



# *The* Internet Shutdowns *Issue*

When the internet is shut down, more than a connection is lost in the dark.

---

## TABLE OF CONTENTS

### THE PROBLEM

- [Shutting off the Lights](#)
- [A Gathering Dark](#)

### NEW PERSPECTIVES

- [Endangering Lives](#)
- [Immobilizing Economies](#)
- [Obstructing Educations](#)
- [Silencing Dissent](#)
- [Voices from the Dark](#)

### COUNTERMEASURES

- [Expose](#)
  - [Mitigate](#)
  - [Prevent](#)
-



# The Problem

At 12:34 PM local time on January 28, 2011, the lights went out in Egypt.

Almost simultaneously, about 3,500 individual Border Gateway Protocol routes – the paths systems use to communicate across the global internet – were withdrawn on orders from the Egyptian government, cutting the country off from the rest of the world and bringing internal communication to a halt. For five days, 93 percent of Egyptian networks remained completely unreachable.<sup>1</sup>

The internet shutdown in Egypt, brought on by a series of anti-government protests that had begun three days earlier, was not the first instance of government manipulation of the web.

The previous year, Tunisia significantly ramped up its already aggressive blocking of specific websites in response to unrest that would ultimately unseat its government.<sup>2</sup> In 2009, Iran, facing protests against the disputed victory of Mahmoud Ahmadinejad in that year's presidential election, slowed the internet to a crawl.<sup>3</sup> And in 2007, Guinean President Lansana Conté mandated the first widely known blackout, shutting down the fledgling internet industry in a nation where less than 1 percent of the population had access at all.<sup>4,5</sup> But never before had an entire country, one where more than a quarter of the population was connected to the internet, simply severed itself from the open web.<sup>6</sup>

The Egyptian government's actions, spotlighting a long-ignored risk, immediately reverberated across the world.

The international backlash was swift and forceful. In the United States, a long-touted bill that would grant the president emergency powers to shut off the internet died in the Senate amid the public uproar without ever receiving a vote.<sup>7</sup> Leaders in Germany, Austria, Australia, and

<sup>1</sup> Jim Cowie, "Egypt Leaves the Internet," *Internet Intelligence* (blog), January 27, 2011, <https://blogs.oracle.com/internetintelligence/egypt-leaves-the-internet-v3>.

<sup>2</sup> Joel Simon, "Tunisia Must End Censorship on Coverage of Unrest," January 5, 2011, <https://cpj.org/2011/01/tunisia-must-end-censorship-on-coverage-of-unrest/>.

<sup>3</sup> Christopher Rhoads, Geoffrey A. Fowler, and Chip Cummins, "Iran Cracks Down on Internet Use, Foreign Media," *Wall Street Journal*, June 17, 2009, <https://www.wsj.com/articles/SB124519888117821213>.

<sup>4</sup> Admire Mare, "State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe," *International Journal of Communication*, no. 14 (2020): 4244–63.

<sup>5</sup> "Individuals Using the Internet (% of Population) - Guinea," World Bank, accessed May 21, 2021, <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=GN>.

<sup>6</sup> World Bank, "Individuals Using the Internet (% of Population) - Egypt, Arab Rep.," n.d., <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=EG>.

<sup>7</sup> "Reaching for the Kill Switch," *The Economist*, February 10, 2011, <https://www.economist.com/international/2011/02/10/reaching-for-the-kill-switch>.



the European Parliament, meanwhile, were compelled to assure the public that they would never seek the authority to shut down the internet within their borders.<sup>8, 9, 10, 11</sup>

In the years since, internet shutdowns have been condemned as a violation of human rights by the United Nations, the African Commission on Human and Peoples' Rights, the Organization of American States, the Organization for Security and Co-operation in Europe, the Freedom Online Coalition, and a host of other international organizations and NGOs.<sup>12, 13</sup>

But even as international condemnation has mounted in the years since 2011, the number of shutdowns – intentional disruptions of internet-based communications by state actors – has grown exponentially, exploding from just a handful in 2012 to at least 213 across 33 countries in 2019.<sup>14, 15</sup> In 2020, even as the total number of shutdowns ticked down slightly due to delayed elections and global stay-at-home orders driven by the COVID-19 pandemic, the total duration of internet shutdowns worldwide jumped 49 percent.<sup>16</sup>

“Since we began tracking government-initiated internet shutdowns, their use has proliferated at a truly alarming pace,” explains Felicia Anthonio, Campaigner and #KeepItOn Lead at Access Now, a global human rights organization that works to defend and extend the digital rights of people around the world and has been tracking internet shutdowns since 2016. “As governments across the globe learn this authoritarian tactic from each other, it has moved from the fringes to become a common method many authorities use to stifle opposition, quash free speech and muzzle expression.”

Internet shutdowns lie along a spectrum, from a full shutdown or blackouts that cut off access to the entire web within a given region, to more targeted partial shutdowns that impact specific services, like popular social media and messaging apps.

<sup>8</sup> Lauren Feeney, “Could Our Government Shut down the Internet?,” *PBS*, February 3, 2011, sec. The Daily Need, <https://www.pbs.org/wnet/need-to-know/the-daily-need/could-our-government-shut-down-the-internet/6975/>.

<sup>9</sup> Renai LeMay, “No Internet ‘Kill Switch’ for Australia, Says Conroy,” *Delimiter*, March 2, 2011, <https://delimiter.com.au/2011/02/03/no-internet-kill-switch-for-australia-says-conroy/>.

