

# Expert Opinion on the Blocking of the X Social Media Platform in Tanzania

By the Open Observatory of Network Interference  
(OONI) Foundation

July 2025

## Table of Contents

Introduction	2
Summary of Findings	3
About OONI	3
OONI's Internet Measurement Methodology	5
Web Connectivity experiment	5
Data analysis	6
OONI measurements from Tanzania	8
Findings: Blocking of X social media platform in Tanzania	9
Blocking of X in Tanzania	10
Network variances	12
Airtel Tanzania (AS37133)	12
Vodacom Tanzania Ltd (AS36908)	13
Tanzania Telecommunications Co. Ltd (AS33765)	13
Zanzibar Connections Company Limited (AS327714)	15
A note on IP-based blocking	15
Conclusion	16

## Introduction

Access to the [X](#) social media platform (formerly known as Twitter) has [reportedly been blocked](#) on networks in Tanzania since May 2025. This document provides an Expert Opinion by the [Open Observatory of Network Interference \(OONI\) Foundation](#) on this block.

[OONI](#) is a nonprofit organization with global expertise on Internet censorship, having built free software tools for measuring Internet censorship since 2012. OONI hosts the [world's largest open dataset on Internet censorship](#) of its kind, consisting of more than 2 billion measurements collected from 29,000 unique networks across 242 countries and territories. Since OONI measurements are collected from the edge of the network, they provide unique insights into the accessibility or blocking of Internet services and can serve as evidence of Internet censorship.

The following sections of this document share further information about OONI, their measurement methodologies, and OONI measurement coverage in Tanzania. More importantly,

the following sections share relevant OONI data and technical analysis that serves as evidence of the ongoing blocking of the X social media platform in Tanzania.

## Summary of Findings

OONI data suggests that access to the social media platform X has been [blocked](#) in Tanzania since 20th May 2025.

Unlike [previous blocks](#) in Tanzania (which were implemented more consistently across ISPs), OONI data [shows variance](#) in terms of the *networks* on which the blocking of X is observed (the block is not observed on all tested networks), the *dates* when the block started on different networks (while most ISPs appear to have started the block around 20th May 2025, others only started blocking X in June 2025), and the *censorship techniques* adopted by ISPs to implement the block.

Overall, access to X appears to be **blocked through a variety of different techniques depending on the ISP**. [OONI data](#) indicates that certain ISPs in Tanzania employ several censorship techniques at different layers at the same time — such as DNS hijacking, TLS interference, and IP level blocks — suggesting a “[defense in depth](#)” **approach to censorship**. This represents a shift in the implementation of internet censorship in Tanzania, with blocking methods becoming increasingly sophisticated and difficult to bypass.

## About OONI

This Expert Opinion on the blocking of the X social media platform in Tanzania is provided by the [Open Observatory of Network Interference \(OONI\) Foundation](#) (hereafter referred to as “OONI”). OONI is a nonprofit organization, legally registered in Rome, Italy, with global operations and extensive global expertise in Internet censorship.

Having pioneered crowdsourced methods for measuring Internet censorship, OONI is a leader in the internet measurement field. OONI won the [2012 Access Now Freedom of Expression Tech Prize](#) for actionable ideas on how to use information technology to promote and enable human rights and deliver social good. More recently, OONI received the [Free and Open Communications on the Internet \(FOCI\) 2023 Community Award](#).

Since 2012, OONI has developed [OONI Probe](#), a free and open source software designed to [measure various forms of Internet censorship](#), including the [blocking of websites](#). Each month, volunteers run [OONI Probe](#) in [around 170 countries](#), including [Tanzania](#), where users have contributed [more than 5 million network measurements from 47 local networks](#) in recent years. By default, OONI automatically publishes network measurements submitted by OONI Probe

users worldwide as [open data in real-time](#). With over 2 billion network measurements collected from 29,000 unique Autonomous Systems (ASes) across 242 countries and territories since 2012, OONI maintains the [world's largest open dataset on Internet censorship](#) of its kind.

More specifically, OONI works on the following:

- **Free and open source tools for measuring internet censorship.** Since 2012, OONI has developed [free and open source software](#) designed to measure various forms of Internet censorship. Through their [OOONI Probe app](#), anyone can [measure](#) the blocking of websites and collect network measurement data in real-time that can serve as evidence.
- **Real-time open data on internet censorship.** OONI maintains the [largest open dataset on Internet censorship](#) to date. As soon as anyone runs [OOONI Probe](#) anywhere around the world, their test results are automatically published by OONI as [open data](#) in real-time. To enable researchers to investigate Internet censorship, OONI provides an [API](#) for downloading the raw data in JSON format, a [web platform](#) (“OOONI Explorer”) for searching through OONI measurements, and a [Measurement Aggregation Toolkit \(MAT\)](#) for generating charts based on aggregate views of OONI data.
- **Research on internet censorship based on OONI data.** OONI has published [more than 75 reports](#) documenting Internet censorship around the world based on the analysis of OONI data. These include a [technical multi-stakeholder research report on Internet shutdowns in Iran](#), facilitated by the European Commission and the United States government. OONI presented this report to members of the Trade and Technology Council (TTC) and to EU Member States of the High Level Group on Internet Governance (HLIG).
- **Partnerships on the study of Internet censorship.** Since 2016, OONI has established [more than 50 partnerships](#) with leading digital rights organizations worldwide to study Internet censorship. These include research collaborations with academic institutions like the [Oxford Internet Institute at the University of Oxford](#) and [Georgia Tech](#), as well as with prominent global nonprofits such as the [Internet Society \(ISOC\)](#).

Over the past decade, OONI data has supported third-party research on Internet censorship in [Iran](#), [Egypt](#), [Malaysia](#), the [Philippines](#), [India](#), [Venezuela](#), [Rwanda](#), [Uganda](#), [Lebanon](#), [Myanmar](#), [Azerbaijan](#), [Ukraine](#), [Russia and Crimea](#) (among many other countries). Freedom House has [cited](#) OONI data in many of their annual Freedom on the Net country reports. OONI data has also supported academic papers, such as research on [China's DNS censorship](#), global [CDN geoblocking](#), global [I2P censorship](#), and on the [deployment of network censorship filters at a global scale](#).

