/25/belarus-bans-tor-and-other-anonymizers/; Newman, Lily Hay. *Belarus Has Shut Down the Internet Amid a Controversial Election*. WIRED. Retrieved Jan 23, 2021, from https://www.wired.com/story/belarus-internet-outage-election.

61 *See supra* note 59.

62 *See supra* note 59.

63 *See supra* note 58.

III. Internet shutdowns during elections and protests

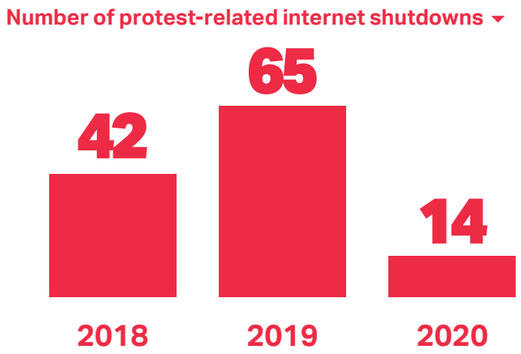
Elections and shutdowns

As the internet became a primary channel for people to access information, authorities that regulate or control traditional media outlets have sought to extend this control online, including as a way to influence elections or undermine democratic processes. This includes disrupting the internet before, during, and after elections, in order to manipulate the free flow of information, restrict opposition groups from reaching out to the electorate for campaigns and organizing, limit election observers' capacity to document and report on election irregularities, and ultimately to rig elections. During shutdowns like this, citizens around the world are prevented from getting information about candidates to weigh their voting options, campaigning for the candidates they support, getting access to basic information such as the location of polling stations, finding out about the election results, and much more. A citizen's access to information during elections is vital to a democratic election and today, the internet is central to the process. From Belarus to Togo and beyond, governments undermined the legitimacy of elections by shutting down the internet, and in some cases, those elections were followed by protests and violence. In 2020, there were at least 17 internet shutdowns related to elections in seven countries.

Governments that shut down the internet in the election period in 2020

On election day in February 2020, as voters in Togo went to the polls to elect their president, authorities blocked access to instant messaging apps.[64] In Guinea, not far from Togo, the government shut down the internet during elections not once, but twice in 2020. The first shutdown was in March 2020 and took place during a referendum on constitutional reform, and the second took place during the presidential election in October 2020. After the second shutdown, violence broke out when the opposition declined to accept the results of the tainted process.[65] In May 2020, Burundi shut down social media during its election.[66] In August 2020 during its election, Belarus repeatedly shut down the internet, blocked social media platforms, and cut access to mobile data, off and on, for more than 120 days. In October 2020, Kyrgyzstan throttled social media and mobile and broadband internet during its contested elections. As the election results were announced, people flooded into the streets to challenge them, ultimately triggering another election in 2021.[67] A few days after the Kyrgyzstan election shutdown, Tanzania first filtered SMS messaging, then blocked social media platforms, and finally shut down the internet entirely.[68] In November 2020, India shut down the internet numerous times in all Jammu and Kashmir districts in anticipation of the District Development Council constituencies by-elections.[69] Lastly, the Burmese government decided to continue to shut down the internet in Rakhine and Chin states in Myanmar even during the highly anticipated elections.[70]

Protests and network disruption



From Black Lives Matter movements across the world, to India's discriminatory Citizenship Amendment Act (CAA) protests, to the Belarus protests, 2020 was a monumental year for the freedom of peaceful assembly and association.[71] The COVID-19 pandemic, and subsequent lockdowns and curfews around the globe, put limits on gathering and made protests dangerous. These and other factors might have contributed to the surprisingly lower number of protest-related shutdowns we documented in 2020. In addition, in 2019, we had documented numerous

64 Xynou, Maria, and Arturo Filastò (2020, October 24). *Togo: Instant messaging apps blocked amid 2020 presidential election*. Retrieved Jan 22, 2021, from https://ooni.org/post/2020-togo-blocks-instant-messaging-apps/.

65 BBC News (2020, October 24). *Guinea elections: Alpha Condé wins third term amid violent protests*. Retrieved Jan 22, 2021, from https://www.bbc.com/news/world-africa-54657359.

66 Taye, Berhan, and Felicia Anthonio (2020, May 20). *Burundi: #KeepItOn: Burundi silences the majority on election day*. Retrieved Jan 26, 2021, from https://www.accessnow.org/keepiton-burundi-silences-the-majority-on-election-day/.

67 Freedom House (2020). *Freedom of the Net: Kyrgyzstan*. Retrieved Jan 26, 2021, from https://freedomhouse.org/country/kyrgyzstan/freedom-net/2020; and BBC News (2021, January 11). Kyrgyzstan election: Sadyr Japarov wins presidency with landslide. Retrieved Jan 26, 2021, from https://www.bbc.com/news/world-asia-55613552.

68 Access Now (2020, October 24). *Tanzania government censoring mobile networks ahead of presidential election*. Retrieved Jan 26, 2021, from https://www.accessnow.org/tanzania-censoring-mobile-networks-before-election/.

69 Government of Jammu and Kashmir Home Department (2020, November 12). Government order no: Home 120 (TSTS) of 2020. Retrieved Jan 22, 2021, from http://jkhome.nic.in/TSTS%2012.11.20.pdf.

70 Anthonio, Felicia et. al. (2020, October 15). *How internet shutdowns are threatening 2020 elections, and what you can do about it*. Access Now. Retrieved Feb 9, 2021, from https://www.accessnow.org/internet-shutdowns-2020-elections/.

71 Access Now (2020). *Defending peaceful assembly and association in the digital age: takedowns, shutdowns, and surveillance*. Retrieved Jan 22, 2021, from https://accessnow.org/defending-peaceful-assembly-and-association-in-the-digital-age.

targeted internet shutdowns that affected a region, neighborhood, or specific ethinic communities.[72] That type of shutdown is often difficult to monitor and document because it's harder to verify on a technical level; observers may not necessarily see a decline in internet traffic or the areas affected are so small they escape notice or get scant media attention. While Access Now and the #KeepItOn coalition reported more than 65 protest-related shutdowns in 2019, in 2020, the number significantly decreased. There were at least 14 shutdowns triggered by a protest, including in Cuba, India, Jordan, Ethiopia, Mali, Uganda, and Iraq. The evident motivation: to silence dissenting voices and get protesters off of the streets.

IV. New countries added to the shame list

Cuba, Tanzania, and Kenya are three countries that had not shut down the internet previously, but joined the list in 2020. In Kenya, it was not the government shutting down the internet, but a non-state actor, Al Shabab, a jihadist fundamentalist group, that deliberately destroyed communications infrastructure on at least two occasions, as we explain in our discussion of Kenya's situation below. This is an indication that the deteriorating security situation at the border of Kenya and Somalia not only affects the security infrastructure in the country but also has an impact on internet service delivery. There is a similar concern in Yemen, Syria, Ethiopia, and other countries where conflict is ongoing and there is a risk of attack on telecommunications infrastructure. Cuba presents an interesting case because the country recently liberalized access to mobile internet, and as we explore in detail below, the shutdown in 2020 shows that while improving connectivity can lead to better civic discourse, it can also be used to organize civil disobedience — which can in turn provoke a government response. Last but not least, the shutdown in Tanzania is a terrifying blueprint for a government's systematic closure of civic space, where authorities chip away at the digital rights of citizens day by day, until they ultimately decide to flip the killswitch.

