Tanzania: Surge in online LGBTIQ censorship and other targeted blocks

OONI

Accessible & Screen Reader Compatible

This report documents the blocking of LGBTIQ websites and other targeted blocks in Tanzania based on the analysis of OONI data.

Maria Xynou (OONI), Mehul Gulati (OONI), Tori Fransis

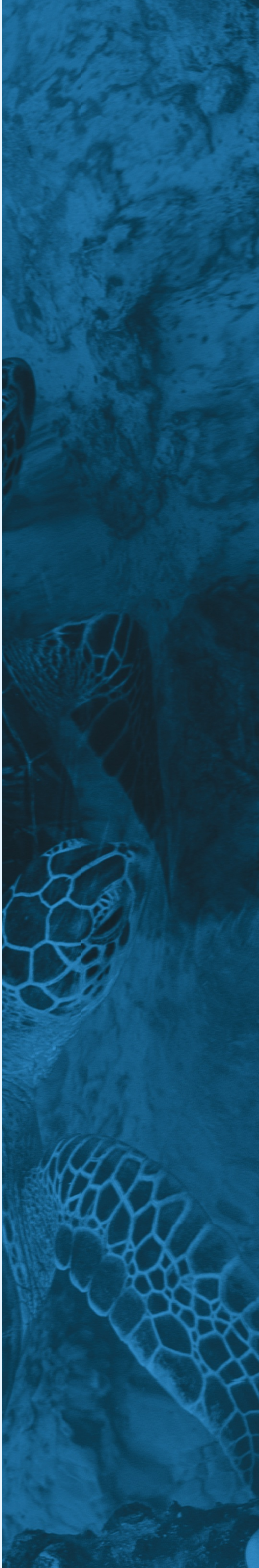
Layout Design: Ura Design

The web version of this report can be accessed here: Web Report

OONI

Publication date: April 11, 2024

Contents



Key Findings

Our analysis of OONI data collected from Tanzania over the last year (between 1st January 2023 to 31st January 2024) reveals the extensive blocking of LGBTIQ sites, which correlates with the escalating discrimination and crackdown on LGBTIQ communities in Tanzania in recent years. Many other blocks identified as part of this study appear to be targeted in nature, as they involve very specific websites, while other (more popular) sites from the same category (e.g. social media, human rights) were found accessible.

Specifically, OONI data collected from Tanzania shows:

- **Blocking of many LGBTIQ websites**, including:
    - LGBTIQ social networks (such as Grindr)
    - LGBTIQ rights (such as ILGA and OutRight International)
    - LGBTIQ news and culture (such as Queerty)
    - LGBTIQ suicide prevention (The Trevor Project)
- **Blocking of online dating websites** (such as Tinder and OKCupid)
- **Blocking of specific websites that defend human rights through grants and petitions** (Change.org, Global Fund for Women, GlobalGiving, Open Society Foundations)
- **Blocking of specific social networking sites** (Clubhouse and 4chan)
- **Blocking of a specific VPN** (ProtonVPN)

The results of our analysis show that most ISPs in Tanzania appear to implement blocks by means of **TLS interference**, specifically by timing out the session after the ClientHello message during the TLS handshake. As the timing of the blocks and the types of URLs blocked are (mostly) consistent across (tested) networks, ISPs in Tanzania likely implement blocks in a coordinated manner (possibly through the use of Deep Packet Inspection technology).

Introduction

Last September, we had the opportunity to attend the Forum on Internet Freedom in Africa (FIFAfrica) 2023 in Dar es Salaam, Tanzania. During the conference, we met participants from Tanzania, who informed us that they had started to experience increased levels of internet censorship in the country in recent months.

As our work centers around the study of internet censorship through the analysis of crowdsourced network measurements collected globally, we were curious to see if we could detect signs of increased levels of internet censorship in Tanzania over the past year — particularly since we hadn't previously observed many blocks in Tanzania in recent years (except for a few cases, such as the blocking of social media during Tanzania's 2020 general elections).

As part of this study, we analyzed OONI network measurement data collected from Tanzania between 1st January 2023 to 31st January 2024. Our goal was to examine whether we could detect signs of internet censorship in Tanzania during this period. As we were mostly interested in cases of internet censorship that would be of public interest and have an impact on human rights, we excluded certain cases (such as the blocking of gambling and adult websites) from the findings presented in this study.