[Harvard's Berkman Klein Center](#) integrated OONI data into their [AccessCheck](#) project. [Internet Society \(ISOC\)](#) includes OONI data in their [Pulse Internet Shutdowns](#) project, which provides a timeline of blocking events and internet shutdowns around the world. Journalists worldwide also

rely on OONI data when reporting on emerging censorship events. For example, OONI data is cited in articles by major news outlets such as [Wired](#), [BBC](#), [CNN](#), [CBC News](#), [CNET](#), [The Intercept](#), [Wall Street Journal](#), [Deutsche Welle](#), [Taggesspiegel](#), [Mada Masr](#), [Al Araby](#), [Time](#), and [Africa Times](#), among many others.

## OONI's Internet Measurement Methodology

Overall, OONI measures Internet services in a crowdsourced way through network-level [experiments](#) run by [OONI Probe app](#) users in [around 170 countries](#) each month. Each of these experiments has a different methodology, all of which are [publicly documented](#). Since these experiments are run from local network vantage points, they offer **unique insights into the accessibility or blocking of Internet services at the edge of the network**. OONI publishes OONI Probe test results (“measurements”) from around the world as [open data](#) in real-time.

To examine the [reported blocking](#) of the X social media platform in Tanzania, OONI analyzed measurements collected from the [OONI Probe](#) testing of the X domains (x.com and twitter.com) in the country. Specifically, OONI analyzed measurements collected from the OONI Probe [Web Connectivity experiment](#), which is designed to measure the blocking of websites.

The following sections explain how the OONI Probe Web Connectivity experiment works, and how OONI performed relevant data analysis.

### Web Connectivity experiment

OONI's [Web Connectivity experiment](#) is designed to measure the blocking of the [websites](#) included in the public, community-curated [Citizen Lab test lists](#), which include domains of the X social media platform (x.com and twitter.com).

Specifically, OONI's Web Connectivity test is designed to measure the accessibility of [URLs](#) by performing the following steps:

- Resolver identification
- DNS lookup
- TCP connect to the resolved IP addresses
- TLS handshake to the resolved IP addresses
- HTTP(s) GET request following redirects

The above steps are automatically performed from *both* the local network of the user, and from a control vantage point. If the results from both networks are the same, the tested URL is annotated as accessible. If the results differ, the tested URL is annotated as [anomalous](#), and the type of

anomaly is further characterized depending on the reason that caused the failure (for example, if the TCP connection fails, the measurement is annotated as a TCP/IP anomaly).

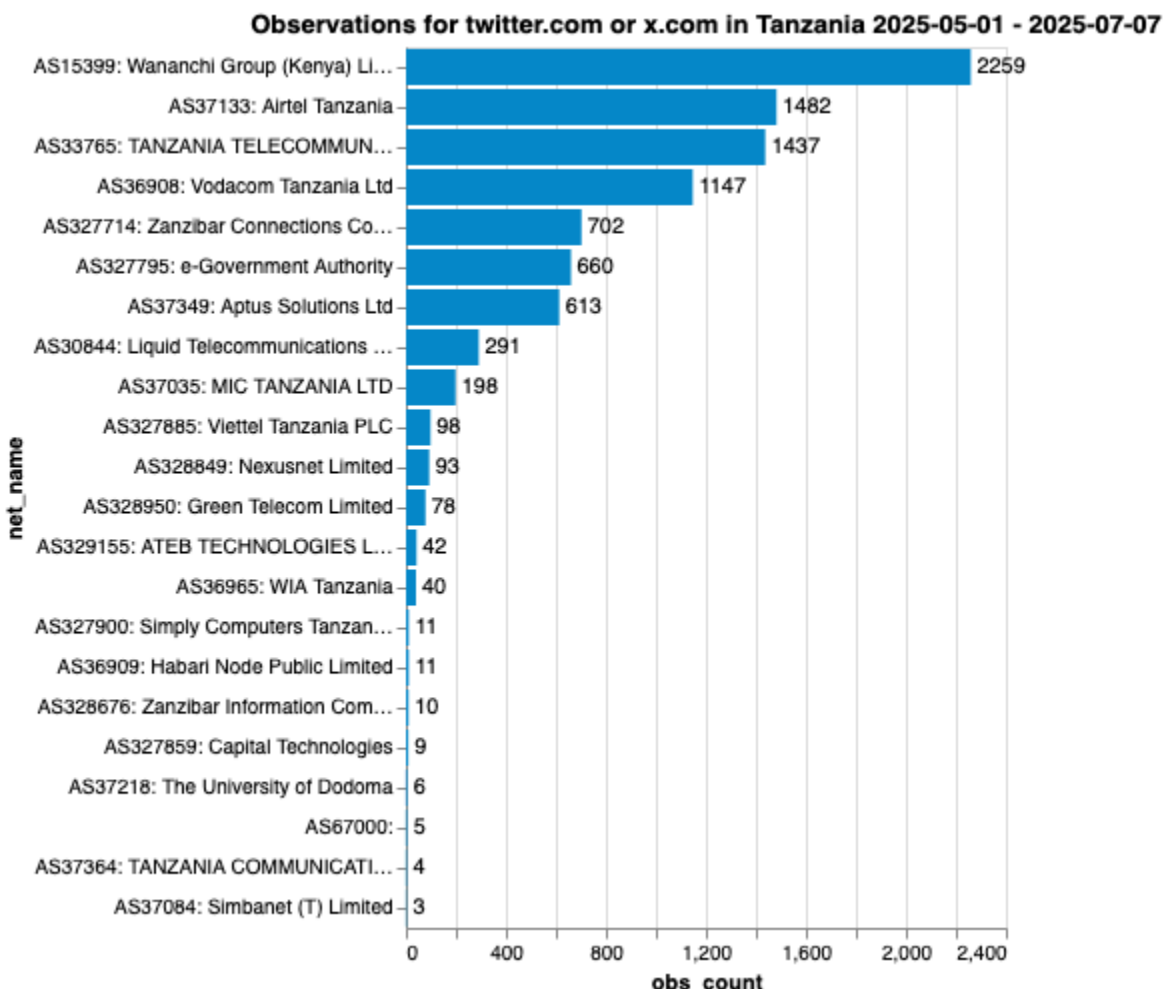
[Anomalous measurements](#) may be indicative of blocking, but [false positives](#) can occur. The likelihood of blocking is therefore greater if the overall volume of anomalous measurements is high in comparison to the overall measurement count – compared on an AS level within the same date range for each OONI Probe experiment type.

