ZAINA FOUNDATION

SIMPLIFIED GUIDE ON INTERNET SHUTDOWN

ABOUT THE AUTHOR

Zaina Foundation is a private, autonomous, voluntary, non-governmental, non-profit sharing organization which was founded in 2017 and registered under NGO's Act of 2002 with the aim of promoting digital rights and Inclusion in Tanzania.
Our vision is to Promote Digital Rights and inclusion in Tanzania through advocacy on affordability and accessibility of internet, digital safety and privacy capacity building, policy reform workshops and convene and mission is to continuously aid women who are Journalists, Human Rights Defenders, Technologists, Lawyers, Activists, women with disabilities and Students alike, to permanently improve the way they protect and access their information online. Please read more about us at www.zainafoundationta.org

Send your feedback about this guide to info@zainafoundationtz.org

ABOUT THIS GUIDE

This is the Proactive simplified internet Shutdown guide for Human Rights Defenders in Sub Saharan Africa. The Internet is the key infrastructure in democracy. Access to the internet and other technological communication tools is vital during this period of human rights in the digital era.

This guide dive in details on Introduction to Internet Shutdown, Network Measurement and Circumventing Internet Shutdown. The aim of this guide is to help the human rights defender to predict, prepare, prevent and respond to internet shutdown in Sub Saharan Africa.

Developed by Zaina Foundation Tanzania and supported by Access Now.

TABLE OF CONTENT

1. Introduction to Internet Shutdown

1.1 Introduction

An internet shutdown can be defined as an "intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information." They include blocks of social media platforms, and are also referred to as "blackouts," "kill switches," or "network disruptions." Internet blackouts can occur at a localized or even national level, where an entire country has its telecommunications cut off.

Shutdowns are becoming more common every year. In 2015, only 15 shutdowns were documented. This number rose to 56 in 2016. In India alone, Human Rights Watch reported 20 shutdowns in 2017. However, www.internetshutdowns.in documented 41 shutdowns for the same period. By late June 2019, 26 of 54 sovereign states in Africa had deliberately disrupted digital communication services or the Internet, one of several practices that governments use to interrupt citizens' access to information, including social media taxes, website takedowns, and punitive actions against bloggers. Globally, more than 450 confirmed shutdowns had been recorded in approximately 50 countries (Access Now, 2020).

Notably, in a variety of cases, governments never publicly acknowledge that they are responsible for a shutdown. Out of the more than 200 incidents of shutdowns reported in 2018, only 77 were acknowledged by the government or entities that ordered the shutdowns. Many governments shut down the internet as a response to violence related to the spread of misinformation and disinformation. In 2018, Ethiopia, India, Nigeria, and Sri Lanka imposed internet shutdowns, citing as the rationale the spread of information on social media believed to incite communal violence. Out of 35 such cases in 2018, authorities in India were responsible for cutting access to the internet 31 times in attempts to stop communal violence. In this category of shutdown, there are notable cases in Sri Lanka and India. (KeepItOn Report, 2018).

In 2018 Access Now (non-profit founded in 2009 with a mission to defend and extend the digital civil rights of people around the world) document on its #KeepItOn Report identifies the key trends that define shutdowns and show the nature and official rationales for shutdowns in the year. Perpetrators of internet shutdowns historically use similar justifications for ordering shutdowns, but these justifications rarely match what observers can conclude is the real motivation. In the 2018 report, the official rationales have included combating "fake news" (properly called disinformation and misinformation), hate speech, and related violence, securing public safety and national security, precautionary measures, and preventing cheating during exams, among others.

1. Internet Shutdown
2.1 Impact of Internet Shutdown

Whether they are ordered in Ethiopia, Chad, Venezuela, India, or Tanzania, and whether they are justified as a measure to fight "fake news" and hate speech or to stop cheating during exams, the facts remain the same. Internet shutdowns:

1) Violate human rights
2) Put people in danger
3) Harm the economy
4) Curtail freedom of expression
5) Cut access to information
6) Inhibits people from assembling and associating peacefully, online and offline.