CUBA

Cuba has a long history of censorship, with restrictions to press freedom, surveillance, and strict control over internet infrastructure. There was some progress in 2018 when the government allowed citizens to access mobile internet (albeit with limited reliability), but most Cubans access the internet through public WiFi hotspots. In 2020, the Cuban government took its censorship a step further, blocking Telegram, WhatsApp, Twitter, and other social media platforms for three days, evidently to silence a rare protest by the San Isidor Movement.[73] As more Cubans use mobile data and the internet to organize around social-political issues, they could see more challenges to their ability to access an open, secure, reliable, and accessible internet. It is worth mentioning that in October 2020, there were numerous reports that people could not access Telegram, a popular messaging app, or circumvention tools such as VPNs, in Cuba. Members of the #KeepItOn coalition sent a letter[74] to Empresa de Telecomunicaciones de Cuba S.A.(ETECSA), a state-run enterprise and sole gatekeeper for internet access in Cuba, requesting information as to why the application was not accessible. As of February 2021, ETECSA had not replied.

72 *See supra* note 12.

73 France 24 (2020, January 14). *Mobile internet: Cuba's new revolution*. Retrieved Jan 22, 2021, https://www.france24.com/en/live-news/20210114-mobile-internet-cuba-s-new-revolution; David Aragort (@DavidAragort) Twitter post. 10:16 p.m. Nov 26, 2020. Retrieved Jan 26, 2021 from https://twitter.com/DavidAragort/status/1332131089746366464; Norges Rodríguez (@Norges14) Twitter post. 10:10 p.m. Nov 26, 2020. Retrieved Jan 26, 2021 from https://twitter.com/norges14/status/1332129539166785541.

74 Access Now (2020, November 4). *Telegram blocked in Cuba? Civil society demands answers*. Retrieved Feb 23, 2021, from https://www.accessnow.org/telegram-blocked-in-cuba-civil-society-demands-answers/.

TANZANIA

While 2020 marked the first time Tanzania has shut down the internet, the government's callous action did not surprise the human rights community. For the past few years, Tanzania has restricted freedom of expression online and off, targeting vulnerable groups like the LGBTQ+ community with harassment, arbitrary arrests, and persecution.[75] The government's introduction of a blogger registration fee, its banning of VPNs, and its clampdown on the media created the breeding ground[76] for the digital rights violations authorities perpetrated during Tanzania's election. A few days before the election, the government installed equipment that would enable authorities to censor content and throttle the internet.[77] Shortly after, citizens started reporting that they could not access Twitter, Facebook, and other social media platforms.[78] In addition, the Tanzania Communication Regulatory Authority (TCRA) ordered[79] telecom service providers to suspend access to bulk SMS messages and voice services. On election day itself, people reported internet disruptions, mainly through the government telecom service provider. As of February 2021, Twitter was still inaccessible in Tanzania without a VPN. Access Now collected stories from victims,[80] detailing the harm to people's ability to work, study, and organize.

The act of shutting down internet services has violated my right as a Tanzanian citizen to the access of information, especially during an election period; it has been extremely difficult to stay apprised of what is happening, especially because not everyone has access to traditional media forms—such as television and radio—at all times. Some of us also do a lot of work online and [internet] shutdowns made it very difficult to perform our duties, affecting even our turnaround times. Work that would normally take a couple of days would end up taking two weeks to complete.

75 Human Rights Watch (2020, February 3). *"If we don't get services, we will die."* Retrieved Jan 26, 2021 from https://www.hrw.org/report/2020/02/03/if-we-dont-get-services-we-will-die/tanzanias-anti-lgbt-crackdown-and-right.

76 *See supra* note 58.

77 Olewe, Dickens (2020, December 22). *Tanzania 'using Twitter's copyright policy to silence activists.'* BBC. Retrieved Jan 22, 2021, from https://www.bbc.co.uk/news/world-africa-55186932.

78 Access Now (@accessnow) (2020). Access Now Twitter post. Twitter, 10:06 a.m. October 27, 2020. Retrieved Jan 26, 2021 from https://twitter.com/accessnow/status/1321075713273958402.

79 Tanzania Communication Regulatory Authority (2020, October 21). Directive on Temporal Suspension of Bulk Messaging and of Bulk Calling Services. Retrieved Jan 22, 2021, from https://www.accessnow.org/cms/assets/uploads/2020/10/TCRA-Directive-to-telcos-in-TZ-to-filter-content.jpeg.

80 Antonio, Felicia et. al. (2020, December 16). *Tanzania is weaponizing internet shutdowns. Here's what its people have to say.* Access Now. Retrieved Jan 22, 2021, from https://www.accessnow.org/tanzania-internet-shutdowns-victim-stories/.

KENYA

In Mandera County of Kenya, which borders Somalia and Ethiopia, there were at least two communication network disruptions in 2020. As security along the border has deteriorated, there have been numerous reports to indicate that foreign actors have disabled the telecom towers for some areas of Mandera. In March 2020, as the fighting between the Somali military and Al Shabaab spilled toward the Kenyan border, signal from a Safaricom tower was jammed[81] for a few hours while the fighting continued. In December 2020, media reports indicated that Al Shabaab destroyed the only Safaricom tower in the Elele area of Mandera, leaving residents without access to communication networks.[82]

V. Who stood out in 2020?

Yemen: ICT infrastructure a war bargaining chip

In 2020, Access Now and the #KeepItOn coalition were able to record at least six incidents of network disruptions in Yemen. Due to the ongoing armed conflict and lack of information as to the cause of the shutdowns, we were unable to independently verify the other network disruptions that were reported.

The different armed groups in Yemen have in one way or another threatened to use internet shutdowns as collective punishment and a bargaining chip to advance their interests, with complete disregard for the needs of the people impacted.[83] For instance, in July 2020, communications networks were reportedly targeted by aerial bombardment,[84] which left at least 15 districts in Yemen disconnected from the rest of the world. When the internet wasn't shut down intentionally, natural disasters[85] and heavy rains[86] have denied Yemenis access. When it wasn't natural disasters, there were outstanding payments[87] to international submarine cable providers and other service providers, resulting in suspended services to some parts of Yemen and the threat of further suspension.

Due to the politicization of the internet infrastructure, telecom companies have been unable to provide regular services or expand

81 Goldaman, David (2020, March 2). *Agent Saboteurs Within Somalia Army Jam Kenya's Safaricom BTS-Mast in Mandera Frontier*. Strategic Intelligence. Retrieved Jan 22, 2021, from https://intelligencebriefs.com/agent-saboteurs-within-somalia-army-jam-kenyas-safaricom-bts-mast-in-mandera-frontier/.

82 The Star (2020, December 18). *Al Shabaab destroys Safaricom mast in Mandera*. Retrieved Jan 22, 2021, from https://www.the-star.co.ke/news/2020-12-18-al-shabaab-destroys-safaricom-mast-in-mandera/.

83 News Yesmen (2020). *Al Houthi militia threatens to stop telecommunication and internet services*. Retrieved Jan 22, 2021, from https://newsyemen.net/new/61334.

84 YPA Agency (July 22, 2020). عمران.. طيران التحالف يقصف شبكة اتصالات عيال سريح Retrieved Jan 22, 2021, from http://www.ypagency.net/279308.

