MITIGATING INTERNET SHUTDOWNS TOOLKIT
“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.”

United Nations, Universal Declaration of Human Rights
The Mitigating Internet Shutdown Toolkit was developed in response to the growing threat of internet shutdowns being used as a tactic by governments and other actors to stifle freedom of expression and deter internet access. This guide expands on the broader Cyber Security and Digital Surveillance knowledge resources developed by Internews South Africa, with the support of technical experts. The toolkit offers a practical in-depth guide on understanding and mitigating the impact of internet shutdowns. Case studies and links to additional resources have also been included for expanded self-learning.

Internews would like to thank and acknowledge the Toolkit’s authors and technical experts, Tawanda Mugari, Digital Rights Africa and Laura Schwartz-Henderson, consultant to OPTIMA, Internews. Internews further acknowledges the support of the Regional Media Institute (MISA) of Southern Africa and the contribution by Golden Maunganidze, Chairperson of MISA Regional.

About Internews
Internews is an international media support nonprofit that - for 40 years and in 100+ countries - believes everyone deserves trustworthy news and information to make informed decisions about their lives and hold power to account.

This toolkit is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of ARISA and do not necessarily reflect the views of USAID or the United States Government.
What the past few years have shown us is that internet shutdowns have increasingly become a potent tool in the arsenal of a variety of state and other actors across the Southern African region, particularly during electoral processes.

Over the past four years, access to the internet was limited or shut down completely during elections in both Tanzania and Zambia, while in Eswatini and Zimbabwe, shutdowns became a common occurrence during democratic protest action. In addition, senior Zimbabwean government officials have warned that they may resort to shutting down the internet if they detect what they described as ‘a rebellion’ during elections.

With rapid developments in technology, internet access has become foundational to freedom of expression and access to information, with access to the internet being taken for granted.

However, precedence has shown us that internet access is not always guaranteed and this raises the need for journalists, including civil society and human rights defenders to be prepared for the eventuality of internet shutdowns and importantly what needs to be done in such circumstances.
Being able to identify early warning signs is crucial to putting measures in place to remain connected. With a number of countries in the region, holding high stakes elections in the coming months, a number of countries have already shown a propensity to switch off the internet. Preparedness during this time is key.

Journalists need to be aware of the legislative environments in the countries they operate in, particularly by keeping an eye on recently introduced laws on cybersecurity. A cursory glance at all the countries in the region that have shut down the internet shows that they have all recently introduced cybersecurity laws which will have significant impacts on media freedoms and freedom of expression.

In cases of partial blockades of the internet, virtual private networks (VPNs) are key for journalists’ safety as well as their continued access to the internet. However, as shared in the toolkit, VPNs may not be very useful when there is a total shutdown of the internet as has happened in the past. This will require different tactics to be utilized to stay connected which are expanded on in this toolkit.

In cases where there is a total blockade, journalists need to be conscious about their physical security and go back to doing journalism as it was done in the ‘good old days’. Some measures include “hunting in packs”, where journalists go in large groups on assignment and are able to account for each other. While journalists are always after exclusive stories or scoops, which is not possible while working in groups, their safety is of more importance and as we always say: “no story is worth dying for.” Hunting in packs also entails that when it is time to retreat, the journalists should also retreat as a group and live to tell the story.

In cases where there are no internet shutdowns, journalists may still need to be wary of new laws and regulations on cybersecurity and surveillance, as alluded to earlier. Ostensibly, cybersecurity laws are enacted to protect users online, but in reality, they have been used to infringe on freedom of expression, the right to privacy and digital rights.

Capacity building for journalists, particularly about safety online, should be an ongoing exercise, with emphasis on new tools and technologies that can promote the safety of media workers. Which is why a toolkit on how to mitigate internet shutdowns provides tactics on what to do when there is a threat of an internet shutdown and when they are at risk of surveillance. It provides practical steps when faced with an internet shutdown and tips on staying connected to continue doing your work.

This toolkit is an important follow on to the on the surveillance and digital security guide also developed by Internews, titled: “A Survival Toolkit for Journalists: How to protect yourself against Digital Surveillance.” More toolkits of this nature will be produced depending on identified gaps and needs.

The internet is ubiquitous and has become a central part of most journalists’ work. Be that as it may, there is a risk that it may be shut down and there is need for media workers to prepare for that eventuality. It is my fervent hope that journalists find these toolkits useful and use them regularly as they go about their daily work.

Best regards,

Golden Maunganidze
Chairperson
MISA Regional
Internet shutdowns have a profound impact on millions of people annually, limiting their capacity to exercise fundamental rights and meaningfully participate in societies, economies, and democracies. Access Now’s #KeepItOn coalition documented 187 shutdowns in 2022. These were introduced by governments in 35 countries – the highest number of countries ever in a single year.

African countries make up a significant percentage of the countries in the world that have deployed shutdowns in the past. Ethiopia is currently the record holder for the world’s longest active shutdown in the Tigray region. Historically, African governments have used internet shutdowns during elections and moments of political uncertainty. With many elections coming up in the region in the next few years, there is an urgent need for civil society organizations, journalists, technologists, lawyers, and other sectors to come together to tell governments that internet shutdowns are neither necessary nor proportionate responses to national security or political problems.