In addition during shutdowns, many victims are unable to reach their families, get accurate information to stay safe, or reach emergency services. Shutdowns disrupt businesses, schools, and ordinary lives, often exacting a significant financial cost

Nations and other intergovernmental bodies have passed a series of important resolutions to condemn shutdowns and caution states against imposing them.

2.3 Who Orders Internet Shutdown?

Shutdowns are ordered under a variety of state structures. Typically, the orders come from authorities in local governments, state/ regional governments, the judiciary, and executive bodies of governments. The entity that orders a shutdown can impact the scope and effect of the shutdown. The geographic reach of a shutdown could extend beyond a country's borders, or be as localized as a few cellular towers on a protest route. Some countries have legislation that facilitates and legitimizes shutdowns, while others issue arbitrary orders that are not necessarily grounded in or supported by law. In many African countries that shut down the internet, the shutdown orders come from the helm of power Of the 21 countries that shut down the internet in the African continent, it is only in Nigeria's Jos North and Jos South that the local government was responsible for ordering shutdowns; elsewhere, these orders were issued via the executive or by central governments. With the exception of Ethiopia, the African countries that suspended the internet in 2018 typically have an authority that regulates the telecommunications sector, yet in many cases the communications regulator did not make an official statement about the shutdowns or provide a justification. Algeria, which shut down the internet in 2018 for school exams, was the only country that gave any notice before imposing a shutdown, and the only one to give clear information about when, why, and for how long the internet would be cut off.

2.4 State of Internet shutdown around the world

Observation can reveal more information for determining the impetus for internet shutdowns, in 2018: they took place in response to protests, militant or terrorist activity (mostly in the Kashmir region in India), elections, during communal violence, to assert information control (including during periods of political instability), on religious holidays and anniversaries, and during school exams. In 2020 Tanzania experienced internet shutdown for more than two weeks during the General election, and in 2021 India experienced internet shutdown 106 times due to several reasons like exams.

It is rare for government justifications to match the cause of shutdowns as reported by the media, civil society organizations, and activists. When they do, they use umbrella terms to justify shutdowns despite details and nuances of what actually happened. When governments shut down the internet, whether through a memo, directive, or just a phone call, authorities will sometimes provide the public with some form of public rationale or justification. The most common justifications cited in 2018, as shown below: public safety, "fake news" (which as we have noted, is properly called disinformation or misinformation) or hate speech and related violence, national security, and school exams.

When governments shut down the internet citing "public safety," it is often evident to observers that, in reality, authorities may fear protests and cut off access to the internet to limit people's ability to organize and express themselves, whether online or offline. The data reveal that when authorities cite "fake news," rumors, or hate speech, they are often responding to a range of issues including protests, elections, communal violence, and militant activity, among others. Using these threats as scapegoats, it appears that governments are leveraging shutdowns to shape the political narrative and control the flow of information.

2.5 Anatomy of Shutdowns

1. Bandwidth Throttling

Bandwidth throttling is the intentional slowing of an internet service or a type of internet traffic by an internet service provider (ISP). It is employed by ISPs to regulate network traffic and ease bandwidth congestion. When one's internet bandwidth is throttled, it results in poor performance of web content or service for the user. Out of the more than 196 internet shutdowns documented in 2018, about 22 were bandwidth throttling. Bangladesh, Cameroon, Chad, India, Kazakhstan, Togo, and Yemen are perpetrators of bandwidth throttling.

2. Broadband Internet Shutdowns

These are cuts to internet access via broadband, such as in a home, office, or business, and are accompanied by mobile internet shutdowns. In 2021 internet shutdown appeared 182 times across 34 countries in Africa. No country shut down access via broadband without also cutting off access to mobile device networks. The spread of cheap smartphones has made mobile internet and networks ubiquitous across many countries and regions, and in the majority of the countries where people experience internet disruptions, they are connecting using smartphones. Therefore, it often has more impact to shut down mobile internet than broadband internet.