85 News Yesmen (2020). *The return of the internet service in Hadhramaut after a two-days of interruption*. Retrieved Jan 22, 2021 from https://newsyemen.net/new/59042.

86 News Yesmen (2020). *Torrential torrents cause the interruption of Internet service in Hadhramaut*. Retrieved Jan 22, 2021, from https://newsyemen.net/new/58962.

87 News Yesmen (2020). *Al-Houthi stops the system of paying internet bills via "Yemen Net" in Aden*. Retrieved Jan 22, 2021, from https://newsyemen.net/new/59213; and News Yesmen (2020). *Internet returns after repair of the submarine cable "Falcon."* Retrieved Jan 22, 2021, from https://newsyemen.net/new/51632.

their businesses. For instance, according to the World Bank, TeleYemen has failed to develop its services and use the capacity it acquired in 2017 due to the political rivalry in Yemen around telecom infrastructure.[88] The fragility of the internet infrastructure has also put Yemen on the world's map. In early January 2020, the Falcon submarine cable in the Suez Canal had two significant cable cuts. While Ethiopia, Kuwait, Saudi Arabia, Sudan, Yemen, and other countries were affected, Yemen suffered the worst impact. Eighty percent of Yemen was cut off the internet, and as there were no other alternatives for connection, the majority of the country went offline,[89] a disruption that affected financial transactions, banking services, and other critical service provisions.[90] There were also numerous reports of vandalism of telecom infrastructure and sabotage by third parties and groups, and these attacks left many disconnected for weeks.[91] According to media reports, Yemeni Telecom had at least 10 incidents of unknown saboteurs stealing their batteries and equipment. The war and these shutdowns have had a devastating impact on digital rights in Yemen.

Belarus: 121 days of internet shutdowns

Belarus is one of the most alarming cases in 2020, showing just how far a government will go to censor dissent during an election. According to the Net Observatory, on June 19 2020, the government tested the Deep Packet Inspection (DPI) equipment, previously bought from Sandvine[92] through the Russian supplier Jet Infosystems, evidently in preparation for the internet shutdowns during the August 9 elections.[93] On the day of the election, the Belarusian government first blocked YouTube, and shortly after, WhatsApp, Telegram, Viber, Vkontakte, and other social media platforms. Authorities proceeded to block VPN providers, Tor Project, and app stores including Google Play.[94] After authorities announced incumbent President Alexander Lukashenko's purported victory in the contested election, people rushed to the streets to protest.[95] Shortly after, the government imposed a full three-day complete outage, starting on August 9 and ending August 12. According to Net Observatory, most telecom service providers were completely offline.[96]

Then the blame game and denial started. Belarus's National Center for Response to Computer Incidents claimed that the disruption was due to a Distributed Denial of Service (DDoS) attack.[97] At the same time, some telecom service providers, notably A1, pointed the finger at the government and announced that the internet access would be restored as soon as the "upstream provider" resumed service.[98] While A1 announced the shutdowns on Twitter and its website, and offered its customers compensation for the interrupted service, civil society demanded more from Belarusian telcos, including that they disclose which government agencies ordered the shutdowns.[99]

For the next 121 days, authorities continued to shut down mobile networks, block websites and social media, and throttle mobile data, in particular on Sundays when Belarusians regularly held demonstrations. This has severely impacted the free flow of information in Belarus. December 6, 2020 marked the first day since the internet and information disruptions started in August that the government did not impose a mobile shutdown in Belarus, but Telegram and other VPNs were still blocked. The protests continue, and it is not clear when Belarus will stop deliberately interfering with internet access and communications.

355 days of internet shutdowns in Rohingya refugee camps in Bangladesh

On September 9, 2019, the Bangladesh Telecommunication Regulatory Commission ordered telecom service providers to disable high-speed mobile internet in the refugee camps Rohingya refugees inhabit. The commission continued to deny high-speed internet to refugees for the next 355 days, and the Rohingya, who had fled to Bangladesh fearing the Myanmar military's ethnic cleansing campaign,[100] were forced to rely on 2G internet speed. This shutdown did not end until late 2020.

A 2G internet speed offers a 250Kbps rate, while 3G and 4G mobile internet connections would normally render 3Mpbs and up to 100Mpbs, respectively. Being restricted to 2G means that users do not have meaningful access to the internet. They are not able to download multimedia content, livestream content online, or access any content that requires more than 250 Kbps speed at a time. They cannot join online video calls, send pictures or videos on Signal or WhatsApp, or place a Facebook Messenger call. They cannot effectively use any service that requires high-speed connection.

This effort to silence the most vulnerable continued even when COVID-19 swept through the refugee camps. On May 15, as the first two cases of COVID-19 were confirmed in the camps, the Rohingya Students Network wrote an open letter to Prime Minister Sheikh Hasina imploring her government to lift the internet ban.[101] These students wanted to use social media and other platforms to get and share information about protecting yourself during the pandemic. They pointed out that internet traffic speed throttling in Bangladesh kept them from getting vital information about the spread of the pandemic, and blocked them from seeking and getting help. According to one resident of the camp, "The last three months I was sick seriously, but I didn't go anywhere due to fear of COVID-19 pandemic [and] my condition [became] serious. I tried to contact a doctor who is a friend of mine but I couldn't talk to him even after calling so many times due to weakness of the network…."[102] The government ignored these pleas for assistance for almost six months.[103]

88 World Bank (2020). *Yemen Monthly Economic Update*.Retrieved Jan 22, 2021, from http://pubdocs.worldbank.org/en/901061582293682832/Yemen-Economic-Update-January-EN.pdf.

89 News Yesmen (2020). *Internet outage and its impact on the lives of citizens in Mouze (field tour).* Retrieved Jan 22, 2021, from https://newsyemen.net/new/50556.

90 *See supra* note 88. *See also* Casey Coombs (2020). *In Yemen, the internet is a key front in the conflict*. Coda. Retrieved Jan 22, 2021, from https://www.codastory.com/authoritarian-tech/yemen-internet-conflict/.

91 Al-Ayyam (2020). *Yemen Mobile operates in Al-Anad again after service interruption and cable theft (in Arabic)*. Retrieved Jan 22, 2021 from https://www.alayyam.info/news/8COYJD3V-URW9YS-3401.

92 Krapiva, Natalia, and Peter Micek (2020, September 2020). *Francisco Partners-owned Sandvine profits from shutdowns and oppression in Belarus*. Retrieved Jan 22, 2021 from https://www.accessnow.org/francisco-partners-owned-sandvine-profits-from-shutdowns-and-oppression-in-belarus/.

93 Net Observatory (2020). *Internet Shutdown in Belarus.* Retrieved Jan 22, 2021 from https://netobservatory.by/belarus-shutdown-2020-en/.

94 Ibid.

95 Reevell, Patrick (2020, August 9). *Protests break out across Belarus following a contested election as police crack down on demonstrators*. ABC News. Retrieved Jan 22, 2021 from https://abcnews.go.com/International/police-military-units-crack-protesters-belarus-contested-election/story?id=72272884.

96 *See supra* note 93.

97 *See supra* note 93.