Internet shutdown advocacy can be tricky: shutdowns are hard to predict, and once they occur it’s supremely hard to organize as internet and communications are curtailed. For this reason, much of the response tends to be reactive and in crisis mode. We put together this guide to help you mobilize your communities to prepare, prevent and resist internet shutdowns. This requires preparation, coordination, and knowledge sharing. Keep reading if you accept the challenge to become an anti-censorship warrior!
WHAT ARE INTERNET SHUTDOWNS & WHY GOVERNMENTS SHUT DOWN THE INTERNET

First, it’s very important to know what an internet shutdown is in order to understand how to effectively prepare and respond.

Often, when we think about internet shutdowns, we think about when the entire internet is cut off. This is called a network blackout. The government can cut mobile networks or fiber/cable/adsl networks or both. Blackouts can occur at the national level or be targeted to a specific region or municipality. Another way that governments shut the internet is through Domain Name Server (DNS) blocking. This occurs when governments block access to specific major social media sites or communication applications such as Facebook, Whatsapp, Twitter, Telegram, or via a Virtual Private Network (VPN) like TOR. Finally, governments can also slow down the internet - either on an entire network, or to a specific website or platform. This is called network throttling and is aimed to make the connection so slow it becomes unusable.

Each of these kinds of shutdowns are implemented differently at the technical level, and so it is important to understand what kind of shutdowns you face in your country in order to know how to circumvent and document the censorship and how to respond. To learn more about how we define internet shutdowns and the ways they occur, technically check out “A taxonomy of internet shutdowns.”

Why would a government shut the internet? It is important to know the rationales governments use in order for advocates to make a case for why internet shutdowns are extreme and ineffective. Governments sometimes provide official justifications for internet shutdowns, and some of the most common rationales they cite are national security issues, communal violence, public unrest or instability, controlling mis/disinformation, and preventing cheating during exams.

Often shutdowns go unacknowledged by governments with no transparency around why or how the shutdown order took place. It is important to understand that in addition to the cited rationales provided by governments, frequent ‘triggering events’ that might lead a government to shut down the internet include protests, elections, ongoing conflicts, major holidays or public events, and visits from public figures.

Access Now has been working for many years to document internet shutdowns through their #keepiton shutdown tracker optimization project (STOP). You can access a global dataset to see the ways in which shutdowns have occurred in your country or review their global reports here.
KNOW YOUR SHUTDOWN: EXAMPLES OF SHUTDOWN TACTICS IN AFRICA

NIGERIA: BLOCKING SOCIAL MEDIA TO CONTROL THE NARRATIVE

Twitter has been a very popular space for Nigerians, especially for youth to actively engage in political conversations. **Nigerians tweet more than any other African country.**

In June 2021, the government banned the platform, citing national security reasons after Twitter deleted a controversial tweet from President Muhammadu Buhari and political activists successfully used the platform for the #EndSARS protests to mobilize against police repression. Twitter was banned for seven months until January 2022.

The ECOWAS court ruled that this shutdown violated international law. However, the Nigerian government has put no policies in place to ensure that shutdowns cannot occur again in the future. According to the Cost of Internet Shutdowns 2022 Tracker, Nigeria lost an estimated 82.7 million dollars during this time.

Zimbabwe has experienced many kinds of internet shutdowns over the years. However, in February 2022, many internet users in Zimbabwe noticed that their internet was not loading.

ZIMBABWE: SLOWING THE INTERNET—NOTORIOUSLY HARD TO PROVE!

It was technically working, but it was so slow—especially to send or receive photos or videos. It is certainly normal to experience connectivity problems, but these slowdowns happened to occur during opposition protests in Harare. **While it is extremely difficult to prove that the government intentionally throttled internet speeds, data shows that speeds were slowed on multiple mobile operators, and prevented live streaming from the rally.** In March 2022, speeds were again throttled.

We can suspect that this was deliberate internet throttling, but it is very difficult to prove from a technical documentation perspective. This is another reason to work to develop better methodologies and to correlate network disruptions with political data!

ETHIOPIA: BLACKOUTS OF SILENCE DURING A CIVIL WAR

November 2020 saw the eruption of fighting in the Tigrayan region and the beginning of a more than two-year full network (internet and phone) blackout. Mobile data remains restricted, and social media has also been blocked with Ethiopia **shutting down the internet 24 times since 2016.**

The government justifies this telecommunications blackout citing instability and national security in the region. In this moment of crisis many people cannot reach their loved ones—“I don’t know even who is dead or who is alive”, said the head of the World Health Organization who comes from Tigray.

The internet blackout affects the entire network, and impacts the ability of journalists, as well as peacekeeping and humanitarian organizations to provide lifesaving services, report on the conflict, and monitor the human rights situation.
These three examples show you that internet shutdowns can happen in a variety of technical ways, based on how the government chooses to interfere with internet services. These cases also make clear that governments justify shutdowns often on the grounds of national security, but shutdowns often occur during moments of protest, political crisis, or elections.

