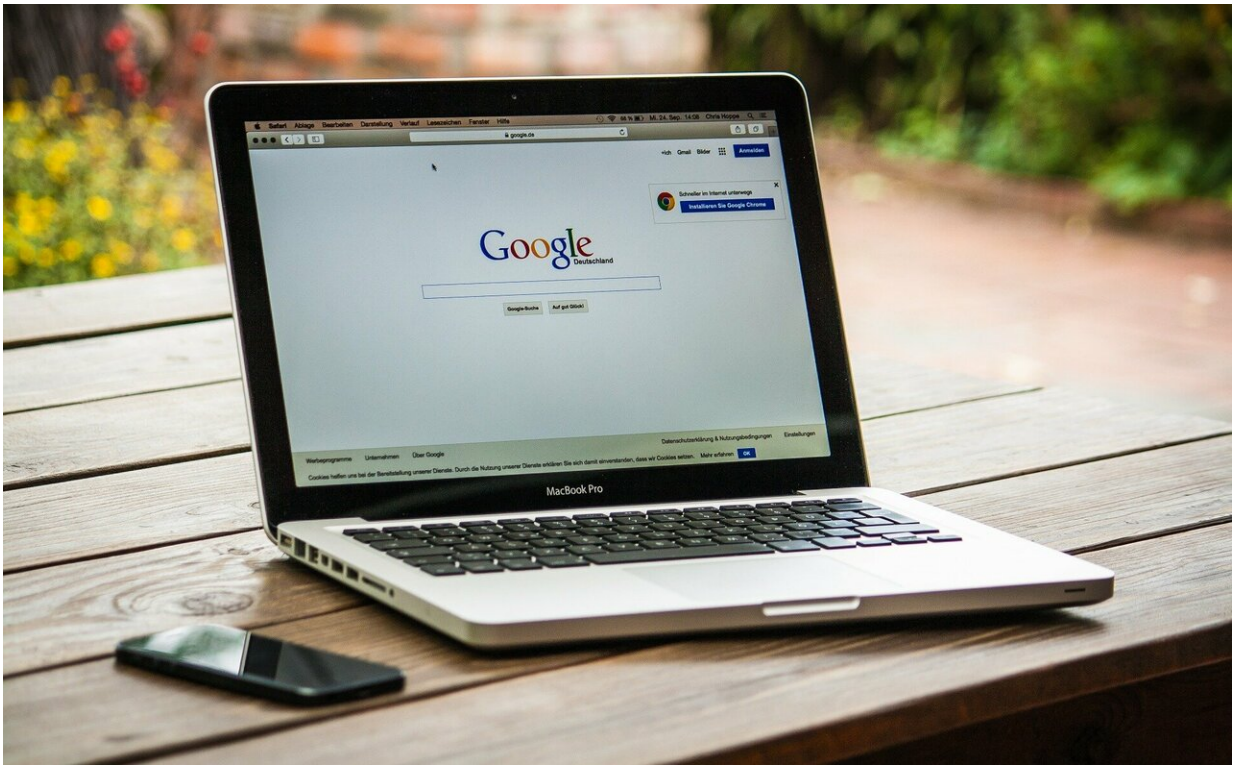
Shutting down the internet doesn't work—but governments keep doing it

February 20 2019, by George Ogola



Credit: CC0 Public Domain

As the internet continues to gain considerable power and agency around the world, many governments have moved to regulate it. And where regulation fails, some states resort to internet shutdowns or deliberate disruptions.

The statistics are staggering. In India alone, there were 154 internet shutdowns between January 2016 and May 2018. This is the most of any country in the world.

But similar shutdowns are becoming common on the African continent. Already in 2019 there have been shutdowns in Cameroon, the Democratic Republic of Congo, Republic of Congo, Chad, Sudan and Zimbabwe. Last year there were 21 such shutdowns on the continent. This was the case in Togo, Sierra Leone, Sudan and Ethiopia, among others.

The justifications for such shutdowns are usually relatively predictable. Governments often claim that internet access is blocked in the interest of public security and order. In some instances, however, their reasoning borders on the curious if not downright absurd, like the case of Ethiopia in 2017 and Algeria in 2018 when the internet was shut down apparently to curb cheating in national examinations.

Whatever their reasons, governments have three general approaches to controlling citzens' access to the web.

How they do it

Internet shutdowns or disruptions usually take three forms. The first and probably the most serious is where the state completely blocks access to the internet on all platforms. It's arguably the most punitive, with significant social, economic and political costs.

The financial costs can run into millions of dollars for each day the internet is blocked. A Deloitte report on the issue estimates that a country with average connectivity could lose at least 1.9% of its daily GDP for each day all internet services are shut down.

For countries with average to medium level connectivity the loss is 1% of daily GDP, and for countries with average to low connectivity it's 0.4%. It's estimated that Ethiopia, for example, could lose up to US$500,000 a day whenever there is a shutdown. These shutdowns, then, damage businesses, discourage investments, and hinder economic growth.

The second way that governments restrict internet access is by applying content blocking techniques. They restrict access to particular sites or applications. This is the most common strategy and it's usually targeted at social media platforms. The idea is to stop or limit conversations on these platforms.

Online spaces have become the platform for various forms of political expression that many states especially those with authoritarian leanings consider subversive. Governments argue, for example, that social media platforms encourage the spread of rumours which can trigger public unrest.

This was the case in 2016 in Uganda during the country's presidential elections. The government restricted access to social media, describing the shutdown as a "security measure to avert lies … intended to incite violence and illegal declaration of election results".

In Zimbabwe, the government blocked social media following demonstrations over an increase in fuel prices. It argued that the January 2019 ban was because the platforms were being "used to coordinate the violence".

The third strategy, done almost by stealth, is the use of what is generally known as "bandwidth throttling". In this case telecom operators or internet service providers are forced to lower the quality of their cell signals or internet speed. This makes the internet too slow to use.

"Throttling" can also target particular online destinations such as social media sites.

What drives governments

In most cases the desire to control the internet is rooted in governments' determination to control the political narrative. Many see the internet as an existential threat that must be contained, no matter what consequences it will have on other sectors.

The internet is seen as a threat because it disrupts older forms of government political control, particularly the control of information. The stranglehold on the production and dissemination of information has always been an invaluable political tool for many African governments.

The loss of this control, at a time when the media has brought politics closer to the people, presents governments with a distinctly unsettling reality. Social media, for example, inherently encourages political indiscipline and engenders the production and circulation of alternative political narratives.

In addition, because it is a networked platform, users are simultaneously and instantaneously local and international and are engaged in an information carnival that is difficult to police. Quite often the narratives therein are at variance with the self-preserving and carefully constructed ideologies of the state.

The shutdown trend

The irony, however, is that as these shutdowns continue, even proliferate, there is scant evidence they actually work. Instead, they seem to animate dissent and encourage precisely the kind of responses

considered subversive by many governments This has been the case in Burkina Faso and Uganda, for example, where such bans have simply increased the profile of the causes being agitated.

Internet shutdowns don't stop demonstrations. Nor do they hinder the production and circulation of rumours: they encourage them instead. Many people are also circumventing the shutdowns through the use of virtual private networks (VPNs). These are networks that redirect internet activity to a computer in a different geographical location thus enabling access to sites blocked in one's own country. VPNS are now par for the course in countries like Zimbabwe.

The future of unfettered internet access in Africa looks precarious should governments continue on this trajectory. The absence in many African countries of enforceable constitutional guarantees that protect the public's right to information means there are few opportunities for legal redress. This makes the development of legislative regimes that recognise and protect access to the internet both urgent and necessary.

Provided by The Conversation