98 A1 Belarus (@a1belarus) Twitter post. Twitter, 5:32 a.m. August 9, 2020, Retrieved Jan 22, 2021, from https://twitter.com/a1belarus/status/1292378297490460672

99 A1 Belarus (@a1belarus) Twitter post. Twitter, 8:32 a.m. Nov30, 2020, Retrieved Jan 22, 2021, from https://twitter.com/a1belarus/status/1333373287850708992; Petition 4330. Retrieved Jan 22, 2021, from https://petitions.by/petitions/4330; Access Now (2020, November 4). *Shutdowns in Belarus: Austrian telco must denounce actions and commit to accountability.* Retrieved Jan 22, 2021, from https://www.accessnow.org/austrian-telco-must-denounce-internet-shutdowns-in-belarus/.

100 Human Rights Watch (2019, September 13). *Bangladesh: Internet Blackout on Rohingya Refugees*. Retrieved Jan 22, 2021, from https://www.hrw.org/news/2019/09/13/bangladesh-internet-blackout-rohingya-refugees.

101 Rohingya Students Network - RNS. (@NetworkRsn) Twitter post. Twitter, 10:19 a.m. May 15, 2020, Retrieved Jan 22, 2021, from https://twitter.com/NetworkRsn/status/1261285024478883841.

102 *See supra* note 14.

103 Sakib, SM Najmus (2020, October 29). *Internet, mobile network restored for Rohingya refugees.* Anadolu Agency. Retrieved Jan 22, 2021, from https://www.aa.com.tr/en/asia-pacific/internet-mobile-network-restored-for-rohingya-refugees/1957098.

Myanmar: 19 months and counting

Beginning in 2019 and continuing throughout 2020 and into 2021, Myanmar imposed the longest shutdown recorded to date. In 2019, the government ordered the shutdown in nine townships of Rakhine and Chin states. The Ministry of Transport and Communications issued the order, citing "disturbances of the peace and use of internet service to coordinate illegal activities."[104] In September 2019, after 71 days, the government restored mobile data in five townships, but then reinstated it in February 2020.

In August of 2020, authorities ordered telecom service providers to lift the complete mobile data blackout and re-start 2G internet services, while also throttling 3G and 4G services. Although 2G internet is better than a total blackout, 2G does not provide meaningful access to the internet. This was supposed to last until March 31, 2021, but as we note above, the military launched a coup attempt, and after it got political support from factions of the Arakan National Party, authorities restored full internet access in Rakhine and Chin states on February 3, 2021. Unfortunately, the military junta cut access to the internet at the beginning of the coup, and has since strategically cut access to the internet and censored social media platforms[105] in a clear attempt to control the communications of people in Myanmar.[106]

In 2020, as Myanmar grappled with the COVID-19 pandemic and most of the world was under lockdown, the government continued to deny its most vulnerable and marginalized populations access to the internet and life-saving information. It appears the internet shutdown was used to hide the human toll of the conflict between the Tatmadaw and the Arakan Army in 2019-2020, as well as the army's "clearance operations."[107] The combination of active violent conflict, COVID-19, and the prolonged and targeted internet shutdown had a devastating impact on the Rohingya.

A collaborative report by civil society in Myanmar and the Cyberlaw Clinic and International Human Rights Clinic at Harvard Law School details the human impacts of these shutdowns in Myanmar. Researchers found "a distinct gendered impact, which hinders women from accessing information more so than their male counterparts," and numerous ways in which the information blackout compounded the damage wrought by COVID-19.[108]

Desperate to access information about COVID-19, connect with their loved ones, and continue their education, the Rohingya suffering the digital blackout were forced to commute long and dangerous distances, "cross checkpoints," and sustain extra expenses to access the internet.[109] One resident described the ordeal as follows:

> **"You have to suffer a lot when you really need to use the internet. In some places, you can get internet access…We have to use a Mytel SIM card. And we have to use the places close to the military compound. I don't want to use that much. But when I really must use the internet, I have to go outside the town and try to get access near the military compound. Sometimes, it rains so hard. It is really a pain when you have to stand up beside the highway while holding an umbrella all the time, to use the internet."[110]**

104 Telenor (2020, June 21). *Network shutdown in Myanmar, 21 June 2019*. Retrieved Jan 22, 2021 from https://www.telenor.com/network-shutdown-in-myanmar-21-june-2019/#:~:text=21%20June%2C%202019%3A%20On%2020,in%20Rakhine%20and%20Chin%20States.

105 *See supra* note 8.

106 *See supra* note 7.

107 108 109 110 *See supra* note 14.

Noting the dire situation in Rakhine and Chin states, human rights advocates launched online campaigns such as #StopInternetShutdownMM and organized protests offline to convince the government to end the information blackout. Some of the protesters organizing or participating in these peaceful protests and campaigns were arrested, fined, or both.[111]

Timeline: Myanmar shutdown actions from 2019-2020

June 21, 2019

Mobile data shut down

Affected area: Buthidaung, Paletwa, Rathedaung, Ponnagyun, Mrauk-U, Kyauktaw, Minbya, Myebon, and Maungdaw

September 1, 2019

Mobile data restored in five townships

February 3, 2020

Mobile shutdown reinstated in all townships

May 2, 2020

Shutdowns reinstated in four townships

Affected area: Buthidaung, Rathedaung, Myaebon, and Paletwa

May 2, 2020

Shutdown lifted in Maungdaw

August 1, 2020

3G and 4G internet throttled in eight townships

August 1, 2020

2G internet enabled in eight townships

October 31, 2020

Restrictions extended to December 31

December 29, 2020

Restrictions extended to March 31, 2021

111 Freedom House. *Myanmar Freedom of the Net (2020) report*. Retrieved Jan 22, 2021 from https://freedomhouse.org/country/myanmar/freedom-net/2020.

India entrenches use of shutdowns to suppress protests, cuts off Jammu and Kashmir

India imposed the lion's share of internet shutdowns in 2020, topping the global shame list — just as it did in 2018 and 2019. The government shut down the internet at least 109 times. While this figure is lower than the totals in the previous two years, India had instituted what had become a perpetual, punitive shutdown in Jammu and Kashmir beginning in August 2019. Residents in these states had previously experienced frequent periodic shutdowns, and in 2020 they were deprived of reliable, secure, open, and accessible internet on an ongoing basis.[112]

In January 2020, the Jammu and Kashmir government did restore 2G internet connection, but such connection was not meaningful.[113] No one in Jammu and Kashmir, except in Ganderbal and Udhampur, had access to 3G and 4G mobile internet, and there were numerous times in 2020 that the government cut off access even to 2G internet.

In some instances, when the inspector general of police for Kashmir shuts down 2G mobile internet, which is later confirmed by the home department of the government of Jammu and Kashmir, they also suspend voice calling and SMS services, leaving people in the area cut, including journalists, entirely off the grid and unable to access alternative means of communications.[114] In places like Anantnag, authorities repeatedly turned off 2G internet citing "the misuse of data services by anti-national elements."[115] In most cases, when people are cut off from 2G in Jammu and Kashmir, there are security incidents between the military and armed groups.[116]

As we have noted above, it is almost impossible to view, upload, and download images, large PDF documents or videos on a 2G internet connection. Disabling 2G means cutting off even the slowest and most minimal internet connection. Notably, when the government suspends mobile services for people using prepaid mobile services in places like Srinagar, they often spare those using post-paid services.[117] In many countries, most ordinary citizens can only afford or get access to prepaid services.[118] This kind of shutdown not only cuts people off from the internet during conflict when residents are in danger and struggling to stay safe, it expands the digital divide among people of different classes and income levels.