Check out CIPESA’s framework for calculating the economic impact of shutdowns. Shutdowns also impact health, education, and other development outcomes. See here for a one page guide outlining the negative impacts of shutdowns created by the Global Network Initiative.

UNDERSTANDING IMPACT OF SHUTDOWNS & CONDUCTING A RISK ASSESSMENT FOR CSOs & HRDs

*CSOs: Civil Society Organisations, HRDs: Human Rights Defenders

In order to conduct effective advocacy against internet shutdowns it is also important to know the many ways in which an internet shutdown can violate human rights and impact societies, economies and democracies.

Often, when we talk about the negative impacts of shutdowns, we focus on how they violate our human rights. In 2016, the United Nations declared internet access an enabling right for all other human rights – this means that when the government denies access to the internet, it is preventing people from their fundamental rights to freedom of expression, work, education, life, and liberty. Internet shutdowns have significant economic impacts, as they disrupt major businesses from conducting work online.

Check out CIPESA’s framework for calculating the economic impact of shutdowns. Shutdowns also impact health, education, and other development outcomes. See here for a one page guide outlining the negative impacts of shutdowns created by the Global Network Initiative.

This GNI paper, authored by Tomiwa Ilori, outlines the social impacts of shutdowns in Africa. Shutdowns that occur around elections also significantly impact the ability of citizens to exercise their democratic rights safely and freely. See here for a shutdowns election guide.
MAKING THE CASE AGAINST SHUTDOWNS IN ZIMBABWE:
THE IMPACT ON HEALTH & DEVELOPMENT

There have been several internet shutdowns in Zimbabwe, since 2016 including blocking of WhatsApp and Facebook and a total internet blackout that lasted for seven days in 2019. Additional incidents have been reported (but often not verified) of throttling of internet speeds during protests. As MISA has reported, Zimbabwe is particularly at risk of future shutdowns around activities during the upcoming elections.

In addition to making the case for why internet shutdowns violate our human rights, it is also important in internet shutdown advocacy to make it clear to governments that internet shutdowns have important and negative impacts on national economies, digital markets, human development, education as well as social, physical and psychological health. If we offer nuanced arguments about the way shutdowns impact societies diversely, it is more likely that governments might think twice before deploying shutdowns.

As part of Internews’ OPTIMA project, research was conducted by Prince Kudakwashe Madiwa, a healthcare delivery expert, to understand the impact of these shutdowns on healthcare service delivery and the government’s wider telemedicine project. This research found that shutdowns significantly impacted doctor’s access to important information, patient’s access to health care services and patient outcomes. This research has been used to argue against internet shutdowns and to bring new voices (doctors, patients) into advocacy campaigns.

In effectively making the case against internet shutdowns, it is important to demonstrate that not only do internet shutdowns impact human rights, but they also impact other important economic and human development outcomes! More research is needed to demonstrate the diverse ways shutdowns impact societies!

It is important to understand how internet shutdowns impact societies and the risks of shutdowns as they relate to human rights outcomes. For this reason, we recommend that you conduct an internet shutdown risk assessment that can help you understand the risk that your community faces around internet shutdowns and skills or knowledge that you may need in order to more effectively prepare for shutdowns and fight back.

You can first take a personal shutdown risk assessment to help you understand your risk of experiencing an internet shutdown. When you complete the questionnaire, you will be able to download your assessment results to understand your risk and customized advocacy resources.

If a shutdown is likely in your country, we also recommend that you design an internet shutdown needs assessment to survey journalists and human rights defenders to understand what the existing capacities and needs are to fight back against internet shutdowns. Please see this full advocacy assembly course to learn how to design a needs assessment for your country. You can also check out some example country needs assessments conducted by Internews’ OPTIMA project from Senegal, Tanzania, India, and Bangladesh.

It is extremely important to work with your communities to understand how shutdowns happen in your country, what the potential triggering events might be, and the actors who you need to form a coalition. This is why community-informed research such as this is so key to effectively battling shutdowns in the long-term!
INTERNET SHUTDOWN SKILLS
YOU NEED!

Internet shutdowns happen very differently in each country and they require nuanced strategies to fight back. In order to engage in internet shutdown advocacy, you will need to build a coalition of many different kinds of people with different skills. Below we have described a few key skills you will need as a coalition to prepare for internet shutdowns and fight back.

Advocacy against internet shutdowns is not easy. Shutdowns often occur without warning, and often take place during major national events or political crises. For this reason, we need to be prepared in advance. We recommend that you work to build a coalition of organizations and individuals with diverse skill sets and networks to engage in longer-term planning around internet shutdowns and to build an internet shutdown action plan.

Things you will need to think about when building this action plan include:
- What are the events that have triggered internet shutdowns in the past (elections? protests?) What did we learn from past shutdowns in our country/region?
- Are there upcoming events like these that could lead to a shutdown? Can we build a timeline to plan around these events?

There are many kinds of advocacy actions that you can take:

**BEFORE**
- There are things that should occur before a shutdown occurs such as translating and localizing guides and resources for your communities, communications and outreach to key stakeholders, and trainings and workshops.

**DURING**
- There are things you should plan to do while a shutdown is happening such as technically measuring censorship, documenting human rights violations, and coordinating with international actors.