The main questions that informed our analysis of OONI data include:

- Which websites presented signs of blocking in Tanzania between 1st January 2023 to 31st January 2024?
- On which networks do we observe these blocks? How do the blocks vary across networks?
- How do ISPs in Tanzania implement these blocks? Which censorship techniques do ISPs adopt?

We also looked at aggregate views of OONI data from the testing of instant messaging apps (WhatsApp, Facebook Messenger, Telegram) and circumvention tools (Tor and Psiphon). We excluded measurements collected from the testing of Signal because they were impacted by data quality issues over the past year.

The methods and findings of our analysis are shared in the following sections of this report.

Methods

Since 2012, the Open Observatory of Network Interference (OONI) has developed free and open source software (called OONI Probe) which is designed to measure various forms of internet censorship, including the blocking of websites and apps. Every month, OONI Probe is regularly run by volunteers in around 160 countries (including Tanzania), and network measurements collected by OONI Probe users are automatically published as open data in real-time.

OONI Probe includes the Web Connectivity experiment which is designed to measure the blocking of many different websites (included in the public, community-curated Citizen Lab test lists). 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. We therefore consider that the likelihood of blocking is greater if the overall volume of anomalous measurements is high in comparison to the overall measurement count (compared on an ASN 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. We therefore disaggregate 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 OONI's heuristics, we are 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. While this method enables us to automatically confirm website blocking in numerous countries (such as Indonesia, Russia, and Iran), in other countries like Tanzania (where ISPs appear to implement censorship using different techniques), we analyze anomalous OONI measurements with our OONI data analysis tool.

As part of this study, we analyzed OONI network measurement data collected from Tanzania between **1st January 2023 to 31st January 2024**. Specifically, we limited our analysis to Web Connectivity measurements because we were primarily interested in investigating the blocking of websites, while aggregate views from the testing of WhatsApp, Facebook Messenger, Telegram, Tor and Psiphon did not present significant volumes of anomalies during the testing period (therefore not warranting more advanced analysis, which is generally aimed towards understanding whether anomalies are false positives or signs of blocking). As mentioned previously, we excluded measurements from the testing of Signal because they were impacted by data quality issues over the past year.

We aggregated anomalous Web Connectivity measurements collected from Tanzania based on failure types ("dns", "tcp_ip", "http-failure", "http-diff") to evaluate if they were consistently present (or if the types of failures varied), as a more consistent failure type observed in a larger volume of measurements provides a stronger signal of blocking. Most of the anomalous measurements presented "http-failures", signaling that the anomalies were triggered by some failure during the HTTP experiment. We further analyzed these failures to detect the specific errors (such as "connection_reset_error" or "generic_timeout_error") that would enable us to characterize potential blocking, and we aggregated the errors to examine whether and to what extent they were consistent across (relevant) measurements on each tested ASN.

This involved analyzing the network information from TLS handshake data in these measurements to evaluate whether the errors were a result of TLS based interference. For example, a measurement may show that DNS resolution returned consistent IPs, that it was possible to establish a connection to resolved IPs, but that the TLS handshake session timed out after the first ClientHello message (which is unencrypted), resulting in a "generic_timeout_error". While we would consider that such a measurement shows signs of potential TLS based interference, we would not draw conclusions from a single measurement alone.

We therefore aggregated the errors to determine whether a large percentage of anomalous measurements for a tested URL presented the same error (e.g. "tls_timeout_error") in comparison to the overall measurement volume on a specific network, within a specified date range. The higher the ratio of consistent errors (from anomalous measurements) in comparison to the overall measurement count, the stronger the signal (and the greater our confidence) that access to the tested domain is (a) blocked, and (b) blocked in a specific way (e.g TLS interference).

As part of our analysis, we excluded cases which provided weak signals. Those included cases with small/limited measurement coverage (in comparison to the overall measurement coverage on a tested ASN during the analysis period), a low percentage of anomalies (in comparison to the overall measurement volume for a tested service on a network), a relatively large proportion of inconsistent failure types and errors, as well as cases which were determined to be false positives based on known bugs or other issues (such as global failure rates as a result of tested services being hosted on unreliable servers, or measurements collected from unreliable networks). Once we started to develop a strong signal on how blocks were implemented in Tanzania (in this study, we found that "tls.timeout_errors" were present in the vast majority of anomalous measurements), we started to consider measurements with different errors as weaker signals (considering them likely false positives). As a result, the findings of this study are limited to measurements that we considered to present stronger signals based on our analysis methods.