<sup>10</sup> Neelie Kroes, “Response to Parliamentary Question P-002322/2011” (2011), [https://www.europarl.europa.eu/doceo/document/P-7-2011-002322-ASW\\_EN.html](https://www.europarl.europa.eu/doceo/document/P-7-2011-002322-ASW_EN.html).

<sup>11</sup> Kyle James, “Internet ‘Kill Switch’ Concerns Voiced in Germany,” *DW*, March 2, 2011, <https://www.dw.com/en/internet-kill-switch-concerns-voiced-in-germany/a-14816106>.

<sup>12</sup> “The Promotion, Protection and Enjoyment of Human Rights on the Internet,” Pub. L. No. A/HRC/32/L.20 (2016), [https://www.article19.org/data/files/Internet\\_Statement\\_Adopted.pdf](https://www.article19.org/data/files/Internet_Statement_Adopted.pdf).

<sup>13</sup> Office of the Special Rapporteur for Freedom of Expression, “Twentieth Anniversary of the Joint Declaration: Challenges to Freedom of Expression in the Next Decade,” Text, Organization of American States, July 10, 2019, <https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1146&IID=1>.

<sup>14</sup> Deji Bryce Olukotun, “Internet Shutdowns – an Explainer,” *Deutsche Welle*, December 12, 2016, <https://www.dw.com/en/internet-shutdowns-an-explainer/a-36731481>.

<sup>15</sup> Berhan Taye et al., “Internet Shutdown News and Report: A Year in the Fight to #KeepItOn,” *Access Now* (blog), March 3, 2021, <https://www.accessnow.org/keepiton-report-a-year-in-the-fight/>.

<sup>16</sup> Isobel Asher Hamilton, “268 Million People Had Their Internet Shut off by Government-Imposed Blackouts in 2020, up 49% from 2019,” *Business Insider*, January 5, 2021, <https://www.businessinsider.com/government-internet-blackouts-human-rights-india-kashmir-coronavirus-2021-1>.



The justifications for shutdowns range from national security concerns to curbing the spread of misinformation, and even preventing cheating on standardized tests. But as blunt instruments impacting entire populations, they raise grave human rights concerns.<sup>17, 18</sup> They also have devastating effects on the economy, healthcare, education, and civil society.

In just the first five months of 2021, Access Now documented 50 internet shutdowns in 21 countries. These disruptions interfere with freedom of opinion and expression, access to information, and freedom of assembly. During crises, like armed conflict or the Covid-19 pandemic of the last year, shutdowns further cut individuals off from life-saving information.

Shutdowns also cost the global economy billions. In Myanmar, where shutdowns have been the most prolonged and severe, the economic loss is estimated at 2.1 billion USD, more than 2.5 percent of the nation's GDP. In percentage terms, Myanmar's shutdowns have inflicted on the country approximately half the damage wrought by the Great Recession on the US economy in less than a third of the time.<sup>19</sup>

## Shutting Off the Lights

The internet is not a single network, but a network of networks.

The closest the internet has to a core are the roughly 420 submarine fiber-optic cables – each a network unto itself – that span an estimated total of more than 800,000 miles. Enough to circle the globe 30 times over, this underwater cable highway transforms isolated networks into the global web.

Commonly known as the internet backbone, these cables, through which the entire global web – text messages and bank transactions, home videos and CT scans – flows as pulses of light through strands of glass little wider than a human hair, are more akin to its spinal cord.

And severing them can leave entire regions immobilized.

In 2008, unintentional damage to two fiber optic cables in the Mediterranean Sea cut connection speeds by up to 70 percent in 14 countries from North Africa to India for several

<sup>17</sup> Deniz Duru Aydin, "Five Excuses Governments (Ab)Use to Justify Internet Shutdowns | DW | 24.10.2016," DeutscheWelle, October 24, 2010, <https://www.dw.com/en/five-excuses-governments-abuse-to-justify-internet-shutdowns/a-36135649>.

<sup>18</sup> Christopher Giles and Peter Mwai, "Africa Internet: Where and How Are Governments Blocking It?," *BBC News*, January 14, 2021, sec. Africa, <https://www.bbc.com/news/world-africa-47734843>.

<sup>19</sup> Samuel Woodhams and Simon Migliano, "The Global Cost of Internet Shutdowns," *Top 10 VPN*, June 7, 2021, <https://www.top10vpn.com/cost-of-internet-shutdowns/>



days, while the Maldives was taken offline entirely.<sup>20, 21</sup> Internet shutdowns, however, rarely stem from intentional damage to the internet's physical infrastructure.

When these submarine backbone cables reach shore, they connect to regional and national networks using the Border Gateway Protocol in a process known as peering.

At these edge points, networks exchange information not only about how to connect with each other, but also the paths to every other network they can reach, creating a global map of the web.

These regional and national networks, in turn, peer with lower-level networks, all the way down to the local Internet Service Providers (ISPs) that carry the global web down to an individual device.

This hierarchical, distributed structure makes the web as a whole remarkably robust, but creates multiple pinch points, allowing state actors to choke off access not just to entire countries, but also subregions and even specific neighborhoods. It can also make shutdowns particularly challenging to track and verify.

In countries where shutdowns are most common, ISPs are often owned by just a handful of providers including, commonly, the state. But even privately held network owners can be compelled to comply with government orders to restrict access to the web.

In highly developed markets like the United States, where there are thousands of ISPs, the sheer size of the market provides a degree of protection. But in many countries, as in Egypt in 2011, the web can be brought to a shuddering halt with just a few phone calls.<sup>22</sup>

Shutdowns – both full and partial – are implemented through local ISPs using six primary methods:

<sup>20</sup> "Severed Cables Disrupt Internet," *BBC News*, January 31, 2008, <http://news.bbc.co.uk/2/hi/technology/7218008.stm>.