**AFTER**
- After a shutdown occurs, it is also important to consider options such as whether you can use strategic litigation to claim that a shutdown has violated the laws of your country or region. You can also think about outreach to actors involved in internet shutdowns, like Internet Service Providers and other private sector actors.

This short guide explains research on ISP’s role in Internet Shutdowns in Africa and how to engage with these actors. This advocacy assembly course teaches you how to engage with the private sector around internet shutdowns.

This advocacy assembly course will walk you through the process of building this kind of an action plan by building a timeline, brainstorming actions, and understanding the stakeholders involved. OPTIMA has also produced a guide to resources on designing shutdown advocacy that is impactful, inclusive and responsive as well as a pre-election checklist on a variety of activities you can conduct before an election to be fully prepared for a potential shutdown. This research evaluates the advocacy strategy used before, during and after the 2017-2018 internet shutdown in the Anglophone regions of Cameroon.
INTERNET SHUTDOWNS CAMPAIGNING ACTIVITIES

For before a shutdown:
- Do we have a plan to circulate key information in the days before a possible shutdown with the goal to PREVENT the shutdown?
- Do we have copy ready to go out to journalists and other stakeholders on how internet shutdowns violate human rights and negatively impact society (to send before the election)?
- Have we coordinated with international organizations like accessnow to send letters to the government to prevent a shutdown?
- Have we created and distributed resources for vulnerable communities such as at-risk human rights defenders, opposition groups, and marginalized groups to know what to do during a shutdown?

For during a shutdown:
- Have we prepared written copy to post to social media and other channels about STOPPING an ongoing shutdown that we have circulated to coalition members and international partners?
- Do coalition members know who might need specific support during a shutdown?
- Do we have people in diverse areas of the country documenting the social and personal impact of shutdowns and prepared to report human rights abuses?

For after a shutdown:
- Do we have a plan to collect impact stories and documentation of human rights abuses that occurred during a shutdown?
- Do we have a plan to coordinate with journalists on accurate reporting of the shutdown and its impact?
- Do we have a plan to coordinate with lawyers on possible post-shutdown legal actions?
Censorship refers to the practice of suppressing or controlling information, opinions, or artistic expression by a governing authority or other controlling entity. It involves the restriction or manipulation of access to certain content, ideas, or communication channels, often with the aim of maintaining political control, protecting national security, or preserving social order.

INTERNET SHUTDOWNS ARE A FORM OF CENSORSHIP THAT IS VERY EXTREME AND IS CONSIDERED BY THE HUMAN RIGHTS COMMUNITY AS NEITHER NECESSARY NOR PROPORTIONATE.

Circumvention in the context of internet shutdowns refers to the act of bypassing or overcoming censorship measures or internet restrictions. It involves using various techniques, tools, or technologies to access blocked websites, communicate securely, and evade surveillance. Circumvention methods can include virtual private networks (VPNs), proxy servers, Tor networks, encrypted messaging apps, and other anonymization tools.

Circumvention plays a crucial role in enabling individuals, activists, journalists, and organizations to bypass censorship and access information freely. Circumvention tools allow people to communicate securely, share news, express dissenting opinions, and organize actions even in the face of internet shutdowns.

However, it is important to note that in some jurisdictions, the use of circumvention tools may be restricted or illegal, and individuals attempting to circumvent censorship may face legal consequences.

It is also important to note that as we described earlier, there are different kinds of internet shutdowns (blocking, throttling, full network blackouts) and not all tools will work to circumvent all kinds of shutdowns.

Below we have outlined some of the tools you can use in different shutdown scenarios, but see here for a full comprehensive guide developed by Internews’ OPTIMA project on shutdown tools and their applicability for different types of shutdowns.
ANTI-CENSORSHIP TOOLS & VIRTUAL PRIVATE NETWORKS (VPN)

A Virtual Private Network (VPN) is a technology that allows you to create a secure and private connection over the internet. It creates a virtual tunnel between your device (such as a computer, smartphone, or tablet) and a remote server operated by a VPN provider. **A VPN will often allow you to circumvent when the government is blocking a major social media platform or an application.** It is not likely to work in a blackout scenario.

When you connect to a VPN, your internet traffic is routed through this encrypted tunnel. This means that your data, such as websites you visit, files you download, or messages you send, is protected from being intercepted or viewed by others. While using a VPN helps you privately engage with online content, it is very important to note that ISPs and governments can detect that you are using a VPN. A good resource for how VPNs work, what they do and what they don’t help with is here.

To prepare for potential internet shutdowns, it is advisable to download various censorship circumvention tools onto multiple devices if you can in the case that a particular tool is blocked or fails.

---

**KEY FEATURES OF A VPN**

**PRIVACY AND SECURITY**

- A VPN encrypts the internet traffic, making it difficult for anyone to eavesdrop or track your online activities.

**ANONYMITY AND IDENTITY PROTECTION**

- By connecting to a VPN server, your IP address (a unique identifier for your device on the internet) is masked, and the websites or services you visit see the VPN server’s IP address instead. This helps protect your identity and adds an extra level of anonymity.

