INTERNET SHUTDOWNS AND ELECTIONS HANDBOOK

A guide for election observers, embassies, activists, and journalists

#KeepItOn

#KeepItOn

This handbook explains how internet shutdowns undermine democractic elections and provides tips and recommendations for key actors to navigate shutdowns and understand and assess the extent to which an election taking place under a shutdown is free and fair. It is aimed at election observers, people on diplomatic missions, journalists, and human rights activists in particular.

This handbook is a publication of Access Now for the #KeepItOn coalition and was written by Afef Abrougui in collaboration with the Access Now team.

Last update: April 2021

Table of contents

I. The facts on internet shutdowns

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. There are different types of shutdowns (see Glossary for definitions). During blanket shutdowns, or total internet blackouts, access to the internet or all telecommunication services is completely cut, usually by a government actor. In contrast, partial shutdowns target specific types of networks (for example, mobile networks) or services such as social media and messaging apps. An internet shutdown can also take the form of throttling, when internet speeds are intentionally slowed down for the purpose of making it harder — or even impossible — for people to upload, download, or access information. One of the tactics commonly used by governments is downgrading mobile internet speeds from 4G and 3G levels to 2G.

Shutdowns can be imposed nationwide or they can be targeted to a specific neighborhood, village, region, or province. Targeted shutdowns can be more difficult to detect and verify, particularly in remote regions and areas that are isolated from the outside world, such as conflict zones that may not be accessible to journalists and human rights defenders due to safety reasons or government-imposed restrictions.

Governments claim that they impose shutdowns for a number of reasons including to protect national security and restore public order, to prevent cheating in school exams, and to hinder the spread of hateful speech and mis- and disinformation. However, the circumstances under which shutdowns are usually ordered reveal that governments actually deploy them as a tactic to restrict citizens' rights to freedom of expression and information, and to interfere with the right to freedom of assembly and association, particularly during events such as elections, conflict, or mass demonstrations.

Between 2018 and 2020, Access Now and the #KeepItOn coalition documented **at least 564 shutdowns around the world**. Most of the shutdowns took place in Africa, Asia-Pacific, and the Middle East and North Africa. These figures, however, may not be comprehensive. Given Access Now's **methodology** for counting shutdowns, which relies on technical measurement as well as contextual information such as news reports or personal accounts, there may be cases of internet shutdowns that have gone unnoticed or unreported.

II. How internet shutdowns harm human rights

Disrupting access to the internet hinders the full enjoyment of a wide range of fundamental rights and freedoms, particularly the right to freedom of expression and opinion, access to information, and freedom of assembly and association. Above all, these restrictions **affect ordinary lives** by preventing people from communicating, harming businesses, and disrupting education and access to online services and opportunities. In times of crisis — such as during armed conflict or a global pandemic — shutdowns endanger public health and safety, as people are unable to get essential information about what's happening around them, reach emergency services, or communicate with and protect their loved ones. Internet shutdowns are inherently disproportionate measures that are not justified under international human rights law.

As early as 2011, the United Nations (U.N.) Special Rapporteur on freedom of opinion and expression, the Organization for Security and Co-operation in Europe (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 were already condemning shutdowns. They issued

a joint declaration stating that cutting off access to the internet "can never be justified, including on public order or national security grounds."

A 2016 U.N. resolution on the promotion, protection and enjoyment of human rights on the Internet also condemns internet shutdowns, and urges states to refrain from ordering them. This resolution was further maintained in 2018. In 2016, the ACHPR passed a resolution condemning government-ordered shutdowns during elections or protests. In a 2019 Human Rights Council report on freedom of peaceful assembly and association in the digital age, the Special Rapporteur on the rights to freedom of peaceful assembly and association said that "network shutdowns are a clear violation of international law and cannot be justified in any circumstances." While in its General Comment no. 37 (2020) on the right of peaceful assembly, the Human Rights Committee called on state parties to the International Covenant on Civic and Political Rights not to "block or hinder Internet connectivity in relation to peaceful assemblies."