<sup>21</sup> Kim Zetter, "Undersea Cables Cut; 14 Countries Lose Web -- Updated," *Wired*, December 19, 2008, <https://www.wired.com/2008/12/mediterranean-c/>

<sup>22</sup> Jim Cowie, "Egypt Leaves the Internet," *Internet Intelligence* (blog), January 27, 2011, <https://blogs.oracle.com/internetintelligence/egypt-leaves-the-internet-v3>.



## Throttling

The internet does not have to be shut off to be made unusable. Instead, ISPs can slow – or “throttle” – connections to the point that loading websites becomes impractical or impossible. State-mandated bandwidth throttling can be particularly hard to identify and verify, making it an attractive option for governments seeking to conceal their actions.

## IP Blocking

Devices connected to the internet, including phones, computers, and the servers that host websites, locate each other across the web by means of unique keys called IP Addresses. ISPs can use these addresses to target shutdowns with almost surgical precision, blocking specific websites and platforms in narrow geographic locations, while still allowing particular individuals in affected regions unfettered access.

## Mobile Data Shutoffs

In many low-income countries, where access to computers is limited but smartphone ownership is common, a shutdown of mobile data services is sufficient to achieve the goals of a complete shutdown while leaving some connection to the global web intact.

## DNS Interference

The Domain Name System (DNS) is the phonebook of the internet, pairing domain names like google.com with an IP address where that website can be reached. Much like the web itself, DNS is a hierarchical system, and these initial requests generally pass through one or more devices, known as recursive resolvers, before reaching the authoritative sources that pair domain names with IP addresses.

When a web service is first requested by a client, its IP address is often stored, or cached, on a resolver on the network. This allows for faster response times, but also creates opportunities for manipulation.

ISPs, which typically control a resolver, can configure it to return no response, an invalid IP address, or the address of a different service entirely, redirecting the user to a location they didn't intend to reach. Even if the ISP's resolver is operating correctly, a DNS injector inserted upstream of the resolver can respond more quickly than the authoritative sources, resulting in users receiving forged answers in an attack known as “cache poisoning”.

## Server Name Identification Blocking

For much of the early history of the web, communication between devices and the servers hosting websites was unencrypted and took place in the open. This made it easy for network



owners to interfere with communication over the hypertext transfer protocol (HTTP), the standard used for most internet-based communication, with websites they wished to block. The advent and rapid spread of HTTPS, an encrypted standard extending HTTP, has made it much more difficult for censors to eavesdrop on or tamper with this communication. Instead, network owners intervene before a secure connection can be established, blocking the connection as soon as a server name identification request is made to a targeted service.

## **Deep Packet Inspection (DPI)**

Information to be transmitted across the internet is first cut up into smaller pieces called packets. These packets consist of two parts: a header, containing information about where the packet originated, its destination, and other metadata used for routing, and a payload, consisting of the actual contents of the communication. During standard internet-based communication, only data in the packet header is used.

DPI occurs when network owners dig deeper into the packet payload to learn not only about which sites or applications individuals are visiting, but what they are doing on them, allowing for much finer-grained control over access to information. In some cases, governments even alter the payload, changing the contents of a website or message as it is being transmitted to the user.

The additional information network owners and monitors can glean from DPI can be used during internet shutdowns to block connections even via Virtual Private Networks. More commonly, however, DPI is used as part of larger and more sophisticated permanent censorship and surveillance operations, like the Great Firewall of China, allowing censors to block access to specific content rather than entire services.

In practice, governments often implement shutdowns using a combination of these tactics. And shutdowns themselves are often dynamic, escalating from partial shutdowns impacting just a few sites and services to total blackouts before receding again.

As tactics evolve, some countries where blackouts have become a fixture of daily life are graduating from shutdowns to far more sophisticated, and permanent, controls on the internet, casting their people into a perpetual informational half-light.



## *A Gathering Dark*

While data prior to 2016 is patchy, and the true total number of internet shutdowns is likely unknowable, nearly 850 intentional shutdowns have been documented and verified over the last decade via Access Now's Shutdown Tracker Optimization Project (STOP). Of these, 768 shutdowns across 63 countries have taken place just in the last five years.

Once a seemingly minor and geographically isolated problem, incidents of shutdowns have grown at an exponential rate, impacting 33 separate countries in 2019 alone and peaking in 2018 with a 72 percent surge in the number of shutdowns year over year.

Now, there is rarely a day where at least one part of the world has not been cast into the dark.



# *New Perspectives*

*“When I lost the internet, I think I lost my life. There is no hope for us now.”*

— Shamima Bibi, Kutupalong Refugee Camp, Cox's Bazar, Bangladesh

Shutdowns don't merely stop people from sending a text or browsing updates on social media. As the internet has grown central to virtually every aspect of life across the globe, particularly during the COVID-19 pandemic, their effects ripple through impacted communities, depressing local economies, cutting off access to education, impeding healthcare delivery, and stifling political opposition.