3. Mobile Internet Shutdowns

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

4."Internet blackouts" or Blanket Internet Shutdowns

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

5. Mobile phone call and text message network shutdowns

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

6. Service-specific (platform) shutdowns

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

2 Internet Measurement

3.1 Internet Measuring Network Tools

1. Active measurement

It is based on the concept of sending probe packets into the network and measuring their behavior as they flow through it. The probe packets are typically emitted from a general-purpose end –host such as a personal computer which is sent toward a destination host by providing a target IP address (or domain name) to the measurement tool. The injection of probe packets into the network provides an indication of the routing behavior, propagation delay, queuing delay, and loss that would be experienced by normal data packets. When and if the probes arrive at a destination, either their arrival is logged or response packets are returned to the sender. Active probing can also be done by approximating the behavior of typical applications, such as sending a request for a web page.

2. Passive measurement

It is observing normal network traffic, so they do not perturb the network. They are commonly used to measure traffic flows, i.e. counting the number of packets and bytes traveling through routers or links between specified sources and destinations.

3. Web Access logs

Logging access activity is a standard feature in web server software that is usually enabled by content providers. Log entries contain the time at which a particular web file was requested, the IP address of the requested, the name and size of the requested file and status code returned to the requester. The content being requested and sources of requests.

4. Packet-trace Collection

Packet traces can be a summarization of traffic (IP flow measurements) or the details of individual packets on a given link. Such measurements require access to a network device (such as a router, switch, or link splitter) or access to a broadcast local area network.

A standard tool for logging individual packets is "tcpdump", which uses packet filters to capture selected packet activity from the network interface. A typical log entry from tcpdump consists of a time stamp, the source/ destination IP/ port numbers, the transport protocol name, details from the packet header, and details of the packet payload. Collection of this information, especially the packet payload itself, provides valuable insights into network use.

5. Simple network management protocol (SNM)

Is an important component in the daily operation of large-scale networks which protocol used by network management systems to communicate with network elements such as routers and switches.

SNMP enables network management systems both to query network elements for data and to send data to network elements that are maintained and available from network elements through the SNMP are specified by a Management Information Base (MIB) and the data set is gathered passively by network elements.

Most of the items in the MIB data set are simple activity counters, such as the number of packets transferred on a specific link. One of the main uses of SNMP MIB data is to ensure that a network is performing within acceptable operational limits. Management systems are configured to provide multiple "views" into the network based on its topological configuration, which enables network managers to assess in nearly real time the state of their systems.

3 How to Document Internet Shutdowns

4.1 Preparing before the shutdowns

Despite an internet shutdown, documenters can still capture important video evidence that can be share d offline or when they are able to get back online.
Shutdowns often coincide with heightened information control and restrictions on freedom of expression and assembly. If you are a documenter, you must take extra precautions to protect yourself and your information during these periods. If there is a risk that authorities will confiscate your phone, or compel you to unlock it and reveal the contents (during a shutdown or otherwise), consider using a separate phone for documenting than your primary personal one. This can help minimize what information you are carrying that can be compromised (e.g. your contacts, accounts, messages, etc). If you are unable to use another device, you can still follow this guide to reduce the amount of sensitive data and improve security on your primary phone. ie (wipe the phone, practice basic phone security, install useful documentation apps, install some everyday apps, keep real personal or private/ sensitive information off the device, use features for obscuring content, set up offline sharing and practice before you're in a crisis situation).

4.2 Capture

Many apps that documenters can use to capture video, ranging from your phone's native camera app, to more specialized document apps like ProofMode, Tella, or Eyewitness to Atrocities. Some apps have features that rely on internet access, and may not be available in the event of an internet shutdowns. Globally, internet shutdowns are on the rise. According to AccessNow's #KeepItOn campaign, there were 128 intentional shutdowns between January - July 2019, compared to 196 in all of 2018, and up sharply from 106 in 2017, and 75 in 2016. Around the world, governments, with the cooperation of telecom companies, are increasingly turning to internet shutdowns as a strategy to repress communities, prevent mobilization, and stop information about human rights violations from being documented and shared.