Acknowledgement of limitations

The findings of this study present several limitations, including:

- **Date range of analysis.** The findings are limited to OONI measurements collected from Tanzania between 1st January 2023 to 31st January 2024. As a result, findings from measurements collected in different date ranges are excluded from this study.

- **Type of measurements.** The findings mainly involve OONI Web Connectivity measurements, pertaining to the testing of websites for censorship. As a result, findings from other OONI Probe experiments (particularly those that don't measure the blocking of websites and apps) are excluded from this study.

- **Tested websites.** The testing is mostly limited to URLs included in two Citizen Lab test lists: the global list (including internationally-relevant URLs) and the Tanzanian list (only including URLs relevant to Tanzania). As these lists are tested by OONI Probe users and there are bandwidth constraints, they are generally limited to around 1,000 URLs. As a result, the lists may exclude other websites which might be blocked in Tanzania, and the findings are limited to the testing of the URLs included in these lists. Given that the lists are community-curated, we acknowledge the bias in terms of which URLs are added to the lists.

- **Testing coverage of websites.** Not all URLs included in test lists are measured equally across Tanzania over time. Whether OONI data is available for a particular website depends on whether, on which networks, and when an OONI Probe user in Tanzania tested it. As a result, tested websites received different testing coverage throughout the analysis period, which impacts the findings.

- **Tested ASNs.** While OONI Probe tests are regularly performed on multiple ASNs in Tanzania, not all networks are tested equally. Rather, the availability of measurements depends on which networks OONI Probe users were connected to when performing tests. As a result, the measurement coverage varies across ASNs throughout the analysis period, impacting the findings.

- **Blocking signals.** As part of our data analysis, we limited our findings to signals that we considered more reliable and indicative of government-commissioned censorship, while excluding cases viewed as presenting weak signals (as discussed previously in the "Methods" section). As a result, we acknowledge the risk of potentially having missed some blocking cases in our findings (if those cases were annotated with weak signals as part of our data analysis).

Findings

Our analysis of OONI measurements collected from Tanzania between 1st January 2023 to 31st January 2024 reveals the blocking of specific social networking sites (Clubhouse and 4chan), specific sites that defend human rights through grants (such as GlobalGiving and Global Fund for Women) and petitions (Change.org), online dating sites (such as Tinder), as well as the blocking of ProtonVPN.

Notably, OONI data sheds light on the extensive blocking of LGBTIQ sites in Tanzania. The blocked websites include LGBTIQ social networks (such as Grindr), sites that defend LGBTIQ rights (such as ILGA and OutRight International), LGBTIQ news and culture (such as Queerty), and an LGBTIQ suicide prevention site (The Trevor Project).

All of these blocks are observed on multiple networks in Tanzania during the analysis period. OONI data shows that on most networks, the blocks are implemented by means of **TLS interference**, as we observe the timing out of the session after the ClientHello message during the TLS handshake. This consistent blocking technique – observed on multiple networks – gives us confidence in the findings, and suggests that ISPs in Tanzania may be using Deep Packet Inspection (DPI) technology to implement the blocks.

Further details are shared in the following sections of this report.

Blocking of LGBTIQ websites

LGBTIQ rights are severely limited in Tanzania. Consensual same-sex sexual acts are criminalized under sections of Tanzania's colonial-era Penal Code, with the maximum sentence involving life imprisonment. According to the International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA), LGBTIQ people in Tanzania face legal barriers to freedom of expression and freedom of association, while the Constitution of Tanzania does not explicitly protect LGBTIQ people against discrimination. Moreover, ILGA notes that laws in Tanzania do not offer protection for LGBTIQ people against discrimination in the provision of goods and services, health, education, employment, or housing. ILGA also notes that laws in force in Tanzania neither aggravate penalties for crimes committed on the basis of "sexual orientation", "gender identity", "gender expression" or "sex characteristics" nor do they explicitly consider such crimes as "hate crimes".