## *Endangering Lives*

As the internet has grown central to healthcare provision, shutdowns pose an increasing risk to human life. While little empirical research exists quantifying the effects, anecdotal evidence suggests that blanket blackouts not only disrupt vital flows of communications between patients and doctors, they can also lead to medicine shortages, delay the deployment of critical medical professionals to emergencies, and threaten the financial viability of healthcare providers.<sup>23, 24, 25</sup>

The COVID-19 pandemic brought these issues into sharp relief: Blackouts cut entire regions off from life-saving public health advice, leaving some communities in Myanmar completely unaware of the existence of the virus months into the pandemic, while in Kashmir shutdowns prevented downloads of mobile test and trace apps, stymying efforts to contain the virus as infection rates exploded across the subcontinent.<sup>26, 27</sup>

<sup>23</sup>Jan Rydzak, “Disconnected: A Human Rights-Based Approach to Network Disruptions” (Global Network Initiative, May 2018),

<https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf>.

<sup>24</sup>Patrick Kingsley, “Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards,” *The New York Times*, September 2, 2019, sec. World,

<https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html>.

<sup>25</sup>Okwen Mbah, Miriam Nkangu, and Zak Rogoff, “Don't Ignore Health-Care Impacts of Internet Shutdowns,” *Nature* 559, no. 7715 (July 25, 2018): 477–477, <https://doi.org/10.1038/d41586-018-05797-4>.

<sup>26</sup>Athar Parvaiz, “Kashmir Internet Blackouts Hinder Health Services, Contact Tracing,” *Reuters*, May 20, 2020, <https://www.reuters.com/article/us-health-coronavirus-india-tech-trfn-idUSKBN22W052>.

<sup>27</sup>Jason Slotkin, “Parts Of Myanmar Unaware Of COVID-19 Due To Internet Ban, Rights Advocates Say,” *NPR*, accessed May 24, 2021,



## *Immobilizing Economies*

Between January 2019 and June 2021, 228 major internet shutdowns in 41 countries cost the global economy billions.<sup>28, 29</sup> But this figure provides only a hazy glimpse of the direct costs of shutdowns.

Unable to connect with international partners and domestic consumers, business owners impacted by shutdowns regularly report lost deals and opportunities for expansion, depriving local communities of economic growth. Informal economic activity, which in many countries commonly takes place via internet platforms including WhatsApp and Facebook groups, ceases when the networks drop.

Internet shutdowns also regularly impact both ATMs and mobile money providers, grinding commerce to a halt. With no means to make or receive payments, businesses are often forced to close entirely.<sup>30</sup>

Shutdowns also impose heavy costs on network providers, limiting the number of providers willing to enter the market and perpetuating the conditions that facilitate shutdowns in the first place.<sup>31</sup>

In 2018, Al-Jazeera reported how a 93-day shutdown in the Anglophone regions of Cameroon had crippled the country's burgeoning technology industry, forcing businesses to shutter and workers to relocate to new areas of the country or to leave entirely.<sup>32, 33</sup>

<https://www.npr.org/sections/coronavirus-live-updates/2020/06/24/882893419/parts-of-myanmar-unaware-of-covid-19-due-to-internet-ban-advocates-say>.

<sup>28</sup> Samuel Woodhams and Simon Migliano, "The Global Cost of Internet Shutdowns," Top 10 VPN, June 7, 2021, <https://www.top10vpn.com/cost-of-internet-shutdowns/>.

<sup>29</sup> Darrell M. West, "Internet Shutdowns Cost Countries \$2.4 Billion Last Year" (Brookings Institute, October 2016), <https://www.brookings.edu/wp-content/uploads/2016/10/internet-shutdowns-v-3.pdf>.

<sup>30</sup> Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards," *The New York Times*, September 2, 2019, sec. World, <https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html>.

<sup>31</sup> Admire Mare, "State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe," *International Journal of Communication*, no. 14 (2020): 4244–63.

<sup>32</sup> Irene Zih Fon, "Tech Startups Struggle to Regain Business and Boost Morale After Internet Shutdown," *Global Press Journal*, October 20, 2017, <https://globalpressjournal.com/africa/cameroon/tech-startups-struggle-regain-business-boost-morale-internet-shutdown/>.

<sup>33</sup> Yarno Ritzen, "Cameroon Internet Shutdowns Cost Anglophones Millions," Al Jazeera, January 26, 2018, <https://www.aljazeera.com/news/2018/1/26/cameroon-internet-shutdowns-cost-anglophones-millions>.



## *Obstructing Educations*

Shutdowns also have a devastating impact on the education systems of affected countries. Even a 1 percent increase in a country's level of internet connectivity has positive impacts on both educational attainment rates and GDP per capita, highlighting the educational stakes of shutdowns.<sup>34</sup> Research has further shown that network disruptions interfere with lesson planning, instruction, and learning as well as impeding communication between instructors, school administrators, students, and families.<sup>35</sup>

School closures driven by the COVID-19 pandemic, affecting roughly 90 percent of enrolled students globally in 2020, made the impact of internet shutdowns on education particularly acute.<sup>36</sup> With remote instruction inaccessible, students were forced to make painful choices to forgo their education or risk not only their health, but also the health and safety of their families and communities.<sup>37, 38 39</sup>

## *Silencing Dissent*

Shutdowns are most commonly deployed around elections and moments of potential social unrest, particularly public demonstrations. While usually excused on grounds of stemming the spread of misinformation and promoting public order, their true purpose is often more nefarious.

During elections, government-imposed blackouts prevent opposition candidates from connecting with voters to build support, restrict the ability of citizens to organize, and undermine the efforts of election observers to ensure the integrity of the vote, insulating those in power from democratic accountability.

In 2021, the Ugandan government ordered a complete internet blackout on the eve of their national elections – elections already marred by violence and the arrest of rival candidates. Amnesty International quickly decried the move as “clearly intended to silence the few

<sup>34</sup> Economist Intelligence Unit, “Connecting Learners: Narrowing the Educational Divide,” June 15, 2021, <https://connectinglearners.economist.com/connecting-learners/>.