4.3 Maintaining Verifiable Media

In maintaining verifiable media during an internet shutdown the researcher could rely on first hand documentation filmed by witnesses to monitor, report, and address human rights violations. They can take steps to authenticate and verify the documentation they receive, a process that can be painstaking and time consuming. Simple way for documenter to verify and corroborate with documentation which are more verifiable during an internet shutdown.

1) Consider encrypting the file
2) Add Description/ metadata
3) Keep backup separate location
4) Use an OTG or wireless drive
5) Use password to protect the drive

4.4 Sharing and Communicating

Internet shutdowns are designed to block people from sharing information and communicating and also push people into less secure forms of communication such as mobile phones and SMS, which are easier for authorities to intercept and monitor.

These are ways of sharing and communicating during shutdowns;

1) Sharing file directly with bluetooth, wifi direct, or NFC
2) Sharing files with a wireless drive or via a wireless local network
3) Communicating via peer - to - peer chart
4) Communicating via encrypted SMS
5) Use of VPN
6) Communicating via DNS servers

4 Circumvention During Shutdowns

5.1 Circumventing shutdowns

Much effort has been done so far by human rights organizations and activists in circumventing shutdowns. Different organizations have been established with the mission to defend and extend the digital rights of people around the world. They provide technical support, advocacy awareness, training, and run different annual conferences on Human Rights.

#KeepItOn coalition works to provide and disseminate customized circumvention tips when a government orders, or is likely to order, a shutdown. Monitoring and verifying internet shutdowns is essential for documenting them and pushing back. There are a number of groups in the #KeepItOn coalition that continuously monitors internet traffic, testing for blocking, throttling, and blackouts, so that these attacks on human rights do not go unopposed anywhere around the world. They include;

- Oracle's Dyn Internet Intelligence Map,
- Internet Outage Detection and Analysis (IODA),
- The Open Observatory of Network Interference (OONI),
- NetBlocks.

These and other groups are doing enormously valuable work collecting technical evidence and shedding light on the nature of internet shutdowns, strengthening the effort to stop them. For example, NetBlocks worked to document throttling and social media shutdowns in Chad, which bolstered the legal challenge that provided more transparency to how they're carried out. Similarly, #KeepItOn coalition have used the measurement community's evidence to submit reports to the United Nations and other intergovernmental processes helping #KeepItOn coalition hold states accountable.

5.1.1 Measuring and Monitoring Tools

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

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

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

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

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

6) Internetshutdowns.in - an online tool by Software Freedom Law Center, India to monitor internet shutdowns in India with a reporting platform.

7) Kill Switch in Pakistan - bytes for All's active monitor of internet shutdowns in Pakistan

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

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

5.1.2 Practical Session Tools

- Open Observatory of Network Interference (OONI)
- ToR Browser
- Psiphon VPN

Activity: Instal, configure and test.

5.2 Circumvention Tools

i. Simple web proxies

Are server-side applications which are accessed through web page forms. To use one of these tools, the user simply visits a web page that includes a url input box. Instead of entering a web page url into the browser address bar, the user enters the address into the web page form by submitting this web page form, the user sends the url request to the proxy web server, and the web server returns the page via the proxy. Simple web proxies do not require the user to download or install any client-side application.

Users need only visit the web page hosting the proxying web application (for instance http://superproxy.com). But simple web proxies do require that users navigate the separate, form-based browsing interface, rather than using the address box on their web browser to enter destination site names. Almost all simple web proxies support themselves by hosting ads. Ads are generally hosted on an initial landing page and are often inserted into proxied web pages.

ii. Virtual Private Network (VPN)