In recent years, LGBTIQ communities in Tanzania have faced increased discrimination and violence. Human Rights Watch reported that the government's crackdown on health care services – such as by closing drop-in centers that provided HIV testing – has had a severe impact on LGBTIQ communities in Tanzania. According to OutRight International, Tanzania's government began a concerted crackdown on LGBTIQ people in July 2016, and the state of LGBTIQ people's human rights in Tanzania has rapidly deteriorated since.

In 2018, the Regional Commission for Dar es Salaam vowed to set up a task force to arrest people suspected of being gay, reportedly resulting in members of Tanzania's LGBT community fearing for their lives, hiding in their homes, and fleeing the country. In response, the UN High Commissioner for Human Rights expressed alarm, warning that such a task force could "turn into a witch-hunt and be interpreted as a license to carry out violence, intimidation, bullying, harassment and discrimination against those perceived to be LGBT".

According to Human Rights Watch, international pressure led the Tanzanian government to disavow the official's comments regarding the task force, but institutional homophobia remained, and the deputy home affairs minister called for arrests of LGBT people in September 2019. In April 2023, Milembe Suleiman, an openly lesbian Tanzanian woman, was brutally murdered and mutilated in a suspected homophobic attack.

Without legal protections and within a climate of discrimination, LGBTIQ communities in Tanzania are increasingly experiencing limits to their rights on the internet as well. Last year, the government reportedly started cracking down on websites and social media accounts that promote LGBTIQ rights, reducing online engagement by LGBTIQ people out of fear of prosecution.

As part of this study, we analyzed OONI network measurements from the testing of LGBTIQ websites in Tanzania between 1st January 2023 to 31st January 2024. We found numerous LGBTIQ websites blocked, including LGBTIQ social networks (such as Grindr), sites that defend LGBTIQ rights (such as ILGA and OutRight International), LGBTIQ news and culture (such as Queerty), and an LGBTIQ suicide prevention site (The Trevor Project). Further details are shared in the following sections.

LGBTIQ social networks

OONI data collected from Tanzania suggests that access to at least 3 LGBTIQ social networking sites is blocked, starting from early 2023. Specifically, OONI data shows that access to Grindr (`www.grindr.com`), Romeo (`www.planetromeo.com`), and Hornet (`hornet.com`) is blocked.

The following chart aggregates OONI measurement coverage from the OONI Probe testing of Grindr (`www.grindr.com`), Romeo (`www.planetromeo.com`), and Hornet (`hornet.com`) on multiple networks in Tanzania between 1st January 2023 to 31st January 2024.

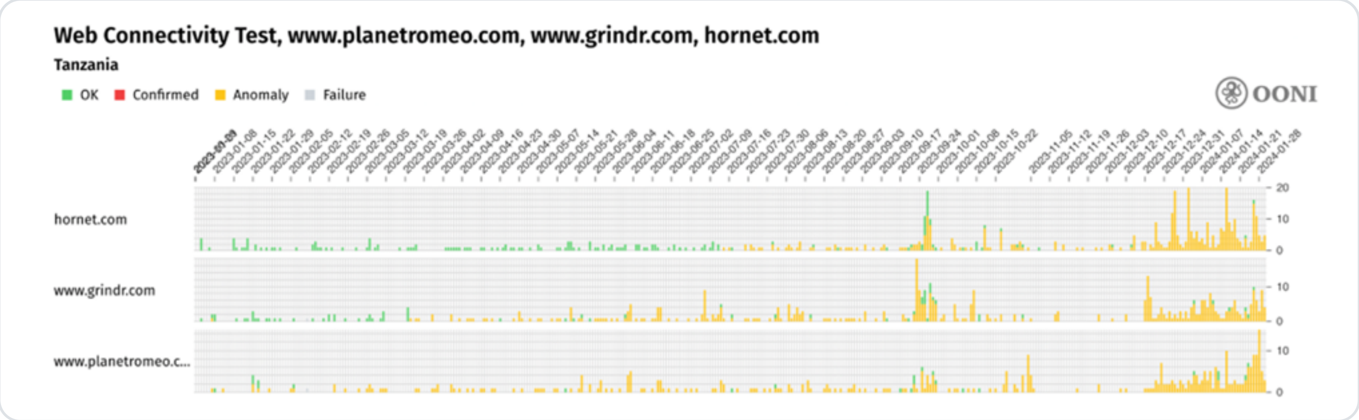


Chart: *OONI Probe testing of Grindr (`www.grindr.com`), Romeo (`www.planetromeo.com`), and Hornet (`hornet.com`) in Tanzania between 1st January 2023 to 31st January 2024 (source: OONI data).*

As is evident, the vast majority of measurements collected from the testing of these 3 domains presented anomalies, presenting a signal of blocking. However, it's worth noting that the overall measurement coverage was rather limited (presenting a limitation to the findings), and we only observe a stable increase in the measurement volume from December 2023 onwards (as well as a temporary spike in measurement coverage in September 2023). Yet, the fact that most measurements (collected from multiple networks) throughout the testing period presented anomalies suggests that access may have been interfered with.