III. Why internet shutdowns are a barrier to democratic elections

Internet shutdowns are a reflection of a general atmosphere of political repression, censorship, human rights violations, weak institutions, or lack of rule of law. During electoral periods, internet access in itself does not address all of the deeper institutional and political factors that interfere with the conduct of free and fair elections, but its disruption makes it harder for different actors to fully engage in the electoral process. Shutdowns undermine the capabilities of election candidates — particularly the opposition — to campaign and exchange ideas. They also prevent voters from accessing information, weaken trust in the electoral process, and obstruct the efforts of those documenting irregularities.

Internet shutdowns violate human rights and democratic freedoms

Human rights, including the rights to freedom of expression and access to information, as well as press freedom, are essential to democratic elections.

As noted in a 2014 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "providing the conditions for free and open political communication is an essential element of ensuring fair and democratic electoral processes." The same report denounced measures restricting freedom of expression in electoral processes online and offline as "especially damaging."

Candidates and political parties competing in elections should be able to organize, assemble, express their thoughts, and freely communicate their electoral programs. Voters, meanwhile, should be able to access information, attend and participate in political rallies and campaigns, make informed decisions, and otherwise freely engage in democratic discourse and the electoral process. The media's role is essential in ensuring equal access to all political parties and candidates to present their political platform and views on issues of utmost importance to voters, scrutinizing candidates and any attempts to interfere with the electoral process, and fact-checking misinformation and disinformation, which can be rife during electoral periods.

Whether they take place before, during, or after an election, internet shutdowns prevent different actors from fully participating in the electoral process and hinder voters from accessing information, engaging in debate, and freely expressing their political affiliations. Shutdowns further make it harder for the media to report and keep the public informed, undermining the capacity of political parties and candidates to campaign and mobilize voters.

Internet shutdowns undermine media access and election fairness

In electoral periods, governments that impose internet shutdowns also deploy other tactics to silence their political opponents, such as through their control over the media and restrictions on electoral campaigning and political gatherings. This gives ruling parties and candidates with close ties to the government an advantage over their competitors, particularly independent candidates and opposition parties. For example, in the absence of an unhindered and reliable access to the internet, opposition candidates may be left with limited options to campaign and attract voters and unable to compete on equal footing with powerful political players who control mainstream media. *This is discriminatory and a violation of equal access to the media, one of the key criteria for democratic elections*.

Furthermore, internet shutdowns imposed following a contested election undermine the capabilities of the losing party — usually the opposition — from organizing to challenge the results. In contexts of political repression and media censorship, organizing protests and campaigns through the internet is one of few — if not the only — tactics available to the opposition and voters to exercise pressure on the authorities. Therefore, disrupting access to the internet only further tips the scales in favor of the winning party, which further exacerbates distrust and suspicion of election rigging and fraud.

Internet shutdowns interfere with the media's watchdog role

Internet shutdowns prevent the media from properly keeping the public informed during the different stages of the electoral process. The media's role in elections is essential in reporting on political campaigns, informing the public about the candidates and political agendas to help voters make informed choices, fact-checking the statements made by political candidates, and investigating and exposing any election rigging.

Shutdowns indicate a general atmosphere of mounting political repression, censorship, and human rights abuses. This makes the role of the media even more essential. Yet disruptions to the internet make it harder for journalists and the media to do their work at a time when credible information is most needed.

Without unhindered access to the internet, media organizations and journalists are unable to properly play the role of a watchdog to ensure the integrity and transparency of the electoral process.

Journalists are unable to file breaking news stories on time, reach out to their newsrooms, access information, and contact sources. While total internet blackouts are the most extreme form of internet shutdowns, restrictions on the use of social media and messaging apps also present a great hindrance as these tools have become essential for journalists and the media to reach out to audiences, disseminate and promote their work, and communicate securely with their sources.

Internet shutdowns weaken the public's trust in the electoral process

Elections are more than just about voting and what happens on election day. Trust in the whole process, including activities that take place before and after election day, is essential, particularly in contexts where lack of trust in the election results can lead to acts of violence.

