Internet shutdowns: here's how governments do it

Lisa Garbe Published: August 8, 2023 9:41am EDT

Senegal's government has shut down internet access in response to protests about the sentencing of opposition leader Ousmane Sonko. This is a tactic governments are increasingly using during times of political contention, such as elections or social upheaval. The shutdowns can be partial or total, temporary or prolonged. They may target specific platforms, regions, or an entire country.

I'm a researcher who investigates the causes and consequences of internet access disruptions and censorship in various African countries. This includes understanding how shutdowns work.

It's important to understand the complex technicalities behind internet shutdowns, for at least two reasons.

First, understanding how an internet shutdown works shows whether or how it can be circumvented. This makes it possible to support affected communities.

Second, the way a shutdown works shows who is responsible for doing it. Then the responsible actors can be held to account, both legally and ethically.

Different forms of shutdowns require different levels of technical sophistication. More sophisticated forms are harder to detect and attribute.

There are two common strategies governments use to disrupt internet access: routing disruptions and packet filtering.

How to shut down the internet

Routing disruptions

Every device connected to the internet, whether it’s your computer, smartphone, or any other device, has an IP (internet protocol) address assigned to it. This allows it to send and receive data across the network.

An autonomous system is a collection of connected IP networks under the control of a single entity, for instance an internet service provider or big company.

These autonomous systems rely on protocols – called border gateway protocols – to coordinate routing between them. Each system uses the protocol to communicate with other systems and exchange information about which internet routes they can use to reach different destinations (websites, servers, services etc).

So, if an autonomous system, like an internet service provider, suddenly withdraws its border gateway protocol routes from the internet, the block of IP addresses they administer disappears from the routing tables. This means they can no longer be reached by other autonomous systems.

As a consequence, customers using IP addresses from that autonomous system can’t connect to the internet.

Essentially this tactic stops information from being transmitted. Information can’t find its destination, and people using the internet will not be able to connect.

The disruption of border gateway protocols can easily be detected from the outside due to changes in the global routing state. They can also be attributed to the internet service provider administering a certain autonomous system.

For instance, data suggests that the infamous internet shutdown in Egypt in 2011 – an unprecedented blackout of internet traffic in the entire country – was the result of tampering with border gateway protocols. It could be traced back to individual autonomous systems and hence internet service providers.

Border gateway protocol disruptions that entirely disconnect customers from the internet are rare. These disruptions can easily be detected by outside observers and traced back to individual organisations or service providers. In addition, shutting down entire networks is the most indiscriminate form of an internet shutdown and can cause significant collateral damage to a country's economy.

Packet filtering

To target specific content, governments often use packet filtering – shutting down only parts of the internet.

Governments can use packet filtering techniques to block or disrupt specific content or services. For instance, internet service providers can block access to specific IP addresses associated with websites or services they wish to restrict, such as 15.197.206.217 associated with the social media platform WhatsApp.

Governments also increasingly use deep packet inspection technology as a tool to filter and block specific content. It's commonly used for surveillance. Deep packet inspection infrastructure enables the inspection of data packets and hence the content of communication. It's a more tailored approach to blocking content and makes circumvention more difficult.

In Senegal, internet service providers likely used deep packet inspection to block access to WhatsApp, Telegram, Facebook, Instagram, Twitter and YouTube.

When internet shutdowns are done through packet filtering, only individuals within the affected network are able to detect the shutdown. Therefore, active probing is required to detect the shutdown. This is a technique that’s used by cybersecurity researchers and civil society actors to study the extent and methods of internet censorship in different regions.

Violation of rights

Though the two most common strategies are routing disruptions and packet filtering, there are many other tools governments can use. For instance, domain name system manipulation, denial of service attacks, or the blunt sabotage of physical infrastructure. A detailed overview of techniques is provided by Access Now, an NGO defending digital civil rights of people around the world.

There is wide agreement that internet shutdowns are a violation of fundamental rights such as freedom of expression. However, governments are developing increasingly sophisticated means to block or restrict access to the internet. It’s therefore important to closely monitor the ways in which internet shutdowns are being implemented. This will help to provide circumvention strategies and hold the implementers to account.