To explore further, we analyzed these measurements to identify the reasons that triggered the anomalies (which would help with characterizing potential blocks) and to rule out false positives. The results of our analysis are presented through the following chart.

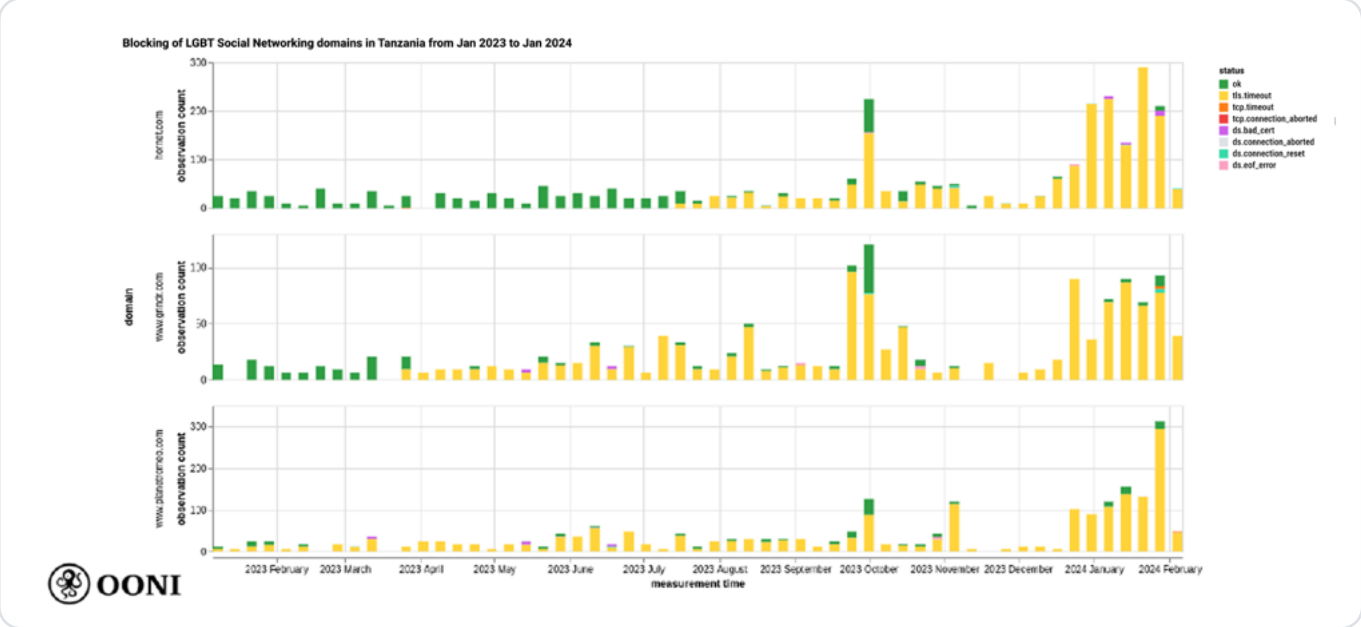


Chart: *Blocking of LGBTIQ social networking sites in Tanzania between 1st January 2023 to 31st January 2024 (source: ooni/data tool).*

The above chart provides a weekly aggregation of OONI measurements collected from the OONI Probe testing of `www.grindr.com`, `www.planetromeo.com`, and `hornet .com` in Tanzania between 1st January 2023 to 31st January 2024. Specifically, it provides the detailed results of the measurements, showing that the vast majority of anomalous measurements (i.e. those that are not annotated as "OK") presented `tls.timeout` errors. As part of our analysis, these errors involve cases where TCP connections to resolved IPs are successful, but the TLS handshake fails (resulting in a TLS timeout error). And more specifically, in these cases, OONI data shows the timing out of the session after the ClientHello message during the TLS handshake. Such cases provide signals of TLS level interference.