<sup>35</sup> Kudzayi Savious Tarisayi and Everjoy Munyaradzi, “A Teacher Perspective on the Impact of Internet Shutdown on the Teaching and Learning in High Schools in Zimbabwe,” *Human Behavior and Emerging Technologies* 3, no. 1 (January 2021): 169–75, <https://doi.org/10.1002/hbe2.230>.

<sup>36</sup> Axelle Devaux, “Digital Learning Needs to Benefit All Children When Schools Close,” May 4, 2020, <https://www.rand.org/blog/2020/05/digital-learning-needs-to-benefit-all-children-when.html>.

<sup>37</sup> Febriana Firdaus, “Indonesia Said a Broken Cable Caused an Internet Blackout in West Papua. Locals Aren't Buying It.,” *Rest of World*, May 20, 2021, <https://restofworld.org/2021/west-papua-deliberate-internet-blackout/>.

<sup>38</sup> Nandita Sengupta, “How Internet Shutdown Has Hurt Students in Kashmir,” *The Times of India*, January 20, 2020, <https://timesofindia.indiatimes.com/india/how-internet-shutdown-has-hurt-students-in-kashmir/articleshow/73356950.cms>.

<sup>39</sup> Nicholas Thomas, “Lessons from the Virtual Front: Tertiary Education in Hong Kong,” *CEA Critic* 82, no. 3 (2020): 297–300, <https://doi.org/10.1353/cea.2020.0025>.



accredited election observers, opposition politicians, human rights defenders, activists, journalists, and bloggers who are monitoring the elections.”<sup>40, 41</sup>

More chillingly, regimes can use shutdowns to conceal far graver human rights abuses, including attacks on civilians. Researchers found that violence during the heat of the Syrian Civil War in 2012 peaked during internet shutdowns, while Amnesty International determined Iran had used a shutdown to conceal the killing of 300 civilian protesters in 2019, suggesting they have become part of a playbook to mask heavy-handed tactics by armed forces.<sup>42, 43</sup>

## *Voices from the Dark*

Those impacted by internet shutdowns do not experience them as aggregate statistics – discrete ticks down in GDP or educational attainment rates. Shutdowns upend entire lives, severing people’s connections to the world. More than anything else, perhaps, shutdowns deny individuals their voice. But it is only through their stories that the true impact of shutdowns can be understood.

“Losing access to the internet can seem like a trivial thing,” Marianne Díaz Hernández, a Venezuelan lawyer, digital rights activist, and #KeepItOn fellow with Access Now, says. “But the pandemic over the last year has shown that the internet truly is a lifeline. When governments shut down the internet, all elements of people’s lives are impacted.”

### **Benjamin, 34, Bukavu, Democratic Republic of Congo Full Shutdown: Dec. 31, 2018 – Jan. 20, 2019**

*The internet was shut off as our country was preparing for our elections. The ruling party had previously banned all demonstrations by opposition parties, and whenever a political opponent tried to make an appearance or an appeal to the public, the government would order the heads of the telecom companies to shut down the internet, text messaging, and sometimes even phone calls. The only way for the people to communicate was to cross the border into Rwanda to buy Rwandan SIM cards.*

*There is ongoing armed ethnic violence throughout our region, and most of the people live in insecurity. Without the internet, conflicts burst out and we do not know about it. Women are*

<sup>40</sup> Nita Bhalla and Alice McCool, “100 Hours in the Dark: How an Election Internet Blackout Hit Poor Ugandans,” *Reuters*, January 20, 2021, <https://www.reuters.com/article/us-uganda-internet-rights-trfn-idUSKBN29P1V8>.

<sup>41</sup> “Uganda: Authorities Must Lift Social Media Block amid Crackdown Ahead of Election,” Amnesty International, January 13, 2021, <https://www.amnesty.org/en/latest/news/2021/01/uganda-authorities-must-lift-social-media-block-amid-crackdown-ahead-of-election/>.

<sup>42</sup> Sarah Myers West, “Research Shows Internet Shutdowns and State Violence Go Hand in Hand in Syria,” Electronic Frontier Foundation, July 1, 2015, <https://www.eff.org/deeplinks/2015/06/research-shows-internet-shutdowns-and-state-violence-go-hand-hand-syria>.

<sup>43</sup> Amnesty International, “A Web of Impunity: The Killings Iran’s Internet Shutdown Hid,” November 16, 2020, <https://iran-shutdown.amnesty.org/>.



*raped. Villages are burned down. It is almost impossible to gather information on these incidents to advocate for the people or to keep them safe.*

*I've been working to build a small network to connect my city of Bukavu. During the shutdown I was arrested for two days, and some of our equipment was confiscated.*

*The internet is our best hope for development. The internet can help us reduce armed conflict, end the system of violence and rape against women, connect communities to share their experiences for sustainable development, facilitate trade, and support education. But because of the shutdown none of this can go on.*

**Wegene, 34, Addis Ababa, Ethiopia**

**Full Shutdown: Nov. 4, 2020 – Ongoing**

*I checked social media one night as I was going to bed and saw government officials calling on everyone to calm down. At the same time, I saw some of my friends getting nervous. Later, I learned that the government had launched an attack on the Tigray region. Moments after that the network was shut off.*

*I live in Addis Ababa, but I was born and raised in Axum, Tigray, and my family is still there. I used to talk to them three days a week, but with both the internet and landline calls down, I haven't been able to reach them.*

