Welcome to the Era of Internet Blackouts

wired.com/story/cloudflare-internet-blackouts-report

Lily Hay Newman

20 janvier 2023

The Iranian government’s latest attempts in recent months to stifle protests through internet blackouts, digital curfews, and content blocking have presented a particularly extreme example of how far regimes can go in restricting digital access. But a new report from the internet infrastructure company Cloudflare, released today, highlights the stunning global prevalence of connectivity disruptions and their increasing relevance to people and organizations all around the world.

In 2022, Cloudflare began publishing reports that compile its internal observations about government internet blackouts and notable outages worldwide. As a content delivery network that also provides digital resiliency services, the company sees an array of signals when a chunk of the internet goes dark. For example, Cloudflare can assess internet protocol requests, like those for the routing system Border Gateway Protocol or the internet address book Domain Name System, to get insight into how a government executed a shutdown and where in the internet backbone it implemented the connectivity blocking.

The specific geopolitical context and technical nuances of different digital disruptions can make it difficult, or unhelpful, to make granular comparisons of disparate incidents. But Cloudflare, which operates in more than 100 countries and interconnects with more than 10,000 network providers, is using its vantage point and visibility into the global internet to track broader trends and offer a sense of scale about how pervasive internet shutdowns have become.

“There's an increasing use of shutdowns as a means of controlling communication,” says David Belson, Cloudflare's head of data insight and a longtime researcher of internet disruptions. “There are single points of failure for internet connectivity, and things that are outside of your control can impact your business, your organization, your individual collaborations. So if you are someone in a position of responsibility, you may have to start factoring that into your risk matrix and thinking about particular steps to ensure that your presence on the internet and the work you do on the internet remains uninterrupted.”

The new report, which looks at incidents from the fourth quarter of 2022, concluded that activity related to internet disruptions was actually lower, or “a little bit less active,” as Belson puts it, than previous quarters of last year. Still, the report listed intentional shutdowns and disruptions in Bangladesh, Cuba, Iran, Kenya, Pakistan, Sudan, and Ukraine, along with the United states, where Moore County, North Carolina, dealt with multiday internet outages thanks to assailants who shot at two electrical substations, causing power outages. In Ukraine and Iran particularly, Cloudflare's reporting was a continuation of ongoing monitoring and incidents.

An internet shutdown imposed by the Cuban government on October 1 was a continuation of shutdowns that began at the end of September in an attempt to curtail protests. The uprisings came in response to a hurricane that caused power outages on the island nation and a widespread feeling among the public that the Cuban government botched the recovery.

The report also highlights an accidental October cable cut in the UK's Shetland Islands as well as technical failures in Australian, Haiti, and Kyrgyzstan.

“The interesting thing about internet shutdowns is that we typically don't see governments shutting down electricity or water or gas. They target the internet because they see shutting down the flow of information as a vital thing to do,” says John Graham-Cumming, Cloudflare's chief technical officer. “For a lot of us the internet is an essential utility that we can't live without. These things really do have an impact, including an economic impact.”

Graham-Cumming and Belson note that they see increasing government reliance in many places on digital curfews and intermittent, recurring shutdowns—a trend that seems very likely to continue. It has even become common in some countries to impose connectivity blackouts for a few hours a day during university exams, purportedly to reduce the possibility of students cheating. And in places like Ukraine, where connectivity outages are driven by persistent, wartime attacks on critical infrastructure, the impacts are unrelenting and serve as a particularly sobering illustration of this new digital normal.