**ACCESS TO RESTRICTED CONTENT**

- A VPN can allow you to bypass geographical restrictions or censorship imposed by certain websites, services, or even governments. By connecting to a VPN server in a different location, you can appear as if you are accessing the internet from that location, thus gaining access to content that might be blocked in your actual location.

**REMOTE ACCESS AND SECURE CONNECTIONS**

- VPNs are often used by businesses and organizations to provide secure remote access to their internal networks for employees working from outside the office. It ensures that sensitive data transmitted between the remote user and the company’s network remains secure.
THINGS TO CONSIDER WHEN CHOOSING A VPN

• **Security and Privacy:** Look for a VPN provider that has a strong commitment to security and privacy. Consider factors such as the encryption protocols they use, their logging policy (preferably a strict no-logs policy), and the jurisdiction in which the provider operates (preferably a country with strong privacy laws).

• **Logging Policy:** Ensure that the VPN service you choose has a clear and transparent logging policy. A strict no-logs policy means that the provider doesn’t store any information about your online activities, ensuring better privacy and anonymity.

• **Server Locations and Coverage:** Check the number and distribution of servers offered by the VPN provider. More server locations provide you with a wider choice of virtual locations to connect to, allowing for better access to geo-restricted content and improved connection speeds.

• **Connection Speed and Performance:** Consider the VPN’s performance and connection speeds. Some VPN providers may slow down your internet connection due to factors like server load or distance. Look for providers that offer fast and reliable connections to ensure a smooth browsing experience.

• **Device Compatibility:** Make sure the VPN service supports the devices and platforms you plan to use it on. Whether it’s Windows, macOS, iOS, Android, or other platforms, compatibility ensures you can protect all your devices.

• **User-Friendly Interface:** A user-friendly VPN interface makes it easier to set up and use the service. Look for intuitive apps or software that offer a simple and straightforward user experience, even for those who are less tech-savvy.

• **Customer Support:** Consider the availability and quality of customer support provided by the VPN service. Look for providers that offer timely and responsive customer support channels, such as live chat, email, or ticket systems.
• **Pricing and Payment Options:** Evaluate the pricing plans and payment options offered by the VPN provider. Compare the subscription costs, available features, and any additional fees. Also, check if they offer a money-back guarantee or free trial period to test the service before committing.

• **Reputation and Reviews:** Research the reputation and user reviews of the VPN service you’re considering. Look for independent reviews and user feedback to get insights into their reliability, performance, and customer satisfaction.

### RECOMMENDED VPNS

- TunnelBear
- Psiphon
- Mullvad
- NordVPN

---

### USING THE TOR BROWSER

The Tor (The Onion Router) browser is a web browser that focuses on protecting your privacy and anonymity while you browse the internet. It is designed to help you access websites without revealing your identity or location. When you use the Tor browser, your internet traffic is routed through a network of volunteer-operated servers called “Tor relays” or “nodes.” These nodes are spread worldwide and help disguise your online activities.

It’s important to note that while the Tor browser provides anonymity, it doesn’t guarantee complete security. It can protect your identity and browsing activities to a certain extent, but it may not provide the same level of encryption as a VPN or protect against all potential threats.

Using the Tor browser is as simple as downloading and installing it on your device, similar to any other web browser. Once you launch the Tor browser, it automatically connects to the Tor network, and you can start browsing websites while enjoying increased privacy and anonymity.

You can get the Tor browser [here](#).

---

### WHAT CAN I DO IF A VPN DOESN’T WORK?

VPNs are excellent tools, not only to circumvent censorship but also to stay safe and private online. However, as we mentioned before, VPNs won’t work in every internet shutdown scenario and sometimes VPNs and circumvention tools are blocked by governments as part of an internet shutdown. For this reason, we also need to develop other plans and strategies for how to communicate if there are other forms of network interference or if your VPN doesn’t work.
Throttling:
Throttling or slowing of the internet can be extremely difficult to circumvent. However, if only specific sites or services are being targeted (such as slowing down only Facebook sites and applications), using any of the previously listed VPNs and circumvention tools might work.

Full network blackouts:
If there is a full network blackout, it is likely that many of the above tools will not work. There are a few tools that are designed for these scenarios. However, it is important to note that these tools require much more testing, and you should download and test them in advance of a shutdown. They might also pose their own security issues.

- **F-Droid**: A tool used for Android app sharing, if both phones have F-Droid, they can swap apps even without Internet
- **Veracrypt**: A tool that lets you create encrypted disks or “virtual” disks that can be shared over USB drive or SD card.

Another circumvention strategy that can be used in total network blackouts relies on satellite technologies. However, satellite communication tools are often highly regulated, they are not immune to blocking or jamming, usage of 2-way satellite communication can be detected, and the costs to using these tools can be quite high.

**THE MOST IMPORTANT CIRCUMVENTION TOOL: PLANNING!**

Often internet blackouts only target mobile connectivity (voice/sms/data) but leave on fiber, cable, broadband or DSL internet. In this case, you might be able to connect via a laptop but not a mobile phone, or at an office or school but not at home. Additionally, often mobile data might be blocked, but SMS and voice calls are available.

For this reason, the most important thing to do to prepare for ‘circumventing’ an internet shutdown is to develop a communication plan based on what communication channels might or might not exist.