*I heard through Médecins Sans Frontières [an international medical humanitarian NGO] that the main hospital in Axum, St. Mary's, had been looted. My father needs medicine for his hypertension and a surgery he had before the war broke out. I wasn't sure he'd be able to get it and there was no way for me to find out. For days I had bad dreams. I couldn't eat. Couldn't work. I thought maybe he was gone.*

*Someone recently passed through Addis Ababa and told me they were okay, but I can't be sure. I still haven't heard his voice.*

**Jameel, 16, Baghdad, Iraq**

**Full Shutdown: Oct. 3, 2019 – Oct. 10, 2019**

**Partial Shutdown: Oct. 2, 2019 – Nov. 21, 2019**

*At the start of the protests – when the government was only blocking social media platforms – VPNs and Tor were effective as I could just open them and go back to using social media as usual, but when the complete shutdown happened they were mostly useless.*

*I couldn't talk to my parents without spending money, nor could I contact my relatives living outside Iraq. I lost connections to all my online friends outside Iraq.*



*Lots of online businesses exist in Iraq, apps, Facebook pages, websites, banks, and more. They've all been severely impacted by the shutdown as their businesses are to a large extent reliant on internet availability. I owned a clothing business based in the US that I managed remotely, and I was completely cut off from suppliers and customers once the shutdown came into effect. I couldn't even stop the online ad campaigns we were running and spending money on daily.*

*The internet is a really important source for news and updates in Iraq, as the accuracy and truthfulness of the TV stations can't be relied on. When the internet was shut down, closures of the TV stations that had been supportive of the protests followed, so the only channels remaining on TV were government-affiliated ones or neutral ones that didn't report on the protests or what was happening.*

*The shutdown has hurt students that relied on online school groups, hurt protestors, hurt Iraqis abroad that wanted to check in on their relatives, hurt Iraqis engaged in online communities, and more.*

*I've lost all hope in my country because of this shutdown.*

**Pino, 36, Tororo, Uganda**

**Full Shutdown: Jan. 13, 2021 – Jan. 18, 2021**

**Partial Shutdown: Jan. 12, 2021 – Feb. 10, 2021, Facebook remains blocked**

*I work in digital literacy, advocacy and research and innovation in digital spaces, specifically for women and girls in Uganda. Digital literacy for women and girls is so lacking here that their presence online is almost not felt. We want to close that gap and bring more women and girls into online spaces, so they can harness the opportunities there.*

*One evening, as I was organizing my audio for our radio station, I realized I had an internet connection issue. I troubleshot all the possibilities and everything seemed to be in place. I called a friend in the city who told me the internet was completely shut down. I almost fell off my chair. At the same time there was a lockdown due to COVID, so we couldn't cross over to Kenya to get access to the internet.*

*It was devastating. I felt like a piece of me had been cut off. I was so idle. It was as if I was on an island all alone. I couldn't reach out to anyone else. It was a total blackout for me.*



**Daisy, 30, Kampala, Uganda**

**Full Shutdown: Jan. 13, 2021 – Jan. 18, 2021**

**Partial Shutdown: Jan. 12, 2021 – Feb. 10, 2021**

*I went to town one day to run some errands when I ran out of cash. To my surprise, there were no operating mobile money outlets, and the ATMs weren't working. Everything was down and everyone seemed confused about what was happening and stranded like me.*

*I sell women's clothes and accessories, liquid soap and packaged foods. I share my products online – on different Facebook and WhatsApp groups – and people reach out to me with their orders and then I deliver them. I have no physical shop so I depend entirely on the internet and referrals.*

*On a good day, I could sell six dresses for about \$22 each, and maybe \$50 worth of food items. With the internet shutdown, I was left with no option but to hawk my goods, make door-to-door calls looking for customers. Some days I didn't make any sales at all.*

*Facebook is still blocked in Uganda and it is like a crime to be on it. Internet shutdowns are a weapon for the government. They use them to frustrate people – especially the youth – and to block the flow of information and keep people in fear.*

**Mohammed, 46, Cox's Bazar, Bangladesh**

**Mobile Data Shutdown: Sep. 9, 2019 – Aug. 29, 2020 (connection remains unstable)**

*The situation for the Rohingya in the refugee camps is dire. The internet was shut down in the camps in September, and authorities seized Bangladeshi SIM cards from the Rohingya to ensure we would not be able to get online. Even after service was partially restored, our phones show 4G but we still cannot connect.*

*The shutdown made it impossible for refugees to contact relatives living abroad to get help, or to get information about our repatriation.*

*Even though the camps are surrounded by security forces, they cannot control inside the camps. The density of housing in the camps, and the difficulty in reaching certain areas has made it easy for traffickers, smugglers, and murderers to hide. Without the internet we cannot share information to stay safe.*

*Things got harder after COVID-19. The World Food Program is still distributing food, but it's not enough, and most other NGOs have stopped operating entirely, so there is no work and no money in the camps. Refugees also can't go out and find work on local farms.*



*When the pandemic started, hospitals shared a lot of information online about the disease, but we weren't able to reach it. Our children also haven't been able to attend online classes, costing them their education.*



# *Countermeasures*

The internet has allowed entire countries to leapfrog forward in their development, delivering the latest information and resources to students and teachers, connecting healthcare workers with remote communities to save lives, and providing a platform for individuals to express themselves and connect across the globe. But the web is not unbreakable.

It's vital society has access to tools to expose where access is being cut off, technologies that mitigate the destructive potential of shutdowns, and connected global movements to help drive change.