Each Web Connectivity measurement provides further network information (such as information pertaining to TLS handshakes) that helps with evaluating whether an anomalous measurement presents signs of blocking. OONI therefore disaggregates based on the reasons that caused the anomaly (e.g. connection reset during the TLS handshake) and if they are consistent, they provide a stronger signal of potential blocking.

Based on their heuristics, OONI is able to automatically confirm the blocking of websites based on [fingerprints](#) if a [block page](#) is served, or if DNS resolution returns an IP known to be associated with censorship. These [blocking fingerprints](#) enable OONI to [automatically confirm website blocks](#) in countries like [Russia](#), [Italy](#), [Kazakhstan](#), [Iran](#), and [Indonesia](#) where ISPs implement blocks with these techniques. For other countries (such as Tanzania) where ISPs implement blocks differently, OONI analyzed anomalous measurements with their [data analysis tool](#) to determine whether those anomalies are symptomatic of blocks.

## Data analysis

To investigate the [reported blocking of X](#) in Tanzania, OONI analyzed [measurements](#) collected from the OONI Probe [Web Connectivity experiment](#) testing of X domains (x.com and twitter.com) on each tested network in Tanzania during the date range of interest: between **1st May 2025 to 7th July 2025**. The analysis was further restricted to networks (ASes) which had a sufficient number of measurements to have a high enough confidence in the findings. While relevant OONI measurements (from the testing of X domains) were collected from a [total of 22 ASes in Tanzania](#) during the analysis period, OONI based their findings on the networks which received the largest measurement coverage and for which the signal for blocking was the strongest.



**Chart:** Number of observations generated from the analysis of OONI measurements pertaining to the testing of X domains (x.com and twitter.com) on all tested networks in Tanzania between 1st May 2025 to 7th July 2025.

As illustrated in the above chart, [most OONI measurement coverage](#) (pertaining to the testing of X domains between 1st May 2025 to 7th July 2025) was collected from the Wananchi Group (AS15399), also [known as Zuku](#), Airtel Tanzania (AS37133), and Vodacom Tanzania (AS36908) networks, informing most of the findings. The notebook used by OONI to perform the data analysis is available [here](#).

In order to perform the analysis more effectively, the raw OONI measurement JSONs were converted into observations and the interpretation of the anomaly from the perspective of the probe (the value of the 'blocking' key in web\_connectivity) was discarded. In doing so, OONI is able to adjust the analysis to the specificity of the blocking patterns seen and improve the accuracy of the findings.

Observations are generated from raw OONI measurement JSONs using the [OONI Pipeline v5](#) and, generally, a given OONI measurement will correspond to multiple observations. An

observation is the outcome of a particular network operation towards a specific target (e.g. “When attempting to perform a TCP handshake to IP address 123.45.67.8 on port 443, we got a connection refused”). These observations are then aggregated by a specific time window (mostly daily) and disaggregated by network (probe\_asn) and/or target (IP address or domain name) and/or DNS resolver configuration.

For the [Web Connectivity](#) measurements, OONI looks at the observations related to the domain names twitter.com or x.com. OONI then inspects the outcome of the DNS resolution, TCP connect, and TLS handshake operations to assess whether these operations are failing consistently in the same way on the same network. HTTPS observations are ignored, since the data format does not enable to distinguish if the error is at the TLS or TCP layer.

## OONI measurements from Tanzania

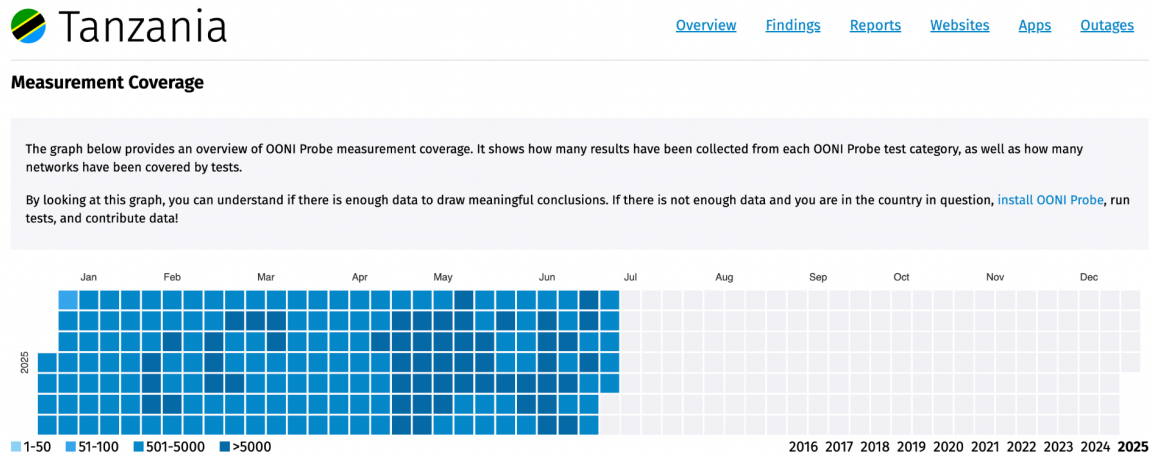
Since 2012, the [Open Observatory of Network Interference \(OONI\)](#) has built free software apps ([OONI Probe](#)) which include [experiments](#) designed to measure various forms of internet censorship, including the [blocking of websites](#) (such as those of the X social media platform). These experiments are run by [OONI Probe](#) users in [around 170 countries](#) (including [Tanzania](#)) every month, testing their networks to detect the blocking of websites and apps. To increase transparency of Internet censorship, OONI publishes OONI Probe test results (“measurements”) from around the world as [open data](#) in real-time.

Since December 2016, [OONI Probe](#) users in Tanzania have contributed [more than 5 million measurements](#) from 47 local Autonomous Systems (ASes). Every day, OONI Probe users in Tanzania continue to [contribute new measurements](#), which OONI publishes in real-time. These longitudinal network measurements – spanning from December 2016 to date – provide insight into the accessibility of tested websites on tested networks in Tanzania.