During the analysis period, we first start to observe TLS timeout errors in the testing of `www.planetromeo.com` on 7th January 2023, while we start to observe such errors on 21st March 2023 in the testing of `www.grindr.com`. On 14th July 2023, we started to observe signs of TLS interference in the testing of `hornet.com` as well. From then onwards, most measurements collected from the testing of these 3 domains consistently presented the same signs of blocking: TLS interference (involving TLS handshake timeouts).

Given that we consistently observe that the testing of Grindr (`www.grindr.com`), Romeo (`www.planetromeo.com`), and Hornet (`hornet.com`) result in the same errors (on multiple networks) over a long period of time, OONI data provides a strong signal of blocking. Recent OONI data suggests that these blocks remain ongoing.

We previously reported on the blocking of Grindr in Tanzania. OONI data also shows the blocking of Grindr in several other countries, including Jordan, Lebanon, Iran, Turkiye, Indonesia, Pakistan, Qatar, and the United Arab Emirates.

LGBTIQ rights

OONI data suggests that access to multiple websites that defend and promote the rights of LGBTIQ communities are blocked in Tanzania.

Specifically, OONI data suggests that (at least) the following **12 domains** defending LGBTIQ rights were blocked in Tanzania during the testing period:

- lgbtvoicetz.org
- outrightinternational.org
- ilga.org
- www.ilga-europe.org
- lgbt.foundation
- lalgbtcenter.org
- transequality.org
- itgetsbetter.org
- www.glsen.org
- www.familyequality.org
- pflag.org
- www.stonewall.org.uk

Each of the above domains links to relevant OONI data, showing that the OONI Probe testing of those domains presented a large volume of anomalies during the testing period (between 1st January 2023 to 31st January 2024), providing a signal of blocking. To evaluate whether these anomalies were symptoms of censorship or false positives, we analyzed OONI data to identify the reasons why these anomalies emerged. The results of our analysis are presented in the following chart, which provides a weekly aggregation of OONI measurement coverage for the above 12 domains between January 2023 to January 2024.