112 After 18 months of total shutdown and later mobile internet services throttling, 4G internet services are being restored in Jammu and Kashmir, as the government announced on February 5, 2021 it was lifting the restrictions. Singh, Manish (2021, February 5). *India is restoring 4G internet in Jammu and Kashmir after 18 months*. TechCrunch (2021, February 5). Retrieved Feb 9, 2021, from https://techcrunch.com/2021/02/05/india-is-restoring-4g-internet-in-jammu-and-kashmir-after-18-months/; and The Indian Express (2021, February 5). *Restoration of internet services in Jammu and Kashmir: A timeline.* Retrieved Feb 9, 2021, from https://indianexpress.com/article/india/jk-4g-internet-mobile-timeline-7176408/.

113 Chima, Raman Jit Singh (2020, January 11). *SC order on internet lockdown in J&K makes right noises but leaves matters of relief to the future.* The Indian Express. Retrieved Jan 22, 2021, from https://indianexpress.com/article/opinion/columns/jammu-and-kashmir-internet-shutdown-supreme-court-article-370-6210489/.

114 Government of Jammu and Kashmir Home Department (2020, January 26). Government order no: Home 06(TSTS) of 2020. Retrieved Jan 22, 2021, from http://jkhome.nic.in/G.O%20No.%2006(TSTS)%20of%202020%20dt.%2026.01.2020.pdf.

115 Government of Jammu and Kashmir Home Department (2020, January 28). Government order no: Home 07(TSTS) of 2020. Retrieved Jan 22, 2021, from http://jkhome.nic.in/G.O%20No.%2007(TSTS)%20of%202020%20dt.%2028.01.2020.pdf; and Government of Jammu and Kashmir Home Department (2020, February 20). Government order no: Home 14(TSTS) of 2020. Retrieved Jan 22, 2021, from http://jkhome.nic.in/14(TSTS)20200001.pdf.

116 Many of the internet shutdown orders contain information about security incidents. For instance, see this one: Government of Jammu and Kashmir Home Department (2020, April 30). Government order no: Home 38(TSTS) of 2020. Retrieved Jan 22, 2021, from http://jkhome.nic.in/38(TSTS)of2020.pdf, and similar ones can be found on this page: http://jkhome.nic.in/orders.html.

117 The Print (2020, May 19). *Internet services snapped in Srinagar after CRPF jawan, cop injured in encounter.* Retrieved Jan 22, 2021, from https://theprint.in/india/internet-services-snapped-in-srinagar-after-crpf-jawan-cop-injured-in-encounter/424671/.

118 *See supra* note 29.

With COVID-19 sweeping through India, numerous digital rights groups called for restoration of 3G and 4G internet in Jammu and Kashmir. Health care workers and others asked the government to restore meaningful internet access so they could download essential information like intensive care unit guidelines.[119] The government did not listen. In fact, in March of 2020, the principal secretary of Jammu and Kashmir's government extended the blackout, stating that "anti-national elements [are] spreading propaganda/ideologies through the transmission of fake news and targeted messages aimed at disturbing the public order…."[120]

There were also shutdowns in India for other reasons in 2020, and these may be ripe for challenge. Notably, in West Bengal, the West Bengal Board of Secondary Education and the state government's Home Department previously introduced a curfew-style internet blackout during the Madhyamik (secondary school) examinations, cutting off internet access every day during certain hours. This internet curfew lasted for more than nine days. However, in 2019, the Jodhpur bench of the Rajasthan High Court warned the state government that it could not order internet shutdowns during exams because it is beyond the scope of the Temporary Suspension of the Telcom Services (Public Emergency and Public Safety) Rules of 2017.[121] This rebuke of this state government practice from the Rajasthan High Court could inform court cases before other Indian high courts. The use of internet shutdowns in December 2019 to combat protests launched across India in response to the discriminatory Citizenship Amendment Act (CCA) resulted in other high courts seizing the issue. The Gauhati High Court on December 19, 2019 directed that the internet shutdown ordered for the entire state of Assam had to be rescinded early,[122] and a bench of the Allahabad High Court in the state of Uttar Pradesh took up a suo moto public interest hearing against the internet shutdown ordered there , observing on January 4, 2020 that it believed that continuous internet access fell with the right to life and liberty under Article 21 of India's constitution.[123]

THE COURT DECISION

A 2019 case against the shutdown in Kashmir made its way to the Indian Supreme Court. In January 2020, the highest court in the country ruled on the merits, declaring that shutdowns interfere with the fundamental right to freedom of expression and the right to life and liberty, that shutdown orders must be publicly available, and that indefinite shutdowns are unconstitutional, among other positive findings. The court also recommended that the existing Network Suspension Rules of 2017 be modified.[124]

119 Majid, Maqbool (2020). *'An Hour to Download ICU Guidelines': Amid COVID-19, Kashmir Doctors Struggle With Slow Internet.* The Wire. Retrieved Jan 22, 2021, from https://thewire.in/rights/coronavirus-kashmir-slow-internet.

120 Government of Jammu and Kashmir Home Department (2020, April 3). Government order no: Home 22(TSTS) of 2020. Retrieved Jan 22, 2021, from http://jkhome.nic.in/22(TSTS)of2020.pdf.

121 SFLC (2018, November 29). *Home Department, State Of Rajasthan: No More Internet Shutdowns For Prevention Of Cheating In Examinations.* Retrieved Jan 22, 2021, from https://sflc.in/home-department-state-rajasthan-no-more-internet-shutdowns-prevention-cheating-examinations.

122 The Print (2019, December 20). *Assam High Court dismisses govt review plea on order to resume internet services.* Retrieved Feb 10, 2021, from https://theprint.in/judiciary/assam-high-court-dismisses-govt-review-plea-on-order-to-resume-internet-services/338537/.

123 Emmanuel, Meera (2020, January 3). *Right to continuous internet part of right to live: Allahabad HC registers suo motu PIL over suspension of internet in UP.* Bar and Bench. Retrieved Feb 10, 2021, from https://www.barandbench.com/news/litigation/right-to-continuous-internet-part-of-right-to-live-allahabad-hc-registers-suo-motu-pil-over-suspension-of-internet-in-up.

124 Internet Freedom Foundation (2020, January 10). *SC's Kashmir communication shutdown judgement is just the beginning of a long uphill campaign.* Retrieved Feb 11, 2021, from https://internetfreedom.in/scs-judgement-on-kashmir-communication-is-just-the-beginning/.

The threat of an internet shutdown in the United States

Countries including the United States and India have laws on the books that facilitate internet shutdowns and communication blackouts. While having a body of law can make legal challenges easier, these laws can also represent a danger in and of themselves. For instance, currently the U.S. president has the authority to shut down the internet, under the communications war powers statute.[125] While this authority has never been used, the amount of deference granted to the president under the statute is unacceptable. All that is required to trigger the president's nearly unchecked powers to shut down communications platforms nationwide is a "state of public peril" or "other national emergency."

While Access Now opposes internet shutdowns in all forms as an inherently disproportionate interference with human rights, the U.S. Congress has proposed limiting the president's war powers through the Preventing Unwarranted Communications Shutdowns Act of 2020.[126] The legislation would restrict powers under the statute in key ways and require more checks and balances, making abuse of the provision less likely.