Over the years, OONI data has shown growing patterns of Internet censorship in Tanzania. In 2020, OONI [documented](#) the blocking of social media platforms ([including Twitter/X](#)) in Tanzania amid the country’s 2020 general election. In April 2024, OONI published a [report](#) documenting the extensive blocking of LGBTQI sites in Tanzania, as well as the blocking of certain websites that support human rights and various online dating websites. OONI has also documented the [blocking of Clubhouse](#), [Grindr](#) and [Proton VPN](#) in Tanzania, as well as the [temporary blocking of the X social media platform](#) in late August 2024. The results of OONI’s analysis previously [showed](#) that most Internet Service Providers (ISPs) in Tanzania appeared to implement blocks by means of TLS interference.

In recent months, OONI measurement coverage in Tanzania has been stable, providing confidence in the findings documented in this report. The following chart illustrates overall

OONI measurement coverage (including results from [all OONI Probe experiments](#)), aggregated from all tested networks in Tanzania between early January 2025 to early July 2025.



**Chart:** Overall OONI measurement coverage aggregated from all tested networks in Tanzania between early January 2025 to early July 2025 (source: [OONI Explorer](#)).

The chart above shows stable OONI measurement coverage throughout the date range of analysis (1st May 2025 to 7th July 2025). The stable and relatively high volume of measurements during the period of interest helps instill confidence in the blocking findings, as it statistically reduces the likelihood of false positives caused by transient network failures.

## Findings: Blocking of X social media platform in Tanzania

Access to the social media platform X has [reportedly been blocked](#) in Tanzania since May 2025, after the official police account was [allegedly hacked](#) to display pornographic content and spread false claims about the president's death.

[OONI data](#) collected from multiple networks in Tanzania corroborates these reports, showing that access to X domains has been blocked on multiple networks in the country since 20th May 2025. Specifically, OONI data shows that access to x.com and twitter.com has primarily been blocked in Tanzania by means of [IP blocking](#), though there are indications of additional censorship techniques (such as [TLS interference](#)) being employed as well. While the block [remains ongoing](#) on several networks in the country, it's worth noting that access to X is [not blocked on all networks](#) in Tanzania.

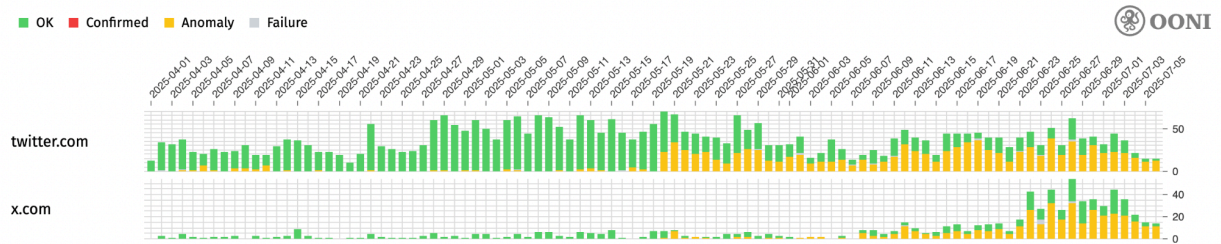
## Blocking of X in Tanzania

The following [chart](#) aggregates OONI measurement coverage from the testing of X domains (twitter.com and x.com) on multiple networks in Tanzania between 1st April 2025 to 7th July 2025.

### Web Connectivity Test, twitter.com, x.com

Tanzania

OK Confirmed Anomaly Failure



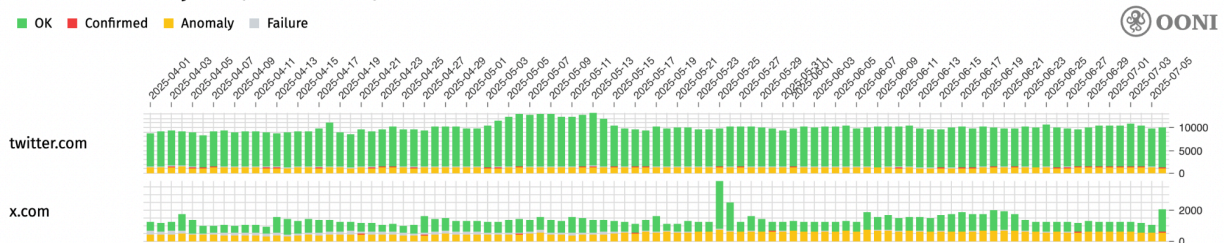
**Chart:** OONI Probe testing of [twitter.com](#) and [x.com](#) on multiple networks in Tanzania between 1st April 2025 to 7th July 2025 (source: [OONI data](#)).

As shown in the chart above, [OONI Probe](#) testing for twitter.com began to show a sharp increase in [anomalies](#) starting on 20th May 2025, suggesting potential blocking. These anomalies persisted and aligned closely with the timeframe [reported](#) by news media regarding the platform's restriction. Although x.com received significantly less testing coverage compared to twitter.com, it also displayed a sustained spike in anomalies during the same period, suggesting a similar disruption.

The hypothesis that X was down globally – as opposed to being blocked locally in Tanzania by ISPs – is ruled out because [global OONI measurement coverage](#) pertaining to the testing of X domains (twitter.com and x.com) shows that they were mostly accessible on tested networks in most countries globally between 1st April 2025 to 7th July 2025, as illustrated below.