The most important thing to take away from this section is that preparation is key and you must plan for a variety of censorship scenarios. Download several VPNs, know how to access a computer if mobile data is targeted, exchange phone numbers with key people if SMS or voice calls still work. Keep in mind that mobile voice and SMS are far less secure and easier for the government to monitor, so be careful. In-person meeting points are often key to set up in advance.
PRE-SHUTDOWN COMMUNICATIONS PLAN CHECKLIST!

- Do we have a key contact info sheet (including telephone, signal, relevant social media, secure location if needed) for key contacts
- Have you circulated a list of verified and secure circumvention tools that coalition members can use in case of blocking of social media platforms?
- Have you established a contact out of the country who can share content and securely operate social media accounts should access be denied within the country?
- Do you know SMS/phone numbers of key contacts to coordinate around network measurement, campaigns & support should internet services be disabled? *note that SMA/voice is easier to surveille, see applications below that make SMS more secure
- If all forms of communication are disabled, do you have a secure location (or set of locations) designated for people to physically meet?
- Have you downloaded key applications to phone and desktop in advance? These can include:
  - Your choice VPN or circumvention tool* (note the risks of using VPNs in certain countries).
  - At least one backup VPN in case of blocking. This could include a self-hosted option like outline or algo which is less likely to be blocked. (requires some technical ability)
  - Peer to peer messaging apps like Briar, Bridgy, or Firechat (refer to circumvention guide for more details on the uses and security tradeoffs of these applications)
  - Network measurement applications such as OONI & NDT speed test
- Other forms of communication you can seek access to:
  - International sim cards
  - Satellite services
  - Mesh networks
  - Offline security & app-sharing software like F-Droid and Veracrypt
  - Applications that make SMS more secure like silence.im or frontline.local
One of the most important skills needed to fight against shutdowns is the ability to collect the technical evidence to prove that an internet shutdown has occurred (as Governments often don’t publicly acknowledge that they have ordered a shutdown).

Without clear evidence, it is very difficult for journalists to report on internet shutdowns, for legal cases to be made against them, and for advocacy communities to push back. You need people in your country who are able to collect this evidence and communicate this technical data with journalists, lawyers and activists.

Network measurement is the area of research that is used to both collect and analyze network data to determine when there has been interference with the network by the Government. As we noted above, shutdowns occur in different ways technically, and there are different tools and methodologies used to detect different kinds of censorship and shutdowns. For example, if you are experiencing blocking of social media platforms you would use the tools offered by the Open Observatory of Network Interference (OONI), but if you wanted to measure full network blackouts you would look at the Internet Outage Detection and Analysis dashboard. Below, you will see a quick visual guide about the tools that you can use for different kinds of censorship, including OONI (the Open Observatory of Network Interference), IODA (the Internet Outage Detection and Analysis project), M-lab (measurement lab), RIPE Atlas, Censored Planet, and Google Transparency Reports’ Traffic Data. Here you will find full descriptions of each of these tools. OPTIMA created this online series of videos to provide you an overview about the major network measurement tools and methods. This network measurement guide provides links to many resources related to measuring censorship and shutdowns. This short guide describes the technical difficulties and approaches we take to measuring network throttling.

<table>
<thead>
<tr>
<th>Website and App Censorship</th>
<th>Network Performance (Speed)</th>
<th>National Internet Outage</th>
<th>Regional Internet Outage</th>
<th>Specific Network Outage</th>
</tr>
</thead>
<tbody>
<tr>
<td>OONI</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>IODA</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>M-Lab</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>RIPE Atlas</td>
<td>PARTIAL</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Censored Planet</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Google Transparency</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>
The cancer of the modern world.

This is how Senegal’s President Macky Sall described social media after protests erupted over his government’s arrest of a main opposition leader and Senegal’s ruling party lost key local elections early in 2022. In Senegal, a country where 70% of the population is below 40, people have taken to social media to discuss politics, to express their anger, and to organize. In French, Wolof, and English, the hashtag #freeSenegal became a rallying cry on Twitter and Instagram to mobilize protests. Senegal’s civil society is one of the most notably vibrant and diverse free civil societies in Africa. However, the Senegalese government, like too many others in Africa and around the world, sees online dissent and political debate as something to be remedied, and is increasingly using forms of digital repression and censorship to control online spaces. In 2021, as protests and online dissent grew, the government did what so many other governments have started to do: they tried to shut it down.

On March 4, 2021, following a day of protests and cases of violence, the government allegedly restricted access to Facebook, WhatsApp, YouTube, and Telegram, and suspended two private television channels that had heavily covered the protests. There is limited evidence available about this internet shutdown incident, in part because the shutdowns reportedly occurred early in the morning and only for a few hours. Additionally, as reported by local actors, civil society was not prepared for such a shutdown, with few people equipped to technically measure incidents of network disruption and little capacity on the part of journalists to adequately cite technical evidence and report on the shutdown.