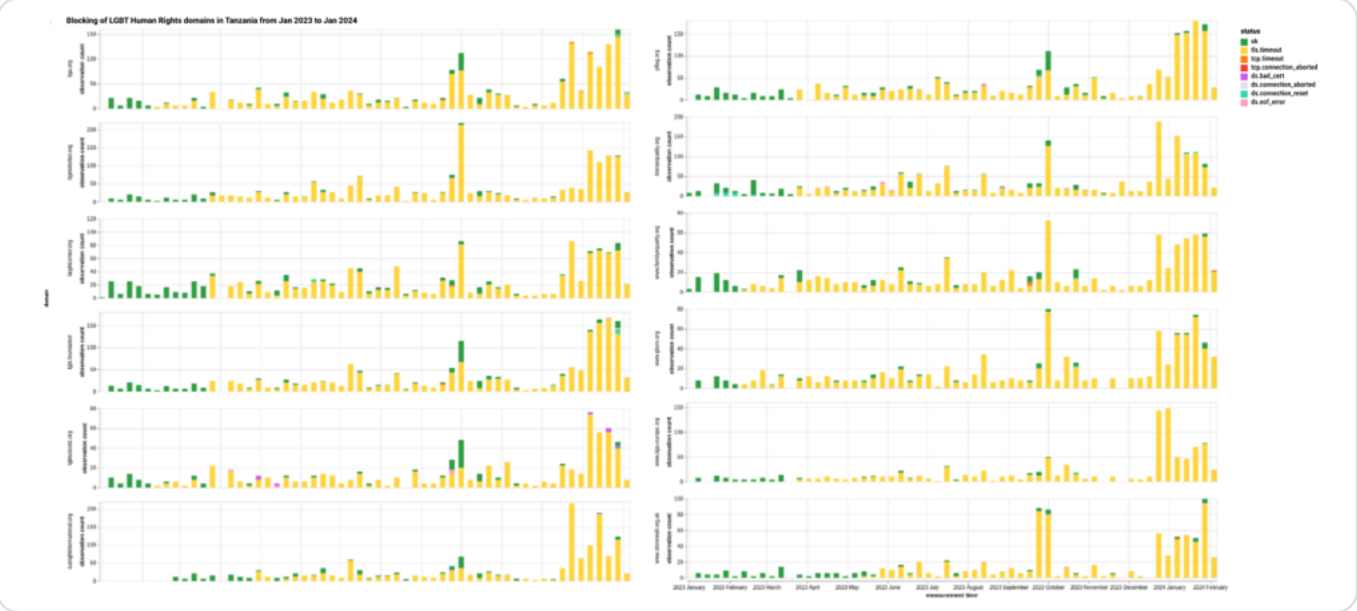


***Chart:** Blocking of domains defending LGBTIQ rights in Tanzania between 1st January 2023 to 31st January 2024 (source: ooni/data tool).*

Similarly to the blocking of LGBTIQ social networking sites (discussed previously), we observe that the vast majority of anomalous measurements presented `tls.timeout` errors throughout the testing period. In these cases, OONI data shows the timing out of the session after the ClientHello message during the TLS handshake, providing signals of TLS level interference. As the type of failure (`tls.timeout`) is consistent throughout the testing period on multiple networks in Tanzania (for multiple domains), the measurements provide a strong signal of blocking.

It's worth highlighting that while OONI data suggests that these domains were previously accessible (annotated in green as "OK" in the above chart), most of the domains in the above chart started to present signs of TLS interference between February 2023 to March 2023. This coincides with the timing of the Grindr block (which appears to have started on 21st March 2023, according to OONI data), suggesting that ISPs in Tanzania may have received orders to block (more) LGBTIQ sites around that time.

Notably, the blocked domains include **LGBT Voice Tanzania** (lgbtvoicetz.org), which has worked to advance equality, diversity, education, and justice for LGBT people in Tanzania since 2009. As part of their work, they protect and promote LGBTIQ human rights in Tanzania through political advocacy, they provide health care support (such as through a free LGBT Clinic Project), and they provide free legal aid and emergency support for LGBTIQ communities in Tanzania (among other services and activities). OONI data suggests that ISPs in Tanzania started blocking access to their website on 7th February 2023.

The blocked domains also include those of international LGBTIQ rights organizations. These include OutRight International, an international non-profit organization defending LGBTIQ rights globally since 1990, and which has recognized consultative status at the United Nations. OutRight International works at a global, regional and national level to eradicate the persecution, inequality and violence lesbian, gay, bisexual, transgender, intersex, and queer (LGBTIQ) people face around the world. OutRight builds capacity of LGBTIQ movements, documents human rights violations, advocates for inclusion and equality, and holds leaders accountable for protecting the rights of LGBTIQ people everywhere. We previously collaborated with OutRight International on a study that examined the blocking of LGBTIQ websites in 6 countries. During the analysis period, OONI data suggests that ISPs in Tanzania started blocking access to `outrightinternational.org` on 25th April 2023.

The blocked domains also include those (ilga.org and www.ilga-europe.org) of the International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA), which is a worldwide federation of more than 1,900 organizations from over 160 countries and territories campaigning for lesbian, gay, bisexual, trans and intersex human rights. Established in 1978, ILGA World has ECOSOC consultative status at the United Nations. During the analysis period, OONI data suggests that ISPs in Tanzania started blocking ilga.org on 7th February 2023, and that they started blocking `www.ilga-europe.org` on 23rd March 2023.

Beyond the 12 blocked domains included in the above chart, the following **5 additional domains** also presented a large volume of anomalies during the testing period:

- lambdalegal.org
- www.glaad.org
- lgbtmap.org
- www.hrc.org
- www.nclrights.org

However, we have excluded these cases from the key findings presented in the above chart because even though these sites are hosted on HTTPS, they were only tested on HTTP – limiting our ability to accurately characterize their blocking (i.e. detect TLS based interference). Therefore, the measurements pertaining to the above 5 domains cannot show whether TLS interference occurred (as that would require testing websites on HTTPS), but they do show that the HTTP experiments resulted in timeout errors, which is consistent with the type of error observed for blocked domains hosted on HTTPS.