## *Expose*

States rarely admit to cutting off access to the internet, and the distributed, physical infrastructure of the web can provide cover for malignant actors, meaning internet shutdowns have historically been notoriously difficult to track. But in recent years, through the combined efforts of academics, technologists and NGOs, new systems have been created to document and verify shutdowns, shining a brighter light on the problem.

## **Tracking outages**

The [Google Transparency Report](#) logs access disruptions to Google products, both accidental and intentional, along with direct access to the outage data and additional context, shining a light on government interference with the web worldwide.

This report, alongside [Facebook's Transparency Center](#) and [Access Now's STOP database](#), contributes crucial data for [The Internet Society's Pulse tracker](#). By providing a live view of global shutdowns and their impact alongside historical data and local context, Pulse and other tools developed by the [Center for Applied Internet Data Analysis \(CAIDA\)](#), [The Open Observatory of Network Interference \(OONI\)](#), [Kentik](#), and [Censored Planet](#), play a crucial role in exposing shutdowns worldwide.

## **Measuring the cost**

The full economic damage caused by internet shutdowns is incalculable, but methodology developed by the Brookings Institution and the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) can provide an estimate of the staggering first-order costs of full and partial shutdowns around the globe.



These methodologies highlight the extreme toll shutdowns impose, providing critical context to citizens, journalists, and policy makers, and allowing them to hold governments accountable for their actions.

## Mitigate

Shutdowns lie along a spectrum – from the targeted blocking of a single site (partial) to complete blackouts (full) – and governments deploy a wide array of tactics in the ever-evolving cat-and-mouse game between those who seek to shut down access to information, and those who seek to circumvent them.

While full internet blackouts can be extremely difficult to circumvent, a range of tools exist to dampen the impacts of partial shutdowns on individuals and communities. As partial shutdowns rely on both identifying attempted connections to banned services and subsequently interfering with those connections, this form of censorship can be bypassed by successfully preventing either.

For those impacted by shutdowns, Access Now provides a global [Digital Security Helpline](#), which offers direct technical assistance to connect people with the services that can keep them online. Jigsaw has also been exploring various mitigation techniques, with tools such as [Outline](#) and [Intra](#).

## Mesh Networks

While impractical for most internet uses, and often lacking in adequate security, mesh networks can provide essential connectivity during full internet shutdowns.

Mesh networks work by bypassing telecommunications infrastructure, tapping straight into radio frequencies that pass data to nearby devices. From there, the data travels – hop by hop – until it can reach its destination or an open network, allowing information from impacted regions to reach the world.

During the 2019 pro-democracy demonstrations in Hong Kong, downloads of mesh-networking apps spiked, reaching several hundred thousand per day,<sup>44</sup> while in the immediate aftermath of the 2021 coup in Myanmar, a single mesh-networking app was downloaded over 1 million times.

<sup>45</sup>

<sup>44</sup>Leo Schwartz, “The World’s Protest App of Choice,” Rest of World, August 10, 2020, <https://restofworld.org/2020/the-worlds-protest-app-of-choice/>.

<sup>45</sup>Fanny Potkin and Jessica Pang, “Offline Message App Downloaded over Million Times after Myanmar Coup,” *Reuters*, February 2, 2021, <https://www.reuters.com/article/us-myanmar-politics-bridgefy-idUSKBN2A22H0>.



## Virtual Private Networks (VPNs)

VPNs are one of the most effective tools to circumvent partial shutdowns.

By connecting users directly to a remote access point – most often in countries without restrictive censorship policies – before routing traffic on to other services, they allow users to bypass targeted blocking imposed in their area, and conceal their internet use from their local ISP. VPNs achieve this through a process known as tunneling, encrypting the communication between a device and a remote service as it passes back and forth between the VPN provider. While an ISP or others snooping on a network can see that the user is connected to a VPN, all other information about their web use is concealed.

Many VPNs are also configured to use DNS servers provided by the VPN provider themselves, effectively thwarting attempts at DNS tampering that might otherwise connect individuals to insecure servers.

As VPNs must route traffic through another server – one often distant from both the origin and destination of internet traffic – they can, however, introduce substantial lags, reducing their usefulness on slow connections. Different VPN providers also offer varying levels of privacy protection, and all traffic can further be exposed to the provider itself. Some countries have further introduced legislation restricting how and whether VPNs can be used.

Although VPNs are legally restricted in some countries, their use around the world is growing rapidly.<sup>46</sup> Following the internet shutdown on August 9, 2020, that accompanied Belarus' national elections, the number of users of a single VPN service in the country jumped from 10,000 to over 1 million in a single day.<sup>47</sup>

## Proxy Servers

Proxy servers function similarly to VPNs, but work at the application rather than the operating system level. Most commonly implemented as a specialized web browser, these applications reroute connections to a remote server through a secure tunnel before passing it on to its destination. Traffic originating from other applications on the same device, however, travels through the user's ISP as normal, leaving it susceptible to blocking.

Tor, originally developed by researchers at US Defence Department's DARPA as The Onion Routing project, takes the standard proxying process one step further.

<sup>46</sup> Rae Hodge, "VPN Use Surges during the Coronavirus Lockdown, but so Do Security Risks," CNET, April 23, 2020, <https://www.cnet.com/news/vpn-use-surges-during-the-coronavirus-lockdown-but-so-do-security-risks/>.

<sup>47</sup> Mikhail Bushuev and Martin Kuebler, "In Belarus, Privacy Apps Help Resist Internet Shutdown," DeutscheWelle, August 17, 2020, <https://www.dw.com/en/in-belarus-privacy-apps-help-resist-internet-shutdown/a-54560843>.