As part of the Internews OPTIMA project, Internews worked with Senegalese organizations Jonction and Computech to conduct an internet shutdown needs assessment with Senegalese civil society and media. In advance of the very contentious 2024 elections in Senegal, OPTIMA, Jonction and Computech organized the Senegalese Prepare, Prevent, Resist network to prepare for the possibility of a larger internet shutdown. As part of this network, journalists and activists took part in network measurement trainings and fellowships and engaged in a public awareness campaign to get people to understand the threat of internet shutdowns and how to use VPNs and circumvention tools. After months of these preparations, an internet shutdown occurred in June 2023 around protests in the country, with access blocked to Facebook, Whatsapp, Telegram, Instagram and Youtube for two days and then shutting down mobile internet for four days. The Prepare, Prevent, Resist network coordinated collecting technical evidence, building legal strategic responses, and distributing information about circumvention strategies. The network has also engaged in an after-action assessment and is collecting evidence on the human impact of the shutdown.
DIGITAL SECURITY TIPS FOR INTERNET DISRUPTIONS

As we mentioned before, establishing a clear plan in advance of a shutdown is key for being prepared to communicate and share information. It is also key to assess your own security risks to understand how you can protect yourself and others during high-risk scenarios.

OPERATIONAL SECURITY

Operational security, often abbreviated as OPSEC, refers to the practices and measures taken to protect sensitive information and maintain confidentiality in the context of sensitive work. It involves strategies aimed at preventing the unauthorized disclosure of information, preserving source anonymity, and safeguarding the integrity of journalistic and civil society organisation investigations.

For CSOs & journalists, operational security is crucial in situations where they handle sensitive or classified information, conduct investigations into sensitive subjects, or work in environments where the freedom of the press may be compromised. By implementing OPSEC measures, organisations can mitigate risks, protect themselves and their sources, and ensure the integrity and impact of their reporting.

HERE ARE SOME KEY ELEMENTS OF OPERATIONAL SECURITY:

- **Source Protection**: Organisations must take steps to safeguard the identity of their sources, especially when dealing with sensitive or whistleblowing information. This may involve using secure communication channels, encryption tools, and anonymization techniques to protect the identity and communications of sources.

- **Secure Communication**: Organisations should utilize secure communication methods, such as encrypted messaging apps (Signal Messenger, Wire Secure Messenger & Delta Chat) or encrypted email services, to ensure that their conversations and information exchanges are protected from interception or surveillance.

- **Digital Security**: Organisations should employ strong digital security practices, such as using strong, unique passwords for their accounts, enabling two-factor authentication, regularly updating software and operating systems, and using virtual private networks (VPNs) to protect their online activities.

- **Secure Storage**: It is important for organisations to securely store their data, documents, and research materials. This can involve using encrypted storage devices or cloud services, as well as ensuring that physical copies of sensitive information are kept in a secure location.

- **Physical Security**: Organisations may need to be mindful of their physical security, especially when working in high-risk or hostile environments. This may include taking precautions to protect their equipment, being aware of their surroundings, and taking steps to minimize the risk of theft or surveillance.

- **Risk Assessment**: Organisations should conduct regular risk assessments to identify potential vulnerabilities or threats to their work. This involves evaluating the sensitivity of the information they handle, assessing the potential risks to their sources, and adapting their operational security practices accordingly.
OPERATIONAL SECURITY

1. Secure Device and Data
   Ensure that your devices, including smartphones, laptops, or tablets, have strong passwords or passcodes set up. Encrypt your important files and data stored on your devices, and consider using partial-disk encryption using VeraCrypt or full-disk encryption to protect sensitive information through BitLocker for Windows machines or FileVault for Mac machines.

2. Backup Important Data
   Regularly back up your important files and data to an external storage device or a secure cloud service. This ensures that even if your device is compromised or inaccessible, you still have access to your essential information.

3. Offline Communication
   During an internet blackout, rely on offline communication methods to exchange information. Use encrypted messaging apps or secure communication tools that function without internet access, such as mesh networks, peer-to-peer communication (Briar, SMS WithoutBorders).

4. Secure Physical Storage
   If you need to store physical copies of sensitive documents or data, ensure they are kept in a secure location. Use locked cabinets or safes to protect them from unauthorized access or theft.

5. Maintain Source Anonymity
   If you are working with sources during an internet blackout, take extra precautions to protect their identities. Use secure and offline communication methods, meet in secure locations, and avoid leaving digital traces that could potentially compromise their anonymity.

6. Stay Informed and Connected
   Even during an internet blackout, try to stay informed about the situation through other means, such as radio broadcasts, local news outlets, or word-of-mouth information. Maintain connections with trusted colleagues, journalists, or contacts who may have access to information or updates.

Even during an internet blackout, try to stay informed about the situation through other means, such as radio broadcasts, local news outlets, or word-of-mouth information. Maintain connections with trusted colleagues, journalists, or contacts who may have access to information or updates.
1. The **KeepItOn Toolkit** is a great place to start both to learn more about the basics of internet shutdowns and also to begin understanding best practices for responding to and advocating against internet shutdowns. AccessNow has developed a range of great resources and keeps the [STOP internet shutdown tracker](https://www.stopinternetshutdown.org), tracking shutdowns around the world from 2016 to present.