There are also other ways the U.S. could impose a shutdown. There is the power of presidential executive orders, which former U.S. President Donald Trump leveraged when he threatened to ban WeChat and TikTok in the U.S.[127] Trump issued orders stating that U.S. persons and companies, and others within the U.S., would be prohibited from doing business with ByteDance Ltd. (the China-incorporated firm that owns TikTok and other apps) and Tencent Holdings (including its WeChat service), starting 45 days after the orders were issued. This essentially set a deadline for companies to sell these apps to U.S. companies to continue operating.

In issuing the orders, the Trump administration did not offer evidence that these applications posed any new specific privacy or security threats to people in the U.S. Instead, the administration pointed more generally to a mix of vague privacy and national security concerns centering on the relationship between TikTok and WeChat's U.S. operations and the operation of their parent companies. Under Chinese law, the parent companies can be forced to give the Chinese government access to any data and insights they retain. TikTok claims that the company locates data outside the reach of the Chinese government, but the Trump administration never addressed those claims. Unless current U.S. President Joe Biden rescinds the actions taken by the prior administration, we can expect to see court cases play out in 2021. Regardless of what happens in this particular instance, however, the threat of an internet shutdown in the U.S. remains.

International organizations standing against shutdowns

The United Nations (U.N.) and other international organizations have boldly spoken out against internet shutdowns worldwide. Such efforts — including unanimous statements from the world's highest human rights body, resolutions, and joint statements from U.N. experts — clarify and confirm that internet shutdowns can never be justified under international human rights law.[128] Governments must therefore refrain from blocking, throttling, or shutting down the internet in order to comply with their international human rights obligations.

125 4.7 U.S. Code, § 606 (1934), Retrieved Jan 27, 2021, from https://www.law.cornell.edu/uscode/text/47/606.

126 Access Now (2020, October 22). *Shutting down the internet shouldn't be so easy*. Retrieved Jan 27, 2021, from https://www.accessnow.org/shutting-down-the-internet/.

127 Access Now (2020, September 18). *Trump executive orders targeting China-linked apps fail to protect privacy, harm human rights*. Retrieved Jan 27, 2021, from https://www.accessnow.org/trump-executive-orders-targeting-china-linked-apps-fail-to-protect-privacy-harm-human-rights/.

128 Organization for Security and Co-operation in Europe (OSCE) (2015, May 4). *Joint declaration by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, on Freedom of Expression and Responses to Conflict Situations*. Retrieved Jan 22, 2021, from http://www.osce.org/fom/154846.

In 2020, leaders at the U.N. became acutely aware of the fundamental importance of access to the internet as the global organization moved the majority of its operations online, while trying to meaningfully reach the global community and advance international cooperation amid a global health crisis, systemic racism, climate change, and rising authoritarianism. Indeed, in 2020 the U.N. Secretary General specifically highlighted the mass digitization of human relations during the health crisis and the inevitable impact this has on the world.[129] It is therefore no surprise that international policy initiatives in 2020 reflected the need to address this reality.

In his final report to the U.N. Human Rights Council in 2020, David Kaye, the former U.N. Special Rapporteur on Freedom of Opinion and Expression, recalled existing international norms condemning internet shutdowns, putting them in the context of the pandemic. In his report, Kaye stresses "there is no room for limitation of internet access at the time of a health emergency that affects everyone from the most local to the global level."[130] Adding to the progress represented by Kaye's report, the international community made huge strides at the U.N. Human Rights Council in connecting and condemning the use of government-ordered internet shutdowns to quell protests and dissenting voices.[131]

Also among the notable developments in 2020 was the launch of the U.N. Secretary-General's Roadmap on Digital Cooperation, a document centering human rights in the digital age. In the Roadmap, the Secretary-General affirms that "blanket internet shutdowns and generic blocking and filtering of services are considered by United Nations human rights mechanisms to be in violation of international human rights law."[132] That statement brings internet shutdowns to the forefront of ongoing efforts on digital cooperation and internet governance worldwide.

Overall, the U.N. provided important guidance and clarified human rights norms surrounding internet shutdowns in 2020. Future advocacy efforts should therefore build on these norms at the local, national, and regional level.

VI. Enabling and profiting from censorship: the case of Sandvine and Allot [redacted]

Shutdowns are not just ordered by governments and implemented by telcos. They are also facilitated by tech companies that supply the censorship technologies. In 2020 we saw Sandvine, a U.S. company with Canadian roots, provide Deep Packet Inspection (DPI) equipment to the Belarusian regime, technology that enabled shutdowns and website blocking during election protests. When a Bloomberg investigation revealed Sandvine's involvement in the Belarus

129 Villar, Mario (2020, April 2). *Antonio Guterres: tras el coronavirus el mundo y las relaciones humanas 'serán distintos'*. Euractiv. Retrieved Jan 25, 2021, from https://euroefe.euractiv.es/section/politicas/interview/antonio-guterres-tras-el-coronavirus-el-mundo-y-las-relaciones-humanas-seran-distintos/.

130 David Kaye (2020, April 23). *Report of the U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Disease pandemics and the freedom of opinion and expression, U.N. Doc A/HRC/44/49. Retrieved Jan 22, 2021, from https://undocs.org/A/HRC/44/49; Berena, Carolina Gonçalves et. al. (2020, June 30). COVID-19 & the right to protest: pressing issues at the 44th Human Rights Council. Access Now. Retrieved Jan 22, 2021, from https://www.accessnow.org/covid-19-the-right-to-protest-pressing-issues-at-the-44th-human-rights-council-this-week/.

131 Berena, Carolina Gonçalves et. al. (2020, June 30). *Pandemics, protests, and power in digital spaces: the 44th U.N. Human Rights Council Session in review*. Access Now. Retrieved Jan 22, 2021, from https://www.accessnow.org/pandemics-protests-and-power-in-digital-spaces-the-44th-u-n-human-rights-council-session-in-review/.

132 United Nations (2020, May). *UN Secretary-General's 'Digital Cooperation Roadmap*. Retrieved Jan 22, 2021, from https://undocs.org/A/74/821; and Organization for Security and Co-operation in Europe (May 2015). *Joint Declaration on Freedom of Expression and Responses to Conflict Situations*. Retrieved Jan 22, 2021, from https://www.osce.org/fom/154846.

shutdowns, the company initially denied all responsibility, claiming that internet access was not "a part of human rights."[133] However, bowing to pressure from the civil society, U.S. elected officials, and the public,[134] Sandvine announced that it would end its contract with Belarusian government, backtracking on its prior statement and acknowledging that access to the internet is a part of freedom of expression, a human right.[135] Sandvine later demanded that the Belarusian government return its DPI equipment and refrain from choking the internet to prevent the free flow of information to Belarusians.[136] It remains to be seen, however, whether Sandvine will take action to address past human rights violations, or undertake clear steps to prevent them going forward.[137] Since the company announced it was leaving Belarus, there have been multiple reports implicating Sandvine technology in rights violations in countries beyond Belarus, including Russia, Turkey, Pakistan, Sudan, Azerbaijan, Uzbekistan, and countries across the Middle East and North Africa region.[138] Will Sandvine refrain from working with these governments to choke and censor the internet, stifling freedom of expression and access to information?