Are services use software that implements a networking protocol to encrypt and tunnel all Internet traffic through a proxy machine. VPN technology has traditionally been used to allow corporate and other institutional users to access internal networks from the public Internet, but in the past few years there has been tremendous growth in the availability of personal VPN services. Among other uses, these personal VPN services act as circumvention tools as long as the VPN proxy is hosted outside a filtering country. VPN services might or might not require installation of client-side software and allow the user to access the web directly through the native browser interface (many rely on existing VPN support in Windows or Mac OSX and so need no extra client software). Because VPN services tunnel all Internet traffic, they can be used for email, chat, and any other Internet service in addition to web browsing. Almost all VPN tools support themselves through fees charged directly to users (charges of $10 to $30 per month are common), though a few also offer free services with restricted bandwidth.

iii. HTTP/SOCKS proxies

Are application level proxies that funnel network traffic through protocols designed to allow web traffic to pass through firewalls. Users generally find lists of these proxies in the form of IP addresses and port numbers on proxy directory web sites. To use a given HTTP or SOCKS proxy, the user enters the IP address and port number of the proxy into a configuration screen of the browser. As a result, no client-side application is needed. The user is able to use the native interface of the browser. These proxies are generally open to the public and have no readily identifiable source of funding (users do not pay to subscribe to them, and the owners of the proxies are anonymous so there is no way to know if they are receiving charitable or government funding).

These tools have no blocking resistance and can be challenging for novice users to use. While it is impossible to accurately estimate how widely these tools are used, we believe they are used less often than web proxies. No HTTP/SOCKS proxies were tested in this study. The rest of the tools tested, which we put in the custom tools category, are not as easily categorized.

5. References

» Cammaerts, B. and Mansell, R., 2020. Digital platform policy and regulation: Toward a radical democratic turn. International journal of communication, 14, p.20.

» https://www.accessnow.org/internet-shutdowns-2020-elections/

» Rydzak, J., Karanja, M. and Opiyo, N., 2020. Internet Shutdowns in Africal Dissent Does Not Die in Darkness: Network Shutdowns and Collective Action in African Countries. International Journal of Communication, 14, p.24.

» Gollatz, Kirsten; Beer, Felix; Katzenbach, Christian (2018). The Turn to Artificial Intelligence in Governing Communication Online

» West, D. Internet shutdowns cost countries $2.4 billion last year, Brookings, 2016. Available at:
https://www.brookings.edu/wpcontent/uploads/2016/10/intenet-shutdowns-v-3.pdf

» #Keepiton, Access Now, 2019, https://www.accessnow.org/keepiton/

» GSMA. (2018) 2018 Mobile Industry Impact Report: Sustainable Development Goals. Available at: https://www.gsmaintelligence.com/
research/?file=ecf0a523bfb1c9841147a335cac9f6a7&download

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

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

» Q.Chen, H. Chang, R. Govindan, S. Jamin, S. Shenker, and W.Willinger. 2002. "The Origin of Power Laws in Internet Topologies Revisited," in Proceedings of IEEE Infocom 2002, June. New York, N.Y.

» W.Stevens. 1994. TCP/IP Illustrated, Vol. 1: The protocols. Addison - Wesley, Boston.

» Yvonne Ng.
https://blog.witness.org/2020/02/documenting-during-internet-shutdowns/

» H. Roberts, E. Zuckerman, J. York, R. Faris, and J. Palfrey, "2010 Circumvention Tool Usage Report, Berkman Center for Internet & Society, 2010,
http://cyber.law.harvard.edu/publications/2010/Circumvention_Tool_Usage.

» E. Zuckerman, H. Roberts, R. McGrady, J. York, and J. Palfrey, "Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites," Berkman Center for Internet & Society, 2010,
http://cyber.law.harvard.edu/publications/2010/DDoS_Independent_Media_Human_Righ

»https://paradigmhq.org/wp-content/uploads/2021/04/Ayeta%20Toolkit%20-%20English%20Version.pdf

ZAINA
FOUNDATION

CONTACT US

info@zainafoundationtz.org
www.zainafoundationtz.org

facebook.com/Zaina Foundation
twitter.com/@Zainafoundation

P.O.Box 75757, Dar es Salaam
Hotline: +255 676 586 199