According to a **2013 Report** of the U.N. Secretary-General to the General Assembly, "it is not enough that an electoral process produces an accurate outcome. Citizens must have trust that this outcome does indeed reflect their will." The report further noted that "credibility does not rise out of the polling process itself, or indeed one single event. The sources of political trust and acceptance lie deeper."

Building electoral trust is thus contingent on a number of factors that reflect the broader atmosphere in which elections are held, such

as a level playing field, neutrality of the electoral authorities and the government vis-à-vis all contenders, respect for human rights and the rule of law, inclusiveness, and transparency.

Shutdowns place the legitimacy of the electoral process into question. They obstruct the free flow of information and expression, which is necessary to build public trust and facilitate transparent and fair elections.

In addition, since government-imposed shutdowns are often used as a tactic to silence and deprive the political opposition of an essential tool to campaign and mobilize voters, these measures further erode public confidence in the neutrality of state institutions vis-à-vis all political contenders.

Internet shutdowns challenge election transparency, integrity, and accountability

Internet shutdowns prevent independent actors working to ensure the transparency, integrity, and fairness of elections — such as international observation missions, non-partisan domestic observers, and activists — from monitoring the conduct of elections and exposing any irregularities.

During an election, finding and communicating essential information, such as reports of irregularities, problems with e-voting systems, and violence, is made more difficult under a shutdown. Shutdowns hinder observers' ability to coordinate with the headquarters of their missions, other observers, and electoral authorities, as well as preventing them from verifying the accuracy of information they receive.

Disrupting access to the internet prior to an election makes it harder for observers to access information that may help them better prepare, take any safety precautions, and monitor different aspects of the pre-electoral phase, such as campaigning and voter registration. The internet also helps voters, citizen journalists, and activists document and disseminate reports and footage of rigging, fraud, and acts of election-related violence when they occur.

Unhindered access to the internet is equally important as the counting of votes begins. Its disruption prevents observation missions and those documenting irregularities from wide and timely dissemination of their statements, reports, findings, and conclusions to the public.

In an election period, timely dissemination of information about irregularities is important to help ensure that fraud is addressed and investigated and that legal challenges are submitted within the timeframes set by a county's laws. When irregularities do not come to light, there is less chance of addressing them, learning from them to improve upcoming election cycles, and most importantly, holding to account those responsible for violations.

IV. How to navigate a shutdown: tips and recommendations

1. Understand the digital rights context

Read news and articles about past or ongoing internet shutdowns and their connection to elections.

Keeping yourself informed can help you better prepare in case a shutdown takes place during an election period. Understanding the role technology and the internet play in different aspects of the electoral process, for example in election campaigning, voting, and voter registration, can help you better assess how shutdowns in a particular context and country interfere with the electoral process. It is also essential to investigate the history of internet shutdowns and other tactics for limiting the free flow of information that have been used in the country

or affected region in the past. For example, you can reach out to digital rights groups and activists working locally for a better understanding of the digital rights situation, including groups that are part of the #KeepItOn coalition. You can also consult organizations that document and monitor internet shutdowns and censorship around the world, including Access Now, who maintains the **Shutdown Tracker Optimization Project (STOP)**, and network monitoring groups such as the **Open Observatory of Network Interference (OONI)**.

2. Prepare yourself before a shutdown happens

Install and use circumvention tools, such as browsers and tools based on Tor technology, Virtual Private Networks (VPNs), and proxies that utilize encryption.

VPNs create their own network that tunnels data through existing networks. A VPN can help you circumvent the blocking of websites or online platforms, including specific services such as social media platforms and instant messaging apps. To prevent people from accessing blocked websites and services, governments often resort to blocking access to VPN providers during a shutdown, making it difficult to install the tool once the block is in place. They also sometimes block traffic from popular VPN providers, rendering them ineffective. We recommend that you download several VPNs in advance if you are at risk of experiencing a shutdown. Not all VPNs can guarantee your privacy or offer you the same level of protection. When choosing a VPN provider, opt for open source tools with publicly accessible codes and transparency on how they protect your data. You should also ensure that the VPN is public about their peer security review process and that their security has been reviewed by independent auditors. If you need help with tool recommendations, you can contact Access Now's **Digital Security Helpline**.

