Digital Repression in Tanzania: Investigating Government Led Internet Censorship

Nikhil Bansal
University of Chicago
bansaln@uchicago.edu
Daniel Ngira
University of Chicago
danielngira@uchicago.edu
Matt Ondeyo
University of Chicago
ondeyo@uchicago.edu

Abstract

Tanzania suffered a major internet outage on October 29th, the day of its national elections in 2025. While Tanzanian authorities have yet to admit to an intentional shutdown, the incumbent government's re-election during the shutdown ignited political tension across the country and has led many Tanzanian citizens to believe that the internet outage was a deliberate move by the government to stifle political discourse. We seek to answer whether potential alternative hypotheses, such as a deep-sea cable outage like the one that occurred in Kenya during a similar period of political unrest in 2024, could explain the brief internet shutdown in Tanzania. We will be borrowing from the methodology of Georgia Tech's IODA project report on the 2024 outage in Kenya and performing a deep dive into more granular historical data using the OONI MAT. We hypothesize that non-localized alternative hypotheses such as deep-sea cable outages are likely untrue, as the outage was observed exclusively within Tanzania.

1 Introduction

In the last decade, cases of internet shutdowns have been used as a tool for digital repression in Sub-Saharan Africa. Governments have increasingly restricted connectivity during moments of political tension, particularly during national elections. The frequency of shutdowns rose from 12 incidents in 2017 to 25 in 2019 [2]. Tanzania has popped up as a major player in this trend. On October 29th, 2025, the country experienced a nationwide disruption that affected mobile data and major social media platforms. This event was confirmed by real-time network telemetry from NetBlocks, which noted a steep drop in traffic on the morning of the election [3]. These disruptions happened during protests over restrictive electoral conditions and the suppression of opposition candidates, which reinforced concerns that connectivity controls are being used as a tool of political containment instead of ensuring public safety.

These actions signal a larger pattern in Tanzania's digital governance landscape. In recent years, authorities have introduced increasingly stringent forms of online regulation. The Electronic and Postal Communications (Online Content) Regulations of 2017 have criminalized content that is deemed "indecent," "obscene," or "disruptive to public order". This categorization grants authorities a wide scope for censorship and has already resulted in arrests for anti-government expression [1]. These regulations require all online content creators, including bloggers and YouTubers, to register and pay licensing fees, and have been used to justify actions such as the suspension of Mwananchi Communications' digital division in 2024 for posting an animated video about political abductions [1]. Government framing of these policies as "child protection" measures has been widely criticized as a pretext for broader censorship. As the Global Network Initiative notes, even mainstream platforms such as WhatsApp, X, and Instagram were rendered inaccessible during the election period [4].

The stakes of such shutdowns extend far beyond freedom of expression. Tanzania's 2016 ICT Policy places the internet as essential infrastructure for economic development, financial inclusion, and employment, with a national goal of achieving 80 percent broadband access by 2025 [2]. The country's informal sector, which represents 76 percent of the na-

tional workforce, relies heavily on mobile phones, mobile money, online marketplaces, and app-based services [2]. Previous analyses show that even short disruptions hinder business operations, interrupt digital payments, reduce advertising reach, and constrain the functioning of electronic fiscal devices used for tax collection.

Given Tanzania's position as the home of Dar-es-Salaam, one of East Africa's largest financial hubs, the effects of a nationwide shutdown spill across borders. Internet disruptions interfere with regional commerce, international banking, and trade logistics. Meanwhile, concerns about state surveillance, intercepted communications, and politically motivated arrests further contribute to an environment in which digital repression shapes civic behavior [3]. In this context, our study conducts an empirical analysis of the October 2025 Tanzanian internet shutdown, combining OONI web-connectivity tests, IODA outage measurements, and cross-national comparison to assess the intentionality, scope, and impact of state-imposed connectivity restrictions. Our analysis contributes to ongoing debates about digital authoritarianism, electoral integrity, and the economic and political consequences of network disruptions.

2 Related Work

Existing work on internet shutdowns in Africa spans several domains, including political repression, digital censorship, human rights, and economic impact. Studies have noted the rise in internet connectivity restrictions by African governments, especially during election cycles or episodes of civil unrest. For example, comparative analyses of shutdowns in Uganda, Ethiopia, Zimbabwe, and Togo highlight how governments strategically time disruptions to suppress mobilization and information-sharing ("Internet Blockings and Government Revenue: Case Study Tanzania"). Similarly, work by civil society groups such as NetBlocks and the Business & Human Rights Resource Centre provides real-time documentation of shutdowns, including traffic anomalies and platform-specific blocking patterns, which has been instrumental in verifying the October 2025 Tanzanian disruption ("Business and Human Rights Center").

