Life behind a VPN as shutdowns reshape Uganda's Internet use

Uganda once again demonstrated remarkable consistency by switching off the internet during elections, repeating a tradition last observed in 2016 and 2021.

This well-rehearsed routine continues to raise important questions, mostly about whether the shutdown itself is now part of the electoral process, and how long a country can keep calling this temporary while repeating it every five years.

Unfortunately, the internet is not like a simple light switch that can be switched on and off without consequences. Shutting it down disrupts long established network routes that are built dynamically over time by routing algorithms.

Even after restoration, networks take time to stabilise, leading to degraded performance, slow services, and broken digital experiences. The long-term technical cost of repeated shutdowns is rarely discussed, yet each disruption weakens trust in the reliability of Uganda's digital infrastructure.

Uganda's digital ecosystem has grown too complex, too essential, and too interconnected to be repeatedly switched off.

Rodney H. Adriko
Internet shutdown

In technology, there is a common principle: If a system is working, do not interfere with it unnecessarily.

When social media is blocked, VPNs become the default utility for netizens to access the internet. However, this shift has introduced new risks. Many users downloaded unverified VPN applications, some of which carry malware or harvest personal data. Sensitive personal and financial information is now being routed through unknown foreign servers, exposing citizens to data leakage, fraud, and surveillance. This is a pattern that is going to continue as the Uganda Communications Commission (UCC) makes effort to block all VPN applications and netizens also work hard to find new ones.

There are also practical side effects such as increased battery drain, device overheating, and unstable connections. One user on X joked that phones were overheating because they were suddenly forced to connect to servers in desert countries in the Middle East.

Financial transactions conducted over VPNs especially banking and mobile money carry elevated risk. In attempting to control online spaces, authorities may have inadvertently pushed citizens into a far less secure digital environment. As such, it won't be surprising if we begin to see an increased in fraudulent activities on user accounts. Efforts by the UCC to block VPNs are neither sustainable nor effective.

While telecom companies undoubtedly lost revenue during the shutdown, the impact runs much deeper. Digital platforms such as SafeBoda and Jumia were effectively paralysed.

Thousands of riders, delivery workers, traders, and online merchants lost income overnight. Many small businesses simply cannot absorb such losses.

Mobile money and digital financial services were also disrupted, locking people out of loans, savings, and day-to-day transactions.

Agricultural financing tools, WhatsApp-based customer service bots, and informal credit systems all went offline. These are not luxuries; they are core economic lifelines.

The shutdown also affected education and professional life. The cumulative effect is a silent but significant economic setback. In the long run, the state itself bears part of the financial cost.

The normalisation of shutdowns raises an uncomfortable question on whether VPN-mediated internet is becoming the new normal in Uganda.

If so, this represents a quiet erosion of digital sovereignty, user safety, and economic efficiency. Clear legal frameworks, transparent decision-making, and narrowly targeted interventions can address security concerns without dismantling the digital economy.

Internet shutdowns cannot be a recurring policy tool. Uganda's digital ecosystem has grown too complex, too essential, and too interconnected to be repeatedly switched off. Each shutdown breaks more than connections as it breaks trust, opportunity, and progress.