In some countries, the use of circumvention tools and VPNs is illegal or subject to restrictions. Make sure to consider any legal and personal safety risks that may arise from your use of such tools. If certain circumvention tools are censored or criminalized in your country, you may want to explore setting up your own personal VPN server outside of the country, though this can also carry significant legal risks in some contexts, and is particularly criminalized in China.

Download and set up secure communication tools.

For secure communication, we recommend that you use applications and services that support end-to-end encryption. It is important to choose services and applications that are open source and undergo regular independent audits. For example, there are several open source instant messaging tools that use Signal Protocol — an end-to-end encryption protocol for messages and voice or video calls — including Signal and Wire. Read the guide provided by each tool carefully before you use them, as some patterns of use may put you or your contacts at risk. If you have additional questions about secure communication tools, get in touch with Access Now's **Digital Security Helpline**.

Keep in mind that using secure communication tools can entail personal and legal risks. Some countries have criminalized use of specific tools, and others are likely to surveil or monitor individuals actively seeking to keep their communications private. Make sure to be informed and to assess the risks before deciding which tools are best for you.

Understand and monitor ongoing internet shutdowns.

If you suspect an internet shutdown, you can consult monitoring tools such as the **OONI Explorer**, a worldwide database on internet censorship based on millions of network

measurements, **Internet Outage and Detection Analysis (IODA)**, and Google's **traffic and disruption tracker**, which provides near-real time data to identify internet outages on various networks. There are also country-specific shutdown trackers, such as **killswitch.pk** and **internetshutdowns.in**. You can measure internet shutdowns and censorship yourself using the **OONI Probe app**, which allows you to run tests and document evidence of various forms of network interference. OONI Probe test results are openly published on the OONI Explorer site in real-time. Before using OONI Probe, make sure you are aware of the **potential risks**.

These risks are primarily associated with testing for censorship, not internet shutdowns. Note that in some countries, censorship testing can lead authorities to identify and target you for surveillance or harassment. Take these factors into consideration as you look for information about whether a shutdown is taking place and how it's being implemented. Learning more can not only help you understand what is happening but also how to respond appropriately.

After an election is held, it is important to keep monitoring the situation, as there have been several cases of shutdowns starting after election day. Governments may impose shutdowns following an election to prevent the opposition and citizens from organizing to challenge the results, and in attempts to cover up election fraud and violence. In some cases, a shutdown may have been difficult to detect and more information may become available after the elections, for example when companies release their transparency reports.

If you're in an area affected by a total blackout, you will not be able to consult these resources online. However, they can be useful when a shutdown affects only the speed of networks or blocks specific services, platforms, and websites. We recommend you save or print this document in case you lose access to the internet.

3. Defend yourself and your community during a shutdown

Get the information out under an internet shutdown.

How you get information out to the world under a shutdown will depend on the type of disruption you are experiencing. Using a VPN can help you circumvent the blocking of specific services and websites, such as messaging apps, social media platforms, and email services. When governments resort to total internet blackouts, they are harder to circumvent. In a situation like this, consider tactics such as storing information, notes, and work on a thumb drive and sending it to someone traveling outside the area affected by a shutdown. For better security, you can opt for encrypting the drive or the files stored on it using software, such as **Veracrypt**.

If you are worried about authorities spying on your communications during an internet blackout, be wary of using a satellite connection. It is easy for authorities to monitor satellite communications, and in some countries even having a satellite handset is criminalized. In addition, using a satellite connection can give away your location, so you don't want to use it if your location should remain secret. This means that if you choose to use a satellite connection, you must carefully consider the type and sensitivity of the information you're sharing and the potential implications. For example, an election observer mission using satellite internet to publish and disseminate a public statement and the mission's findings will not face the same level of risk as a journalist communicating with an anonymous source blowing the whistle on election fraud. You can refer to **this guide the Committee to Protect Journalists created** for the 2021 elections in India for the most up-to-date challenges and relevant defense tips.