### Web Connectivity Test, twitter.com, x.com

OK Confirmed Anomaly Failure

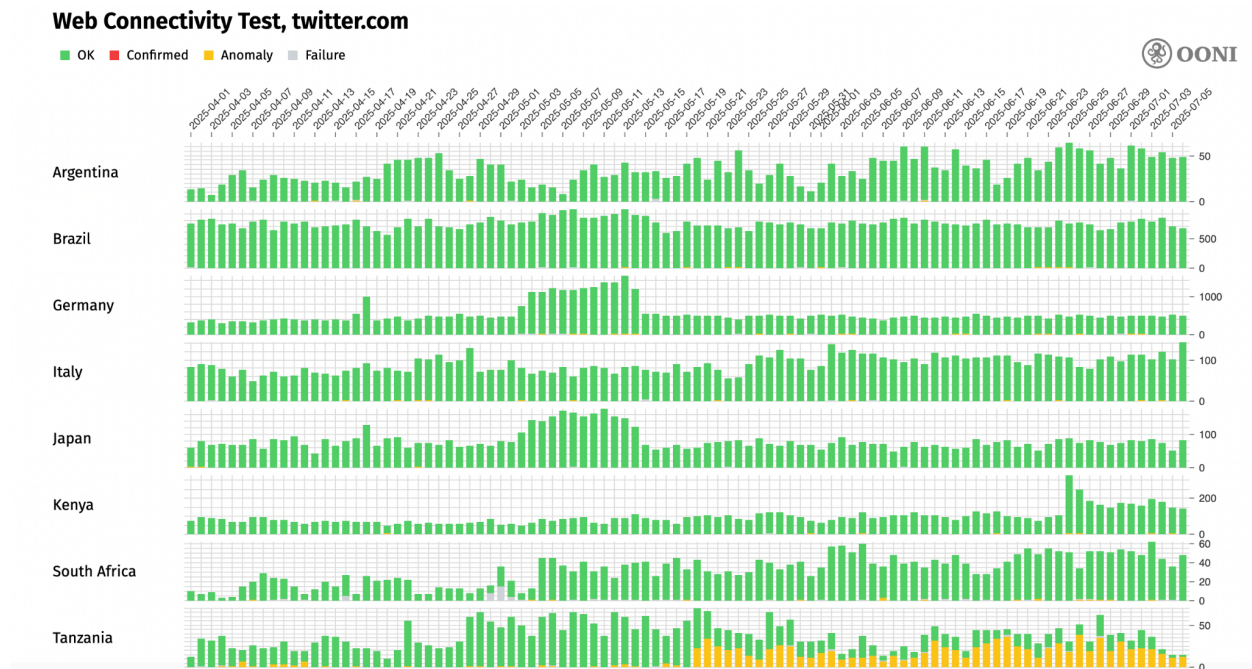


**Chart:** Global OONI Probe testing of twitter.com and x.com between 1st April 2025 to 7th July 2025 (source: [OONI data](#)).

The above chart [shows](#) global OONI measurement coverage pertaining to the [testing](#) of X domains (twitter.com and x.com). If X were down globally, the above chart would have

presented an increase in measurements annotated as “anomalous” because the testing would have failed globally. Instead, the above chart shows that most measurements were “OK”, meaning that it was possible to successfully access X domains from thousands of networks in most countries around the world. X therefore seemed to be globally accessible during the analysis period, suggesting that any restrictions were imposed locally.

This is further evident when disaggregating by country and viewing the OONI Probe testing of twitter.com in Tanzania in comparison to several other countries, as illustrated below.

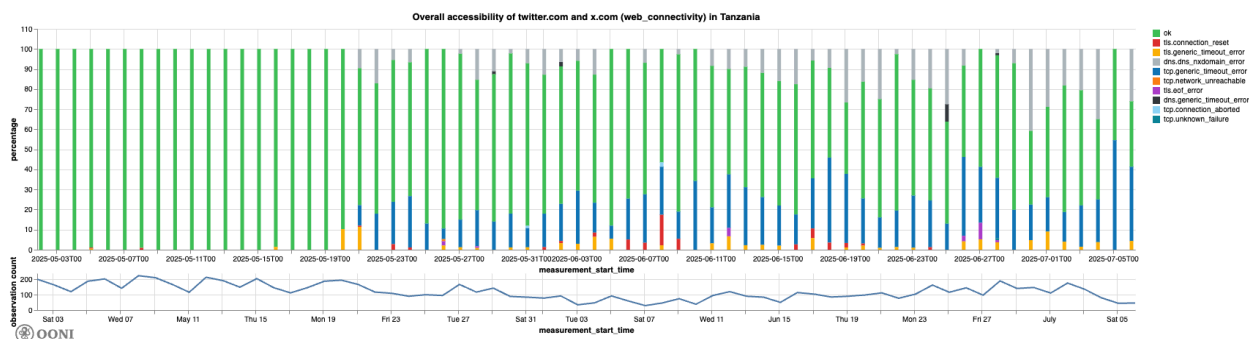


**Chart:** Comparative OONI Probe testing of twitter.com in Tanzania and other countries (Argentina, Brazil, Germany, Italy, Japan, Kenya, South Africa) between 1st April 2025 to 7th July 2025 (source: [OONI data](#)).

To understand whether the [anomalous measurements in Tanzania](#) were symptomatic of censorship, OONI [analyzed](#) relevant measurements. The results of their analysis are presented below.

Starting from 20th May 2025, OONI data [shows](#) an **overall increase in the failure rate** when testing twitter.com or x.com from local networks in Tanzania. The following chart aggregates OONI measurement coverage from the testing of X domains in Tanzania between 1st May 2025 to 7th July 2025, while presenting the specific failures that emerged.

## Expert Opinion by the Open Observatory of Network Interference (OONI) Foundation on the Blocking of the X Social Media Platform in Tanzania



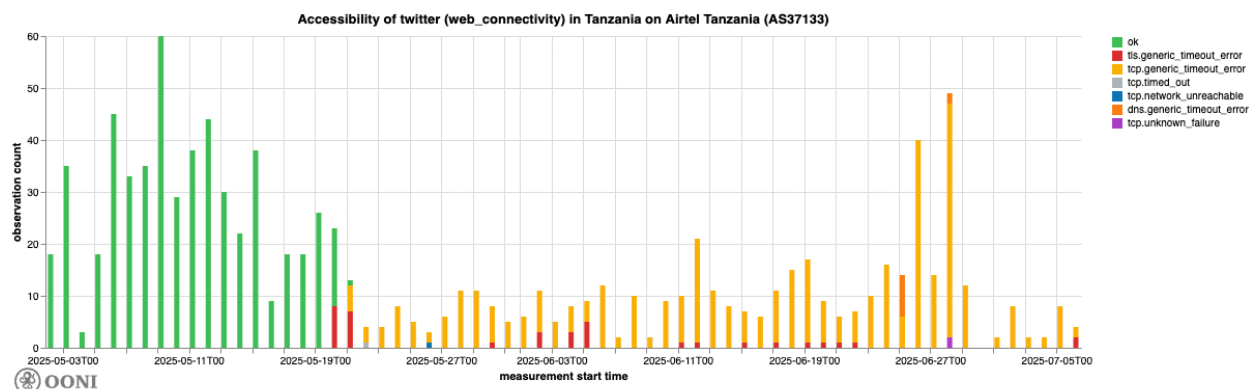
**Chart:** Analysis results from the OONI Probe testing of X domains (twitter.com and x.com) on multiple networks in Tanzania between 1st May 2025 to 7th July 2025 (source: [OONI data](#)).