Another company implicated in internet shutdowns in 2020 is the Israeli company Allot. The firm has struck deals in Kenya,[139] Azerbaijan,[140] and Tanzania,[141] and Access Now is aware that this company is trying to set shop in other East African countries. Like Sandvine, Allot sells DPI technology, which enables those using the equipment to read the contents of each packet of information traversing through the network. Allot promotes the surveillance capacity of its products, including the ability to see who is using which applications online, what they're doing in the apps, where they're logged on from, what videos they're watching, and with whom they interact. The firm also touts the technology's censorship capacities,

133 Gallagher, Ryan (2020, August 28). *Belarusian Officials Shut Down Internet With Technology Made by U.S. Firm*. Bloomberg. Retrieved Jan 22, 2021, from https://www.bloomberg.com/news/articles/2020-08-28/belarusian-officials-shut-down-internet-with-technology-made-by-u-s-firm; Gallagher, Ryan (2020, September 11). *U.S. Company Faces Backlash After Belarus Uses Its Tech to Block Internet*. Bloomberg. Retrieved Jan 22, 2021, from https://www.bloomberg.com/news/articles/2020-09-11/sandvine-use-to-block-belarus-internet-rankles-staff-lawmakers.

134 Access Now (2020, September 22). *Sandvine, Francisco Partners facing mounting pressure for accountability around censorship tool*. Retrieved Jan 22, 2021, from https://www.accessnow.org/sandvine-francisco-partners-facing-mounting-pressure-for-accountability-around-censorship-tools/.

135 Gallagher, Ryan (2020, September 15). *Francisco-Backed Sandvine Nixes Belarus Deal. Bloomberg*. Retrieved Jan 22, 2021, from https://www.bloomberg.com/news/articles/2020-09-15/sandvine-says-it-will-no-longer-sell-its-products-in-belarus.

136 Business & Human Rights Resource Centre (2020, September 25). *Sandvine demands that the National Traffic Exchange Center (NTEC) in Belarus refrain from choking the internet to prevent the free flow of information to Belarusians*. Retrieved Jan 22, 2021, from https://www.business-humanrights.org/en/latest-news/sandvine-demands-that-the-national-traffic-exchange-center-ntec-in-belarus-refrain-from-choking-the-internet-to-prevent-the-free-flow-of-information-to-belarusians/.

137 Access Now (2020, September 16). *Censorship tech company Sandvine's human rights "commitments" are too little too late*. Retrieved Jan 22, 2021, from https://www.accessnow.org/sandvine-human-rights-commitments-too-little-too-late/.

138 Gallagher, Ryan (2020, Oct. 8). *American Technology Is Used to Censor the Web From Algeria to Uzbekistan*. Bloomberg. Retrieved Jan 22, 2021, from https://www.bloomberg.com/news/articles/2020-10-08/sandvine-s-tools-used-for-web-censoring-in-more-than-a-dozen-nations; and Technology & Law Community (2020, October 24). *Sandvine … the surveillance octopus in the Arab region*. Retrieved Jan 22, 2021, from https://masaar.net/en/sandvine-the-surveillance-octopus-in-the-arab-region/.

139 Allot (2020). *Safaricom Gains Valuable Insights and Rolls Out Security-as-a-Service (SECaaS) For Its Customers*. Retrieved Jan 22, 2021, from https://www.allot.com/resources/success-stories/safaricom/.

140 QURIUM (April 10, 2018). *Corruption, Censorship, and Deep Packet Inspector Vendor*. Retrieved Jan 22, 2021, from https://www.qurium.org/alerts/corruption_censorship_and_a_dpi_vendor/.

141 Peter Micek (@lawyerpants) (2020). Peter Micek Twitter post. Twitter, 11:17 a.m. October 30, 2020, Retrieved Jan 22, 2021 from https://twitter.com/lawyerpants/status/1322179746160062464.

including the ability to "block harmful content," "record detailed web activity logs," and "control dangerous traffic."[142]

But this equipment can do more. It can shut down entire networks, websites, or services, degrade traffic so people cannot transmit video or photos, and speed up and slow down, redirect, or block traffic to or from certain users and servers. From a remote vantage point, the operator of these "middleboxes" can control traffic flows, or sit back and monitor our data as it transits the network.

In the lead-up to the October 28, 2020 presidential election in Tanzania, the Tanzania Communication Regulatory Authority, acting under the repressive Magufuli government, forced telecom and internet service providers to install internet filtering equipment made by Allot, and then deliberately disrupted Twitter, WhatsApp, and Telegram one day before the election. As of February 2021, Twitter was still blocked in Tanzania.[143]

In the same time frame in 2020, Allot's technology was likely being used simultaneously by the governments of Azerbaijan and Tanzania to unlawfully block internet traffic in their respective countries.[144]

In both Belarus and Tanzania, the evidence shows the sitting governments installed DPI technology before elections that challenged their hold on power, indicating that the ensuing censorship and internet shutdowns were premeditated. Sandvine, Allot, and other suppliers of this kind of censorship technology have a responsibility to heed clear signs their tools will be used to violate human rights, and to walk away from these kinds of sales.

VII. Challenging internet shutdowns on legal grounds: the case of Togo and Indonesia

We saw a number of court victories in the fight against internet shutdowns in 2020. These wins not only set a very important precedent, but are also a testament to the work civil society is doing to show courts and the public that internet shutdowns are a violation of human rights. We are used to governments ignoring appeals from citizens and the international community to #KeepItOn, so it is refreshing to have courts confirm that the fight for an open, secure, reliable, and accessible internet is not in vain, and that those challenging shutdowns are on the right side of history.

One such victory was in Indonesia, where the Jakarta Administrative court ruled that the deliberate 2019 internet shutdowns in Papua and West Papua were unlawful.[145] The case was brought by a coalition of civil society groups working on freedom of expression issues in Southeast Asia, including the Alliance for Independent Journalists (AJI) and Southeast Asia Freedom of Expression Network (SAFEnet). In their lawsuit against the Indonesian Ministry of Communication and Information and the president of Indonesia, the civil society claimants argued that the network disruptions violated the

142 Allot. *URL Traffic Filtering*. Retrieved Feb 10, 2021, from https://www.allot.com/service-providers/url-traffic-filtering/.

143 *See supra* note 80.

144 *See supra* note 140. *See also* Tackett, Carolyn et. al. (2020, October 15). *As conflict escalates, Azerbaijan's internet shutdown puts lives further at risk*. Retrieved Feb 9, 2021 from https://www.accessnow.org/azerbaijan-armenia-internet-shutdown/; and Geybulla, Arzu (2019). *Surveillance and Internet Disruption in Baku*. Coda Story. Retrieved Feb 9, 2021 from https://www.codastory.com/authoritarian-tech/surveillance-and-internet-disruption-in-baku/.