Communicate safely under an internet shutdown.

An internet shutdown — particularly a total blackout — can hinder your access to encrypted communication tools, and put you and others at risk. Before opting to use an insecure communication tool, make sure to assess the risks and potential consequences. It is important to consider who you are communicating with and any risks you may be exposing yourself and them to during these communications, think about whether you're exchanging any sensitive information, and determine whether it is better not to communicate until secure tools are available. For example, in the event of a total blackout, a journalist using a landline phone to interview a government official may face less risk than someone at a human rights organization who is using the same insecure, unencrypted phone networks to discuss evidence of election fraud or coordinate and communicate internally about their response to election violence. Amnesty International published **a guide outlining steps you can take** to communicate and document human rights violations during an internet shutdown.

Increasingly, people affected by internet shutdowns, researchers, and engineers have come up with creative ways to access and share information during total blackouts. These solutions include sneakernet, offline mesh communications, roaming subscriber identity module (SIM) from neighboring countries, and non-digital communications such as ham radio. They all carry different risks so it's important to properly assess which options are available and whether it is appropriate.

Document rights violations under an internet shutdown.

When communicating and getting information out to others during a shutdown becomes difficult or impossible, it's even more important to document what's happening on the ground, whether it is evidence of rigging and election fraud or human rights violations and violence. Even if you cannot share this evidence in real-time, it can later be used to inform the world of what happened during the shutdown and help people demand accountability. Documentation can take different formats, including videos, testimonies, photos, and written notes. Securing and storing this information is essential to make sure you do not lose it and avoid taking personal safety risks. If you're using your phone for documentation purposes, make sure to password-protect it and to set up screen lock and lock timer. You may also want to use a separate phone for documentation, as this minimizes the amount of personal information the authorities or other actors may be able to access if they seize your phone, such as the content of your messages, contacts, personal photos, etc. You should also consider encrypting your files and backing up your data. For detailed and practical tips, read **WITNESS' guides on documenting violations and rights abuses** during internet shutdowns, including how to **set up a phone for offline documentation** and **maintain verifiable media** during an internet shutdown.

Collecting and sharing evidence of human rights violations under internet shutdowns or censorship is often extremely difficult and puts you at great risk. Guides from WITNESS and Amnesty International mentioned above help you create an executable plan to ensure success in doing so. Make sure you download and read these guides, prepare your hardware, software, and contacts ahead of events of shutdowns, follow recommended protocols if a shutdown happens, and acquire necessary tools or apps to aid your plan.

V. Where to learn more, and how to take action

→ If you are aware of a potential internet shutdown ahead of an election or a shutdown during the election period, you can contact the #KeepItOn coalition and Access Now

at **shutdownalert@accessnow.org**. The **#KeepItOn 2021 Elections Watch** has a list of elections Access Now is watching in 2021 for possible shutdowns.

➔ If you are monitoring shutdowns and looking for a country's history of internet censorship and disruptions, the **OONI Explorer** has data on millions of network measurements collected from more than 200 countries. Access Now's STOP database also lists some incidents of internet shutdowns by year and by country from 2016.

➔ To learn more about the harms of internet shutdowns, check out the **#KeepItOn campaign website**, its **FAQ page**, and the **#KeepItOn report** on internet shutdowns recorded in 2020.

➔ If you are a journalist, member of civil society, or human rights defender who needs technical advice to get back online or secure your online communications during a shutdown, you can contact the **Access Now Digital Security Helpline (Helpline)**. We provide 24/7 assistance free of charge in nine languages.

➔ For digital security tips and guidance, check out the Helpline's **Anti-doxxing guide** and the **Guide to Safer Travel**. The Electronic Frontier Foundation has a comprehensive guide titled **Surveillance-Self Defense**. The guide includes tips on how to **communicate securely with others**, **preparing a security plan**, **choosing the right VPN** for you, and **circumventing internet censorship**.