Data sent through the Tor browser is encrypted multiple times, each time receiving a new destination IP address, before leaving a device. That data then bounces across the Tor routers where, one by one, the layers of encryption are peeled back until the fully decrypted data can be forwarded on to its final destination. This structure reduces the risk of any one proxy server being compromised and revealing the contents of web-based communication.

Some websites, including BBC News, are also mirrored directly within the Tor Network, providing greater defense against disruption.<sup>48</sup>

The Tor Network, however, is blocked in a number of countries and its use may be restricted.

Beyond the spread of tools and services individuals can use to circumvent shutdowns, the underlying technologies of the internet itself are also evolving through the emergence of new standards and protocols, including encrypted DNS and Encrypted Client Hello (ECH), to provide greater privacy and security to individuals on the web, simultaneously limiting the tactics that can be used to shut it down.

## *Prevent*

In the last decade, internet shutdowns have gone from virtually unheard of to an everyday occurrence around the world. To curb this trend, and the havoc it wreaks on individuals and communities, multilateral organizations and popular movements must together play a central role in the fight to keep the internet open and free for all.

The United Nations Human Rights Council has escalated its commitment to ending internet shutdowns in recent months, requesting a full report on the trend by the Office of the High Commissioner for Human Rights in July 2021. The Special Rapporteur on the Freedoms of Peaceful Assembly and Association has further called on, “States, international institutions, businesses, and other stakeholders to commit themselves to end internet shutdowns.”<sup>49</sup>

## **#KeepItOn**

At the grassroots level, [#KeepItOn](#), a global coalition of more than 240 organizations from 105 countries, has been fighting internet shutdowns through a range of creative approaches since 2016. The coalition has engaged in grassroots advocacy, direct policy-maker engagement, technical support, and legal intervention, to end shutdowns and prevent them from taking place in the future.

<sup>48</sup> “BBC Launches Tor Mirror Site To Thwart Media Censorship,” NPR.org, October 24, 2019, <https://www.npr.org/2019/10/24/773060596/bbc-launches-tor-mirror-site-to-thwart-media-censorship>.

<sup>49</sup> United Nations, Human Rights Council, Ending Internet shutdowns: a path forward, A/HRC/47/24/Add.2 (15 June 2021), available from <https://undocs.org/A/HRC/47/24/Add.2>.



## Legal Action

In the last year, legal action against shutdowns, supported by coalitions including #KeepItOn, has emerged as one of the most effective tools to curtail the use of internet blackouts.

A 2020 decision by the [Economic Community of West African States \(ECOWAS\)](#) Community Court of Justice, a body that holds jurisdiction over 15 states in West Africa, held that a 2017 internet shutdown in Togo violated human rights, and ordered the government to pay restitution and keep the internet on in the future.<sup>50</sup> Lawsuits over the last four years have further restored at least some degree of connectivity from Cameroon to Sudan to Kashmir.<sup>51, 52, 53</sup> Even where suits have formally failed, they've provided vital transparency on the origins, duration, and impact of shutdowns.

The relatively predictable nature of internet shutdowns – inevitably deployed during elections, or moments of civic unrest – provides further opportunity to head off this threat before it emerges.

“We’ve been working hard to get ahead of the game, and challenge shutdowns before they even take place, rather than picking up the pieces once the damage has been done,” says Access Now’s Felicia Anthonio. “The #KeepItOn coalition is starting to find real success identifying regions at risk of shutdowns, and working with communities to build capacity and bring pressure to bear before the government cuts access or blocks communications platforms.”

The use of internet shutdowns is accelerating at an astonishing pace, plunging ever greater numbers into darkness and threatening to break the promise of a borderless internet. But these recent successes offer more than a glimmer of hope. As global partnerships come together to force this threat into the light, and new technologies develop to keep communities connected, momentum continues to build to secure the future of a free and open internet.

---

<sup>50</sup> Felicia Anthonio et al., “ECOWAS Court Upholds Digital Rights, Rules 2017 Internet Shutdowns in Togo Illegal,” *Access Now* (blog), June 25, 2020, <https://www.accessnow.org/internet-shutdowns-in-togo-illegal/>.

<sup>51</sup> Media Defence, “Media Defence and Veritas Law Bring Case Before the Constitutional Council of Cameroon Challenging Internet Shutdown,” *Media Defence* (blog), May 4, 2017, <https://www.mediadefence.org/news/mldi-and-veritas-law-bring-case-before-the-constitutional-council-of-cameroon-challenging-internet-shutdown/>.

<sup>52</sup> Reuters Staff, “Some Internet Service Restored in Sudan after Court Ruling,” *Reuters*, July 9, 2019, <https://www.reuters.com/article/us-sudan-politics-internet-idUSKCN1U41PN>.

<sup>53</sup> Swati Bhasin, “2G Mobile Internet Services Restored In Parts Of Jammu And Kashmir,” *NDTV.Com*, May 12, 2020, <https://www.ndtv.com/india-news/2g-mobile-internet-services-restored-in-parts-of-jammu-and-kashmir-2227514>.



## **About Jigsaw**

[Jigsaw](#) is a unit within Google that forecasts and confronts emerging threats. The unit conducts pioneering research and demonstrates the power of emerging technology to keep our world safer. Jigsaw collaborates with both external and internal partners—including academic and civic organizations – to build and scale research and technology. Among the current focus areas are disinformation, online toxicity and harassment, violent extremism, and free expression.

## ***The Current***

[The Current](#) is Jigsaw’s online publication. It outlines today’s digital threats and solutions, and offers an accessible, interactive channel for Jigsaw research. Issues so far have explored disinformation, violent white supremacy, and toxicity online.