As illustrated in the chart above, many of the observed failures involved TCP timeout errors, TLS timeout errors, and TLS connection reset errors — indicating that access to X domains was, in some cases, blocked through [TLS interference](#) and, in others, through [IP-level blocking](#). It's worth noting though that throughout this period (between 20th May 2025 to 7th July 2025), some measurements were [successful](#), indicating that access to X domains was *not* blocked on all networks in Tanzania. OONI data shows [variance](#) across ISPs in both the blocking of X domains and the censorship techniques used to enforce the restrictions.

## Network variances

### Airtel Tanzania (AS37133)

Starting from 20th May 2025, OONI data [shows](#) that the testing of X domains (twitter.com and x.com) on Airtel Tanzania (AS37133) primarily resulted in TCP timeout errors (suggesting IP-level blocks), as well as in a few TLS timeout errors.



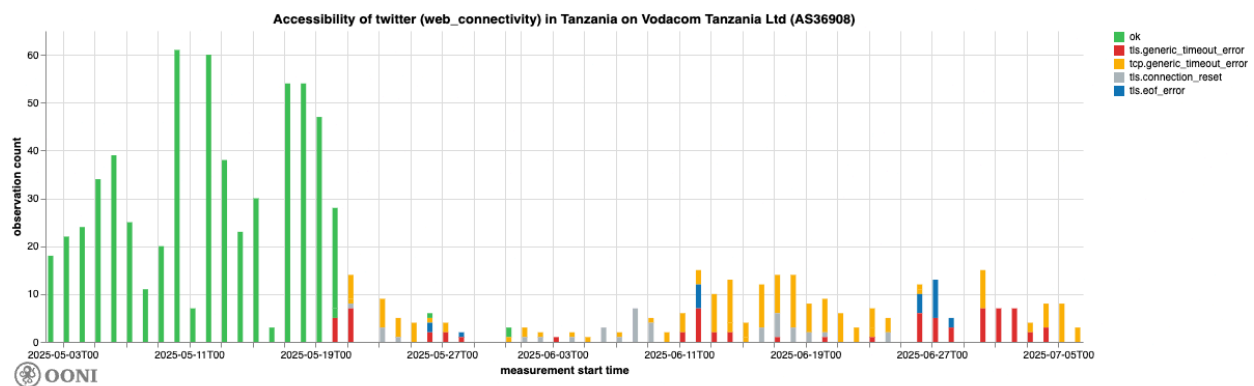
**Chart:** OONI Probe testing of twitter.com and x.com on Airtel Tanzania (AS37133) between 1st May 2025 to 7th July 2025 (source: [OONI data](#)).

When OONI measurement coverage is disaggregated on this network (AS37133) by IP addresses hosting X domains (`162.159.140.229` and `172.66.0.227`) and network types (mobile, WiFi,

VPN, unknown), there is not much difference, suggesting that the block occurred consistently across all IPs and network types.

### Vodacom Tanzania Ltd (AS36908)

Also starting from 20th May 2025, OONI data [shows](#) sustained presence of failures in the testing of X domains (twitter.com and x.com) on Vodacom Tanzania Ltd (AS36908). Many of these failures are TCP timeout errors, suggesting an IP-level block, while some of these failures also suggest TLS level interference.



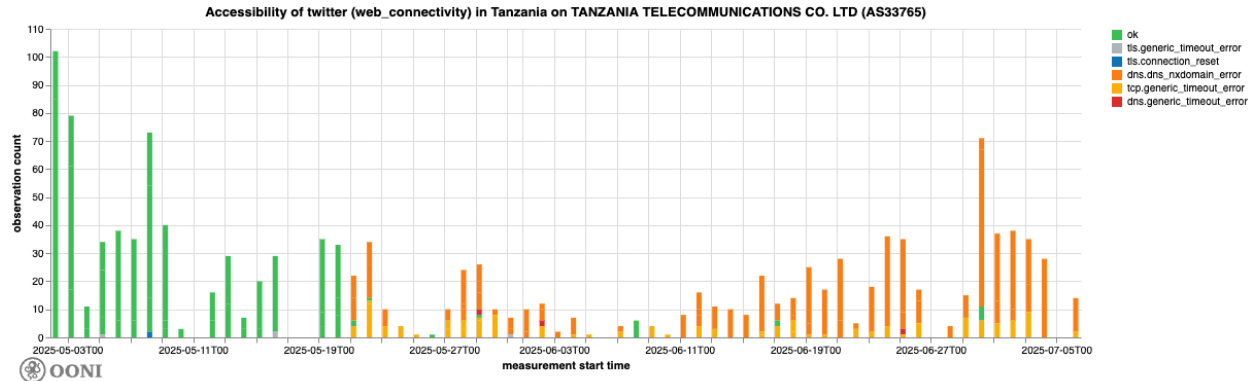
**Chart:** OONI Probe testing of twitter.com and x.com on Vodacom Tanzania Ltd (AS36908) between 1st May 2025 to 7th July 2025 (source: [OONI data](#)).

As part of investigating the variance in failure types observed on this network (AS36908), OONI further disaggregated the measurements by IP address and network type. OONI did not notice any significant difference in distribution of blocking methods depending on the IP or network type. This suggests that Vodacom may be using a variety of different methods to implement the block or that the block is implemented in a way that is not entirely consistent.