145 Access Now (2020, June 3). *Court rules the internet shutdowns in Papua and West Papua were illegal*. Retrieved Jan 22, 2021, from https://www.accessnow.org/court-rules-the-internet-shutdowns-in-papua-and-west-papua-are-illegal/.

fundamental rights of Indonesians. In particular, as a result of the internet shutdowns, journalists reporting from the regions of Papua and West Papua could not undertake their daily work to fulfill the right to provide timely and accurate information to the public. Access Now intervened with an amicus brief, arguing that internet shutdowns violated the right to free expression and access to information, freedom of assembly, as well as impacting economic and cultural rights, which are firmly rooted in Indonesia's Constitution and international human rights law.[146] The court ruled that internet shutdowns were a violation of the law by government officials.[147]

Another victory against internet shutdowns came from the Economic Community of West African States (ECOWAS) Community Court of Justice, which ruled that the September 2017 internet shutdown ordered by the Togolese government during protests were illegal and an affront to the applicants' right to freedom of expression.[148] The lawsuit was filed by Amnesty International Togo and other applicants, represented by Amnesty and Media Defence.[149] Access Now led a coalition of eight organizations to intervene, arguing that the shutdown was inconsistent with regional and international frameworks and violated the fundamental human rights of the Togolese people. While the government argued that it implemented the shutdowns on national security grounds, the court decision clearly stated that the justifications were inadequate and that the shutdowns violated the applicants' right to freedom of expression under the African Charter on Human and People's Rights.[150]

With the growth of the Digital Rights Litigators Network, Access Now and our partners commit to bringing more lawsuits against governments and companies to achieve transparency and accountability for internet shutdowns. In 2021, we plan to develop resources that will help our #KeepItOn coalition members and the broader digital rights community successfully challenge internet shutdowns in their respective jurisdictions and allow digital rights litigators to share experiences and lessons learned in Togo, Indonesia, India, and beyond. We invite jurists in institutions like law schools, bar associations, pro bono initiatives, and judges' organizations to collaborate with our network, and encourage them to fight shutdowns from their own perches.

Challenges and opportunities

1. #KeepItOn challenges and opportunities

The #KeepItOn coalition continues to face challenges in galvanizing efforts to strengthen policy and advocacy against internet shutdowns and highlight their impact on human rights globally. Given the dynamic and unpredictable nature of internet shutdowns as an issue, the coalition has over the years identified the need to employ a holistic and coordinated response, entailing gaining an understanding of the digital rights and political ecosystem, having the technical expertise for monitoring and running measurement tests, the ability to make a determination of how a shutdown has been implemented, and much more. The coalition continues to explore ways to ensure that

146 Krapiva, Natalia et. al. (2020, May 13). *Indonesians seek justice after internet shutdown.* Retrieved Jan 22, 2021, from https://www.accessnow.org/indonesians-seek-justice-after-internet-shutdown/.

147 The Jakarta Post (2020, June 3). *Jokowi 'violates the law' for banning internet in Papua, court declares.* Retrieved Jan 22, 2021, from https://www.thejakartapost.com/news/2020/06/03/jokowi-violates-the-law-for-banning-internet-in-papua-court-declares.html.

148 Anthonio, Felicia et. al. (2020, June 25). *ECOWAS Court upholds digital rights, rules 2017 internet shutdowns in Togo illegal.* Retrieved Jan 22, 2021, from https://www.accessnow.org/internet-shutdowns-in-togo-illegal/.

149 Media Defence (2020, Jun 25). *Landmark Judgment: ECOWAS Court Finds Togo Violated FoE with Internet Shutdown.* Retrieved Jan 22, 2021, from https://www.mediadefence.org/news/landmark-judgment-ecowas-court-finds-togo-violated-foe-with-internet-shutdown.

150 Kapriva, Natalia (2020, July 14). *ECOWAS Togo court decision: Internet access is a right that requires protection of the law.* Retrieved Jan 22, 2021, from https://www.accessnow.org/ecowas-togo-court-decision/.

the right partners get the necessary resources at the right time to carry out these tasks. We struggle to ensure that those offering measurement tools at minimum follow the principles of do no harm and continue to empower and put those affected by shutdowns at the center of focus. Moreover, we continue to see governments further narrow or close civic spaces in contexts where shutdowns are most prevalent, making it harder for grassroots advocacy movements to take hold or grow.

For these reasons, we are seeing the number and capacity of civil society organizations operating in such countries, and the number of people who have the skills needed for a holistic response, dwindle. However, the coalition does provide the opportunity to highlight these risks and threats to internet freedom at a global level, and this may help reduce the risks partner organizations in these countries are likely to face.

Coordinating these moving parts is a big task, but Access Now Grants, our grassroots grants program, is providing support to groups for capacity-building initiatives focused on internet shutdowns, and we believe this support can help to mitigate and improve the situation.[151]

Despite the challenges human rights advocates faced this year in fighting shutdowns, there are also new opportunities to push back against these acts of repression. Civil society groups and stakeholders across the globe share a common goal and passionate commitment to end internet shutdowns worldwide. We are seeing increased interest among governments, development partners, academia, regional and international blocs, the private sector, telecommunications and tech companies, and the general public in stopping shutdowns. While 2020 was a difficult year due to the COVID-19 pandemic, it also brought new recognition and emphasis on the internet as a means of ensuring continuity in work, education, and other critically important aspects of people's lives. It is therefore heartwarming to see that civil society has remained resilient and now has more support in our efforts to keep governments accountable through the #KeepItOn campaign.

2. Lessons learnt

As the coalition becomes increasingly strategic and innovative in fighting internet shutdowns, using diverse approaches, governments are also proactively preparing to impose shutdowns, learning from one another, and investing millions in the resources and infrastructure to control the online space. We don't have millions. However, we do have more than 240 civil society organizations globally that are dedicated to stopping shutdowns for good.

The #KeepItOn coalition now represents more than 100 countries, and we are continuing to explore opportunities for growth while building on lessons learnt. Shutdowns continue to be arbitrary and in many cases unpredictable, so we have identified strategic collaboration with grassroot groups as continuing to be a high priority. This campaign needs to become progressively more proactive rather than reactive. For instance, elections have shown to be a trigger point for internet shutdowns. Our elections calendar helps us map the countries where governments are likely to cut internet access or otherwise interfere with online communications during an election. In 2020, we have worked together to preemptively warn people against election-related shutdowns, provide them with the appropriate circumvention tips and tools in advance, and then actively monitor internet traffic before, during, and after the elections. In 2021, we will take this fight to the next level, doubling down on the effort to ensure everyone has access to an open, accessible, secure, and reliable internet that is necessary for democratic elections around the world. We will invest more in helping election observers around the world identify the different forms of internet shutdowns that can undermine the integrity of an election.

151 Access Now (nd). Access Now Grants. Retrieved Feb 9, 2021, from https://www.accessnow.org/grants/.

Even though Access Now coordinates the #KeepItOn coalition, the model for our coalition's work is decentralized — and that is a strength. We work very closely with organizations and individuals who have first-hand experience of internet shutdowns and we strive to define our campaign by these lived experiences. In providing guidance and resources to the coalition partners, Access Now aims to foster its development with the explicit aim of being inclusive and raising up the true diversity of experiences. This kind of collaboration and inclusiveness is crucial to the coalition's effort to stop shutdowns wherever they are ordered, and we pledge to keep improving that collaboration.

We also see an urgent need for stakeholders and groups that provide humanitarian support to at-risk communities, particularly international civil society organizations, to support the fight against internet shutdowns and highlight the impact shutdowns have on vulnerable populations. Moving forward, Access Now and the #KeepItOn coalition will go further to understand and document how people who are already targeted for discrimination and exclusion, particularly women, LGBTQ+ groups, ethnic and religious minorities, and others left at the margins of society, are disproportionately affected by internet shutdowns. We hope you will join us in this just fight.

CONTACT

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

Or reach out to
Felicia Anthonio at **felicia@accessnow.org**

Bangladesh: September 2029 - August 2020

Belarus: August - December 2

Myanmar: June 2019 - Ongoing

India: August 2019 - January 2020

Yemen: July 2020 -

SHATTERED DREAMS AND LOST OPPORTUNITIES

A year in the fight to #KeepItOn

#KeepItOn