Appendix: The language of internet shutdowns: a glossary of terms

2G, 3G, 4G, 5G refer to the different generations (hence the "G") of mobile broadband wireless communication technologies as opposed to first generation wireless mobile services (1G), which rely on analog radio technologies. Each generation offers faster speeds and has to meet higher quality standards. For example, a 2G internet speed offers a 250Kbps rate, while 3G and 4G mobile internet connections would normally render 3Mpbs and up to 100Mpbs, respectively.

A **blanket shutdown** or a **total blackout** is a disruption where internet access is cut entirely.

Encryption is the **process** of encoding information or communications in a way that can only be read by someone who can decipher or decrypt it back into a readable format. Information can be encrypted and decrypted using a piece of information called **encryption keys**. One way to encrypt one's communications is through **PGP**, which stands for **Pretty Good Privacy**, an email encryption system allowing users to exchange encrypted emails. Emails sent using PGP are converted into ciphertext on a user's device before they are sent over the internet. When in transit, third parties such as your government or your ISP cannot read the messages. Only the recipient can read them after decrypting the ciphertext using their encryption key.

End-to-end encryption is a **method** of communicating where only the sender and the receiver can access and read the messages or emails transmitted. End-to-end encryption is considered more secure than **Transport Layer Security (TLS)**, which only encrypts communications while in transit between a user's device and the servers of a company or service. With end-to-end encryption, no third parties can access or read those communications, not even the company.

An **internet shutdown** or an **internet blackout** 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.

Internet throttling is the practice of intentionally slowing down internet speeds, making it difficult or impossible for users to upload or download information. Throttling can also target specific services, applications, and platforms, rendering them unusable.

Landline connections refer to voice and data communications **transmitted** through physical cables, as opposed to wireless communications. They include, for example, fixed telephony and wired data services.

Metadata, often described as data about data, is information about the communications exchanged between a sender and a recipient, but not the content of the message. It includes information such as with whom you're communicating, dates and times of the communications, your location when conducting the communication, length of the conversations, and the subject line of an email. Metadata is **important**, because while it may not reveal the content of your conversations, it can still reveal a lot about you and your life.

A **Mobile network** or a **cellular network** is a **radio network** that enables users of mobile devices to send and receive wireless voice and data communications.

Network disruptions target specific or all telecommunication networks as opposed to particular services. For example, they can affect 3G or 4G mobile networks.

Open source is a type of computer software code whereby its authors make it available for others to use, study, redistribute, and modify. This makes the code available for everyone with the skills to inspect, including for any vulnerabilities, which can thus help enhance the security of a tool or app.

Partial shutdowns are disruptions that target specific services such as social media platforms and messaging apps or networks such as mobile networks.

Satellite internet is internet access provided by Internet Service Providers (ISPs) **using** communication satellites. It works when an ISP sends signals to a satellite in space, which are then sent back to Earth and captured by a user's satellite dish.

Sneakernet is an informal term for the transfer of electronic information by physically moving media such as magnetic tape, floppy disks, optical discs, USB flash drives, or external hard drives between computers, rather than transmitting it over a computer network.

About the #KeepItOn coalition

This handbook is a publication of Access Now for the #KeepItOn coalition and was written by Afef Abrougui in collaboration with the Access Now team.

The **#KeepItOn campaign**, coordinated by **Access Now**, unites and organizes the global effort to end internet shutdowns. The coalition comprises more than 240 member organizations from over 100 countries across the world, including research centers, human rights groups, press and media freedom organizations, and internet measurement monitoring groups. Since 2016, the coalition has made use of a range of tactics to fight shutdowns, including grassroots advocacy, direct policy-maker engagement, technical support, and legal intervention.

CONTACT

For more information, please reach out to Melody Patry at **melody@accessnow.org**.

INTERNET SHUTDOWNS AND ELECTIONS HANDBOOK

A guide for election observers, embassies, activists, and journalists

#KeepItOn