### Tanzania Telecommunications Co. Ltd (AS33765)

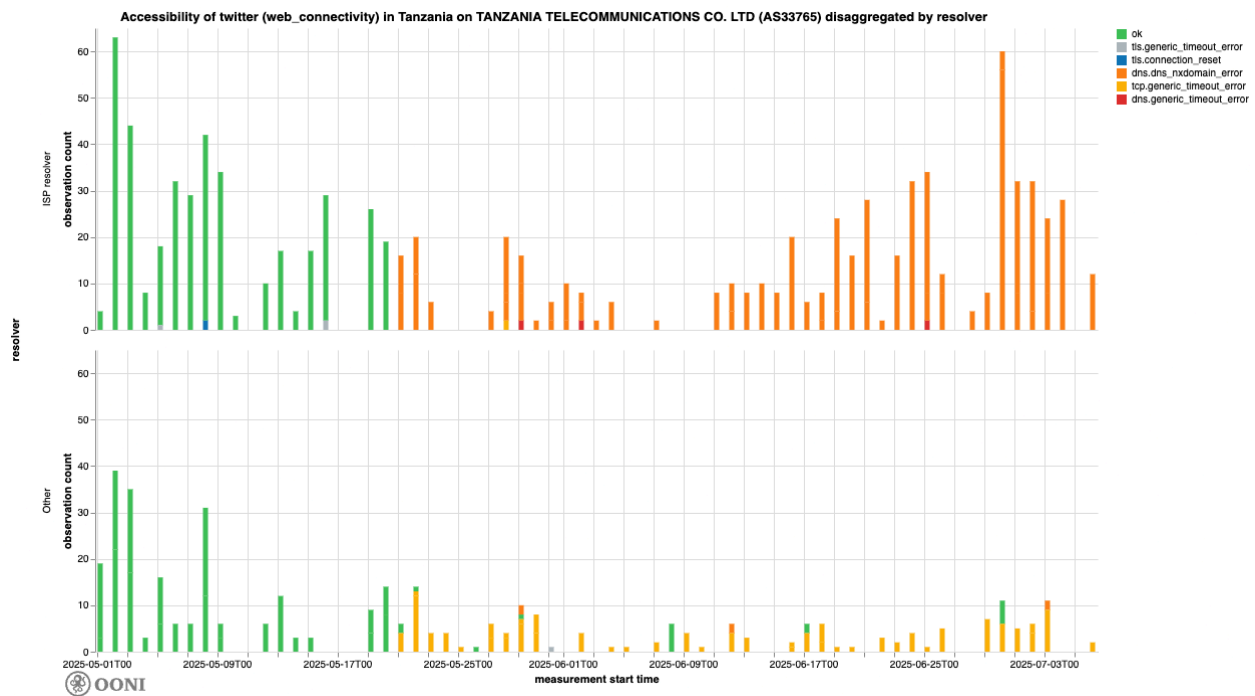
Starting from 21st May 2025, OONI data [shows](#) the blocking of X domains on Tanzania Telecommunications Co. Ltd (AS33765). The failures are a mixture of DNS resolution errors and TCP timeout errors, but there are also a few instances of TLS timeouts and connection resets, as illustrated in the chart below. The presence of a mixture of DNS, TCP and TLS failures seems to suggest the use of a variety of different methods to implement the block.

Expert Opinion by the Open Observatory of Network Interference (OONI) Foundation  
on the Blocking of the X Social Media Platform in Tanzania



**Chart:** OONI Probe testing of twitter.com and x.com on Tanzania Telecommunications Co. Ltd (AS33765) between 1st May 2025 to 7th July 2025 (source: [OONI data](#)).

The following chart disaggregates the observations by the DNS resolver used by the probe. The term “ISP” is used to signify that the probe is configured to use the resolver provided by the Internet Service Provider (ISP), while “Other” signifies that it is using a public resolver (such as Cloudflare or Google DNS).



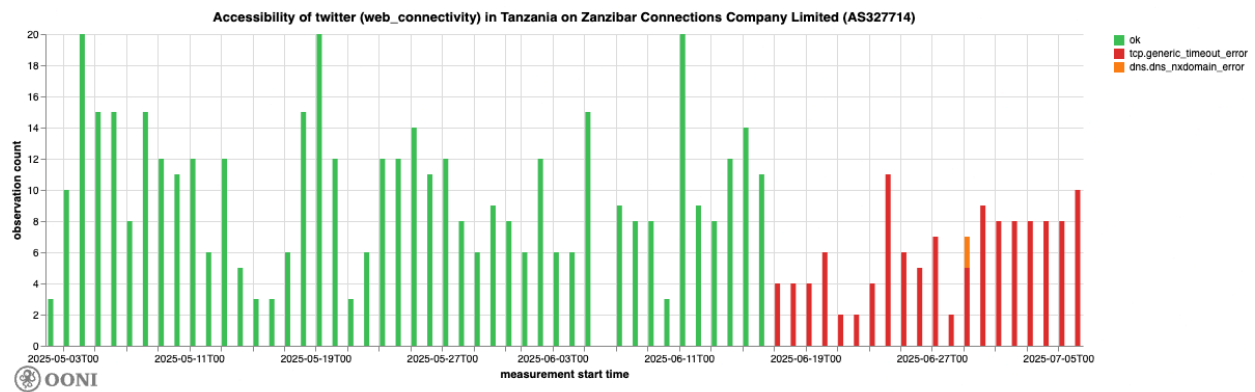
**Chart:** OONI Probe testing of twitter.com and x.com on Tanzania Telecommunications Co. Ltd (AS33765) between 1st May 2025 to 7th July 2025, disaggregated by resolver (source: [OONI data](#)).

From the above chart, it is evident that when the ISP-provided resolver is used, the returned DNS answer is “NXDOMAIN”, suggesting that the resolver is [performing DNS hijacking](#). However, when a third party DNS resolver is used, the site is *still* unavailable – even though the probes get a valid answer – because it is blocked at the TCP level. This suggests that this ISP (AS33765) is

**implementing the block at both DNS and TCP/IP levels**, making it harder for users to circumvent the block (i.e just altering their DNS resolution configuration would not suffice for circumventing the block).

### Zanzibar Connections Company Limited (AS327714)

While OONI data suggests that the [blocking of X in Tanzania started on 20th May 2025](#), the block appears to have been implemented on different dates across various networks in the country. About a month later, starting from 17th June 2025, OONI data shows the [complete blocking](#) of twitter.com and x.com on Zanzibar Connections Company Limited (AS327714), as all subsequent measurements resulted in TCP timeout errors (illustrated in the chart below).




**Chart:** OONI Probe testing of X domains (twitter.com and x.com) on Zanzibar Connections Company Limited (AS327714) between 1st May 2025 to 7th July 2025 (source: [OONI data](#)).


The persistent occurrence of TCP timeout errors in all measurements collected from 17th June 2025 onward strongly indicates that access to X domains on this network was blocked through **IP-based blocking**.

### A note on IP-based blocking

OONI data suggests that the blocking of X is implemented on some networks by means of [IP based blocking](#). This type of blocking method presents the risk of resulting in **unintentional collateral damage** if there are multiple, unrelated, sites or services hosted on the same IP address that is blocked. The specific IPs used by x.com and twitter.com are `162.159.140.229` and `172.66.0.227`, which are owned by Cloudflare.