2. The **OPTIMA Prepare, Prevent, Resist Internet Shutdown Resource Library**: The Prepare, Prevent, Resist Resource Library is organized into four overarching categories to help you find the resources most relevant to you. When conducting advocacy, carrying out awareness raising efforts, or simply learning more about shutdowns and what you can do to prepare, it is likely that you will benefit from a range of resources from more than one of these categories. The guides are designed to better contextualize resources, offer connections between specific materials, and support you in navigating the library stacks. Think of these as your librarian’s reference books!

3. The **OPTIMA Internet Shutdown Advocacy Needs Assessment**: OPTIMA has created a methodology for assessing internet shutdown risk and advocacy capacity in specific countries. Check out this website to see example research from Senegal, Tanzania, India and Bangladesh. You can also take your own assessment and receive a customized risk & resource report.

4. The **Advocacy Assembly Internet Shutdown Academy** includes extended courses on a range of skills needed for internet shutdown advocacy, including an introduction to internet shutdowns, developing an internet shutdown action plan, engaging with the private sector on shutdowns, documenting human rights violations during shutdowns, detecting internet shutdowns with IODA, and measuring shutdowns and internet censorship with OONI. More courses are being added, and you can take these courses yourself or use them as a way to train others in your network!

5. **OONI (Open Observatory of Network Interference)** is the world’s largest open dataset on internet censorship and is used to determine whether specific websites or applications have been blocked. OONI Probe allows you to collect data on your own device through an application, whereas OONI Explorer allows you to explore data that has been collected by testers from around the world.

6. The Cyber Security and Digital Surveillance toolkit
7. The Fact Checking toolkit - Please share specific resource
8. The Safer Journo Guide (for journalist group specifically) - Resource shared on email
9. The Legal and regional aspects of the Cyber Security space - Litigation Session to cover this
10. **A Taxonomy of An Internet Shutdown**: In this paper written and published by Access Now, the authors outline each of the various technical mechanisms for implementing a shutdown, and the options for mitigating each type. The goal of this resource is to support technologists and civil society groups working to end shutdowns through a technical resource to understand, prepare for, circumvent, and help document deliberate network disruptions.
11. **Digital Safety Tips for Network Disruptions**: This visual guide by Accessnow outlines some basic steps to prepare for and navigate internet shutdowns from understanding shutdown types, to using VPNs and establishing communications, to documenting network disruptions.
12. **Quick Guide to Circumvention Tools for Use in Different Shutdown Scenarios**: Internews developed this primer that offers an overview of many of the most effective circumvention tools you can use to connect during a shutdown.
13. **Lawyer’s Hub user-friendly Internet Shutdown primer**: Lawyers Hub Kenya built this user-friendly primer that provides an easy-to-read introduction to shutdown advocacy, including definitions of shutdowns, network measurement tools, censorship circumvention methods and other useful information for understanding and responding to shutdowns before they occur.
14. **The OPTIMA Network Measurement Training** is a multi-module virtual course for anyone interested in learning the basics of internet shutdowns, and how to use three of the most common measurement tools: OONI, MLab, and IODA.
15. **Magma** is an open-licensed, collaborative repository that provides comprehensive instruction and resources for people working to measure information controls and online surveillance activities. In it, users can find the resources they need to perform their research more effectively and efficiently.
**FACTSHEET**

### Advocating Against Shutdowns

**BEFORE**
- Build a diverse coalition of organizations and individuals invested in fighting back against shutdowns.
- Ensure this coalition has developed an action plan & has a mechanism to coordinate actions.

**DURING**
- Coordinate with your coalition members and the communities you serve to make sure they are safe & that information is being communicated.
- Use national and international channels to argue to STOP an ongoing shutdown.

**AFTER**
- Use research and documentation to tell the stories of how the shutdown impacted communities.
- Engage in outreach to new stakeholders to encourage them to reflect on their experience with the shutdown & fight back.
- Continue to lobby international and national actors to prevent future shutdowns.

### Challenging shutdowns in courts

**BEFORE**
- Develop a baseline understanding of your countries laws that may allow for shutdowns or prohibit shutdowns.

**DURING**
- Work with lawyers to develop a legal strategy should a shutdown occur.

**AFTER**
- Collect evidence and determine if strategic litigation would be an effective strategy to argue that the shutdown violated national or international law.

### Connecting & communicating during a shutdown

**BEFORE**
- Download (and test!) a range of circumvention tools.
- Develop a communication plan for a variety of shutdown scenarios.

**DURING**
- Try different circumvention tools & methods.
- Document which tools and methods work and don’t work.

**AFTER**
- Communicate with international actors and tool developers about your experiences using their tools so that they can improve.
- Document stories of the effectiveness of tools to help promote VPN use.

### Documenting shutdowns

**BEFORE**
- Train yourself and others in how to use network measurement tools to collect technical data.

**DURING**
- Collect network data using a variety of tools!
- Coordinate with others to collect data from many regions to ensure you have data on different locations and ISPs!

**AFTER**
- Use the collected evidence to analyze the shutdown scenario.
- Work with organizations like Access Now and OONI to produce reports to clearly document how a shutdown technically transpired.
- Be sure to also use qualitative research to document the social, psychological, and economic impact of shutdowns too!