Research on Tanzania specifically shows a pattern of regulations aimed at controlling digital spaces. Reports from TechCabal highlight the shutdown of more than 80,000 websites in 2025 and earlier cases of punitive actions against journalists and content creators under the Electronic and Postal Communications (Online Content) Regulations of 2017, which necessitate the licensing of online publication and criminalize broad categories of speech ("TechCabal"). These findings align with broader analyses of digital repression across the continent, where policies ostensibly intended to regulate harmful or illegal content are leveraged to silence dissent.

From a human rights perspective, the Global Network Initiative documents instances in which entire platforms like WhatsApp, Instagram, and X were made inaccessible in Tanzania during politically sensitive periods ("GNI Statement on the Nationwide Internet Shutdown in Tanzania"). Research on online participation under censorship further suggests that such blocks significantly alter user behavior, suppress political speech, and disrupt civil society networks. Economic analyses of internet shutdowns in Africa remain limited, but the existing work emphasizes the substantial financial consequences of connectivity restrictions. The SSRN study "Internet Blockings and Government Revenue: Case Study Tanzania" employs an interrupted time-series model to demonstrate that while Tanzania's 2015 election (no shutdown) saw increases in tax and total revenue, the 2020 shutdown coincided with reductions in revenue, disruption of VAT collection, and impaired functionality of electronic fiscal devices. Related work on the "internet economy" (Barua et al., Blinder, Kogut) highlights how digital connectivity drives productivity, financial inclusion, and informal sector growth. This suggests that shutdowns disrupt economic fundamentals rather than isolated digital platforms.

The technical analyses of outages use network measurement frameworks such as OONI and IODA to differentiate between deliberate government interference and alternative explanations like submarine cable failures. A recent Georgia Tech IODA report on the 2024 Kenya outage provides a methodological template for this approach, comparing cross-country signals to rule out cable damage. Our study applies a similar technique, referencing IODA's cross-national dashboards to compare Tanzania's traffic patterns with those of Kenya, Mozambique, and Somalia, none of which experienced comparable disruptions during the same window ("IODA: The Kenya June 25, 2024 Internet Disruption").

By bringing together economic, political, and network-measurement perspectives, the literature shows that shutdowns are rarely technical accidents. Instead, they are complex political interventions with measurable social, civic, and economic costs. Our study builds on these works by combining platform-specific blocking evidence from OONI, country-level reachability data from IODA, and regional comparative analysis to evaluate the intentionality and broader implications of Tanzania's October 2025 shutdown.

3 Results

Our first step in performing this analysis was to determine the exact time that the outage occurred. We analyzed

data from Georgia Tech's IODA database and found that the outage occurred from around noon on October 29th (election day) to noon on November 1st. In Figure 1, we see there was a brief 2-hour return of internet connectivity around noon on October 30th (a day after the elections), but the outage soon returned.

Internet activity on these graphs is naturally cyclical over the course of the day, as internet traffic typically downcycles during late night hours and upcycles during daylight hours. We can see that active probing and the number of unique source IPs completely craters at noon, which is typically when internet activity would reach its peak in Tanzania.

Figure 2, shows that the region that reported the highest outage score by IODA's metrics was Dar-Es-Salaam, the largest city in Tanzania and a major financial hub in East Africa. We suspect that it is not necessarily because Dar-Es-Salaam was uniquely targeted for the shutdown, but rather because it is one of the areas in Tanzania with the highest level of internet usage. Figure 3 shows the areas impacted by the outage in Tanzania.

Kenya is a bordering East African country (in fact, bordering one of the regions in Tanzania that reported one of the highest outage reporting) but did not receive a similar disruption in the same time period. In the IODA article analyzing the veracity of the deep-sea cable claim for Kenya's internet disruption last year, IODA mentions that they noticed a similar disruption in the internet service for Tanzania (which helps validate the claim that the PEACE and DARE cables were disrupted rather than internet service intentionally being shut down). However, figure 7 shows that we did not observe a similarly major disruption in Kenya, Mozambique, or Somalia even though they're connected via deep sea cables using TeleGeography's map

Our next step was to perform platform-specific connectivity testing using OONI, which mirrors the data trends seen in the IODA analysis. Regarding Twitter.com, figure 4 shows a high volume of anomalies on election day. This was followed by an apparent post-election outage that resulted in a scarcity of test data and a substantial number of confirmed failures on November 3 and 4.