## Expert Opinion by the Open Observatory of Network Interference (OONI) Foundation on the Blocking of the X Social Media Platform in Tanzania

 **162.159.140.229** • HOST



AS OF 17 JUL 2025 | 11:50 UTC

---

Summary

Reverse DNSNo Data

Forward DNS

www.onewheelwiki.ericgagnon.net, www.jfkihozzpublic.ericgagnon.net, www.thescrapedoctor.com, dev.cftls.t.co.cdn.cloudflare.net, upload.x.com, tweetdeck.x.com, support.x.com, pink.green-service.xyz, echochamber.social, ipv6.ericgagnon.net, test.cftls.t.co.cdn.cloudflare.net, tdapi.x.com, cf.twing.com, ms3.twitter.com, mail.twitter.com, probe.twitter.com.cdn.cloudflare.net, api.x.com.cdn.cloudflare.net, webdisk.ericgagnon.net, jfkihozzpublic.ericgagnon.net, eg2wedding.ericgagnon.net, ethicshelpline.x.com, ton.twitter.com, ads-api.x.com, x.com, shopify-staging.twitterintegration.com, mastodon.metsuke.com, www.ericg5.com, ng5xymyuuv3z2.1.0.7pu4nu2lqpyi4zgdqit3kuq25a.tgrqyon.dns0.org, pro.x.com, about.x.com, syndication.x.com, blog.twitter.com, assets1.twitter.com, analytics.twitter.com, stream.twitter.com, pro.twitter.com, www.tweetdeck.com, distribulous.ericgagnon.net, pro.twitter.com.cdn.cloudflare.net, api.twitter.com.cdn.cloudflare.net, global.cftls.t.co.cdn.cloudflare.net, www.watcher.ericgagnon.net, api-stream.twitter.com, tdapi.twitter.com, shopify.twitterintegration.com, dev.cftls.t.co, cpanel.ericgagnon.net, cpcontacts.ericgagnon.net, cf.x.com, probe.twitter.com, ms1.twitter.com, legacy-api.twitter.com, caps.twitter.com, support.twitter.com, assets2.twitter.com, test.cftls.t.co, ramonageprevost.ericgagnon.net, www.dasdasdsda.ericgagnon.net, jf.twitter.com, static.twitter.com, mobile.x.com, dasdasdsda.ericgagnon.net, mail.ericgagnon.net, partnerstream2.twitter.com, dev.twitter.com, www.twitter.com, ads.twitter.com, td.twitter.com, www.t.co, webmail.ericgagnon.net, api-stream.twitter.com.cdn.cloudflare.net, api.x.com, www.toxicshithole.com, s.twitter.com, downloads.tweetdeck.com, data.twitter.com, ms2.twitter.com, legalrequests-dev.twitter.com, xn--r8jo4a0b.com, mobile.twitter.com, api.twitter.com, about.twitter.com, api.tweetdeck.com, t.co, phyllisbrowning.co, data.green-service.xyz, cf.twitter.com, twitter.com, next.vision-tunnel.com, ton.x.com, blog.tweetdeck.com, onewheelwiki.ericgagnon.net, communitynotes.x.com, tcsgreensafehouse.com, ads-api.twitter.com, payments-staging.twitter.com, ias.x.com, www.notfall-uhr.com, jf-t.x.com, analytics.x.com

**Image:** Forward DNS for 162.159.140.229 as of 17th July 2025 (source: [censys](#)).

As can be seen in the above image, most domains pointing to these IP addresses are related to twitter.com or x.com. Those which are unrelated [show a 1001 error](#) when accessed, which seems to suggest that these IPs are reserved for X related web resources.

So while OONI does *not* currently observe any evidence of potential overblocking, if the DNS and hosting configuration were to change in the future, this method of blocking X could potentially lead to overblocking and unintended collateral damage.

## Conclusion

Access to online information in Tanzania is becoming increasingly restricted. The [ongoing blocking of the social media platform X](#) in Tanzania, which began on 20th May 2025, follows [earlier temporary restrictions during the country's 2020 general election](#) and [again](#) in late August 2024. This recurring censorship of X is part of a broader pattern of digital repression, which includes the [blocking of LGBTQI websites](#), [human rights platforms](#), [online dating services](#), and circumvention tools such as [Proton VPN](#).

While OONI data suggests that [previous blocks in Tanzania were implemented quite consistently](#) across ISPs (with most anomalous measurements showing TLS timeout errors and providing strong signals of TLS interference), the [current blocking of X](#) appears to have been implemented quite differently.

Specifically, OONI data from Tanzania shows **variance** in terms of:

- Which ISPs implemented the blocking of X (as the block is [not observed on all tested networks](#));
- When each ISP started blocking X (OONI data [shows](#) that some ISPs started implementing the block on 20th May 2025, while [others](#) only started blocking X in June 2025);
- Censorship techniques (OONI data suggests that ISPs implemented a combination of various censorship techniques, beyond TLS-level blocks observed in [previous studies](#)).

While OONI data from [Zanzibar Connections Company Limited \(AS327714\)](#) provides a strong and persistent signal of IP-based blocking (as all relevant measurements resulted in TCP timeout errors), other ISPs appear to have implemented the blocking of X using a variety of different censorship techniques. OONI data from [Tanzania Telecommunications Co. Ltd \(AS33765\)](#) suggests that the blocking of X is implemented at both the DNS and TCP/IP level, making it harder for users to circumvent the block (i.e just altering their DNS resolution configuration would not suffice for circumventing the block). Meanwhile, OONI data from [Vodacom Tanzania Ltd \(AS36908\)](#) and [Airtel Tanzania \(AS37133\)](#) shows that most measurements resulted in TCP timeout errors (suggesting IP-level blocks), and that some measurements resulted in TLS timeout errors as well.

It's worth noting that the two IPs (`162.159.140.229` and `172.66.0.227`) that x.com and twitter.com resolve to are Cloudflare IPs, but their blocking does not appear to currently cause collateral damage (as those IPs are reserved for X related web resources). However, this may pose a risk of overblocking in the future if the provider were to change their configuration.

Overall, access to X appears to be **blocked through a variety of different techniques depending on the ISP**. [OONI data](#) indicates that certain ISPs in Tanzania employ several censorship techniques at different layers at the same time — such as DNS hijacking, TLS interference, and IP level blocks — suggesting a “[defense in depth](#)” **approach to censorship**. This represents a shift in the implementation of internet censorship in Tanzania, with blocking methods becoming increasingly sophisticated and difficult to bypass.