We observed comparable patterns in the WhatsApp connectivity tests. Similar to the Twitter data, we detected a marked increase in anomalies on election day as we can see in figure 5. This instability persisted post-election, characterized by a significant volume of anomalies recorded from November 3 through November 5.

A similar pattern emerges with Signal, a platform designed for private and secure communication. However, in this instance, we observed confirmed failures, in addition to anomalies as shown in figure 6, both leading up to and on election day, culminating in a subsequent service outage

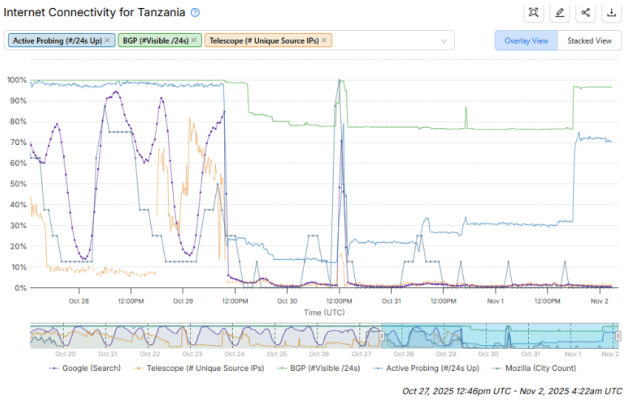


Figure 1: IODA time series for Tanzania around the 2025 election, showing a sharp drop in reachability consistent with a nationwide shutdown.

4 Conclusion

Our analysis strongly suggests that the internet disruption observed in Tanzania from October 29 to November 1, 2025, was a deliberate, state-sponsored shutdown rather than a technical failure or deep-sea cable outage. By leveraging data from Georgia Tech's IODA project, we established that the outage was geographically isolated to Tanzania. Unlike the 2024 disruption in Kenya (where simultaneous outages in neighboring countries corroborated a subsea cable failure) our cross-reference of network traffic in Kenya, Mozambique, and Somalia during this period showed no comparable anomalies. Furthermore, OONI connectivity data revealed a targeted pattern of censorship: specific platforms (Twitter, WhatsApp, Signal) experienced distinct blocks and "throttling" anomalies that coincided precisely with the election timeline and subsequent political unrest. This granular targeting of communication tools, particularly those offering encryption (Signal, WhatsApp), further indicates a strategic intent to stifle political discourse and coordinate surveillance rather than a generalized infrastructure failure.

Based on these findings, several remedial and preventive actions are necessary to protect digital rights in the regions. Organizations such as the Zaina Foundation and international watchdogs must continue to preserve forensic network data (like the IODA and OONI traces collected in this report). This evidence is critical for filing legal challenges against the Tanzania Communications Regulatory Authority (TCRA) and for supporting potential sanctions by the African Commission

Figure 2: A ranking of interaet outage scores per city in Tanzania

on Human and Peoples' Rights (ACHPR). Service providers like Signal and Meta (WhatsApp) are uniquely equipped to implement censorship-resistant routing (such as domain fronting) for users in high-risk regions. Additionally, these platforms should publish real-time transparency reports confirming traffic drops to publicly refute government denials of interference.

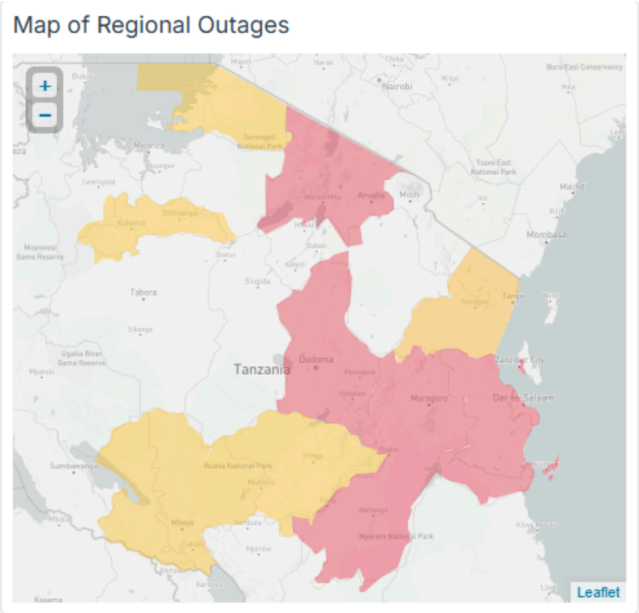


Figure 3: A map of regional internet outages in East Africa

References

[1] Kenn Abuya. *Tanzania removes 80K online platforms in major digital crackdown.* https://techcabal.com/2025/05/06/tanzania-removes-80000-online-platforms/. Accessed December 10, 2025. 2025.

[2] Francis Stephen Nyonzo. *Internet Blockings and Government Revenue: Case Study Tanzania.* SSRN working paper. DOI: 10.2139/ssrn.4695755. 2025. URL: https://ssrn.com/abstract=4695755.

[3] Matshepo Sehloho. *Tanzania: Government imposes nationwide internet restrictions amid election day protests.* https://www.business-humanrights.org/en/latest-news/tanzania-government-imposes-nationwide-internet-restrictions-amid-election-day-protests/. Accessed December 10, 2025. 2025.

[4] Shreya Tewari. *GNI statement on the nationwide internet shutdown in Tanzania during the 2025 elections.* https://globalnetworkinitiative.org/gni-statement-on-the-nationwide-internet-shutdown-in-tanzania-during-the-2025-elections/. Accessed December 10, 2025. 2025.

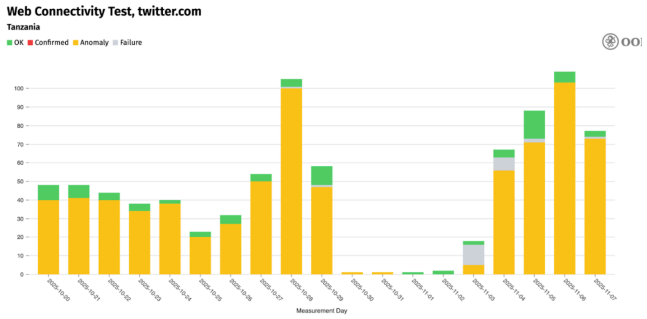


Figure 4: OONI data showing Twitter's connectivity in Tanzania from 20th November, 2025 - 7th Decemeber, 2025

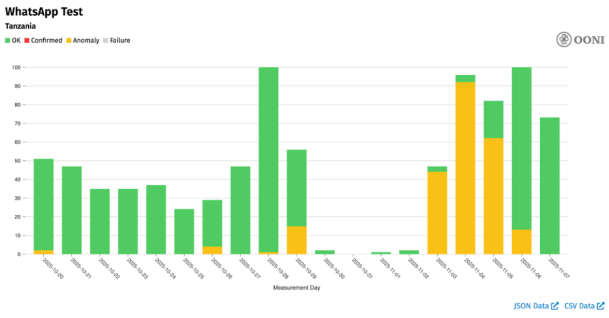


Figure 5: OONI data showing WhatsApp's connectivity in Tanzania from 20th November, 2025 - 7th Decemeber, 2025

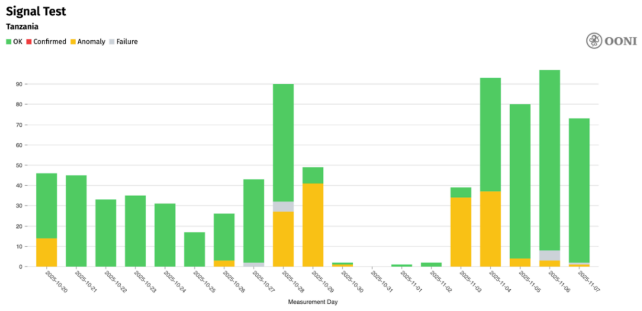
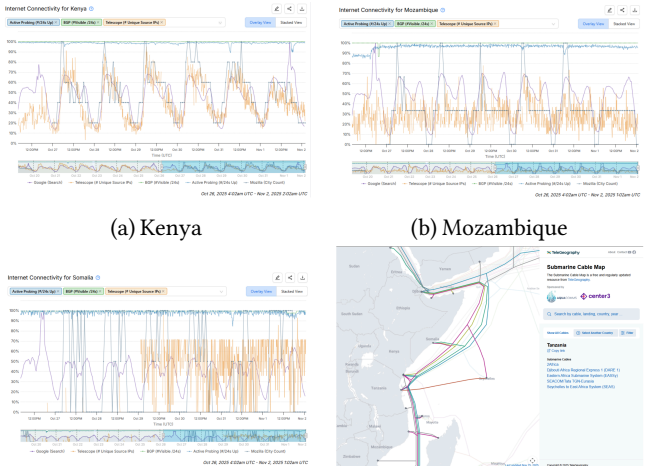


Figure 6: OONI data showing Signal's connectivity in Tanzania from 20th November, 2025 - 7th Decemeber, 2025



(a) Kenya (b) Mozambique

(c) Somalia (d) Cable map

Figure 7: Regional connectivity around Tanzania's 2025 shutdown and the underlying cable topology.