Even though our ability to characterize and confirm the blocking of the above 5 domains is limited (because they were tested on HTTP), the following factors provide signals of blocking:

- **Volume of anomalies:** They presented a large volume of anomalies throughout the analysis period;
- **Start date of anomalies:** They started to present anomalies during the same period (February 2023 to March 2023) as the other 12 blocked domains listed in the previous chart;
- **Type of error:** The presence of timeout errors during the HTTP experiment is consistent with the types of errors observed when (other) blocked domains are measured on HTTPS (timeout errors during TLS handshake).

It is therefore very possible that lambdalegal.org, www.glaad.org, lgbtmap.org, www.hrc.org, and www.nclrights.org were blocked in Tanzania as well during the testing period.

LGBTIQ news and culture

OONI data suggests that access to at least 5 LGBTIQ news and culture domains (`afterellen.com`, `www.mambaonline.com`, `www.globalpride2020.org`, `www.out.com`, `www.queerty.com`) were blocked in Tanzania during the analysis period.

The following chart aggregates OONI measurement coverage from the OONI Probe testing of these domains on multiple networks in Tanzania between 1st January 2023 to 31st January 2024.

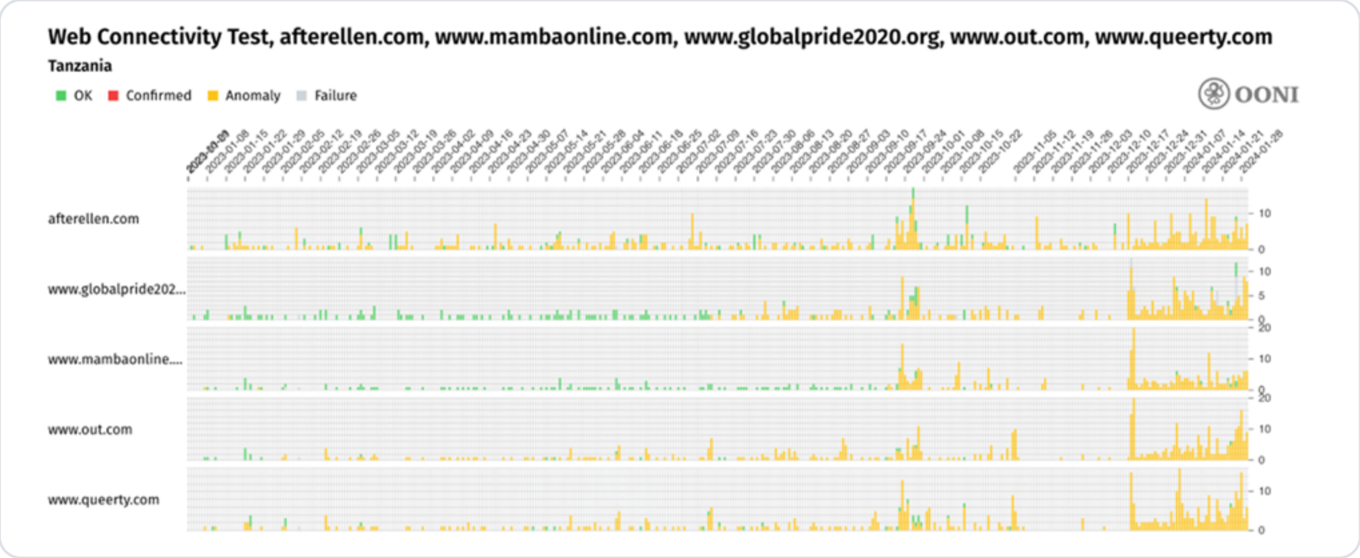


Chart: *OONI Probe testing of `afterellen.com`, `www.mambaonline.com`, `www.globalpride2020.org`, `www.out.com`, `www.queerty.com` in Tanzania between 1st January 2023 to 31st January 2024 (source: OONI data).*

As is evident from the above chart, these 5 domains presented a large volume of anomalies in recent months (providing a signal of blocking), but they each started to present anomalies at different times. During the testing period, the testing of afterellen.com started to present anomalies on 3rd January 2023, the testing of www.queerty.com started to present anomalies on 7th January 2023, the testing of www.out.com started to present anomalies on 5th February 2023, the testing of www.globalpride2020.org started to present anomalies on 14th July 2023, and the testing of www.mambaonline.com started to present anomalies on 18th September 2023.

We analyzed these anomalous measurements to determine the reasons that triggered the anomalies, characterize potential blocks, and rule out false positives. The results of our analysis are presented through the following chart.

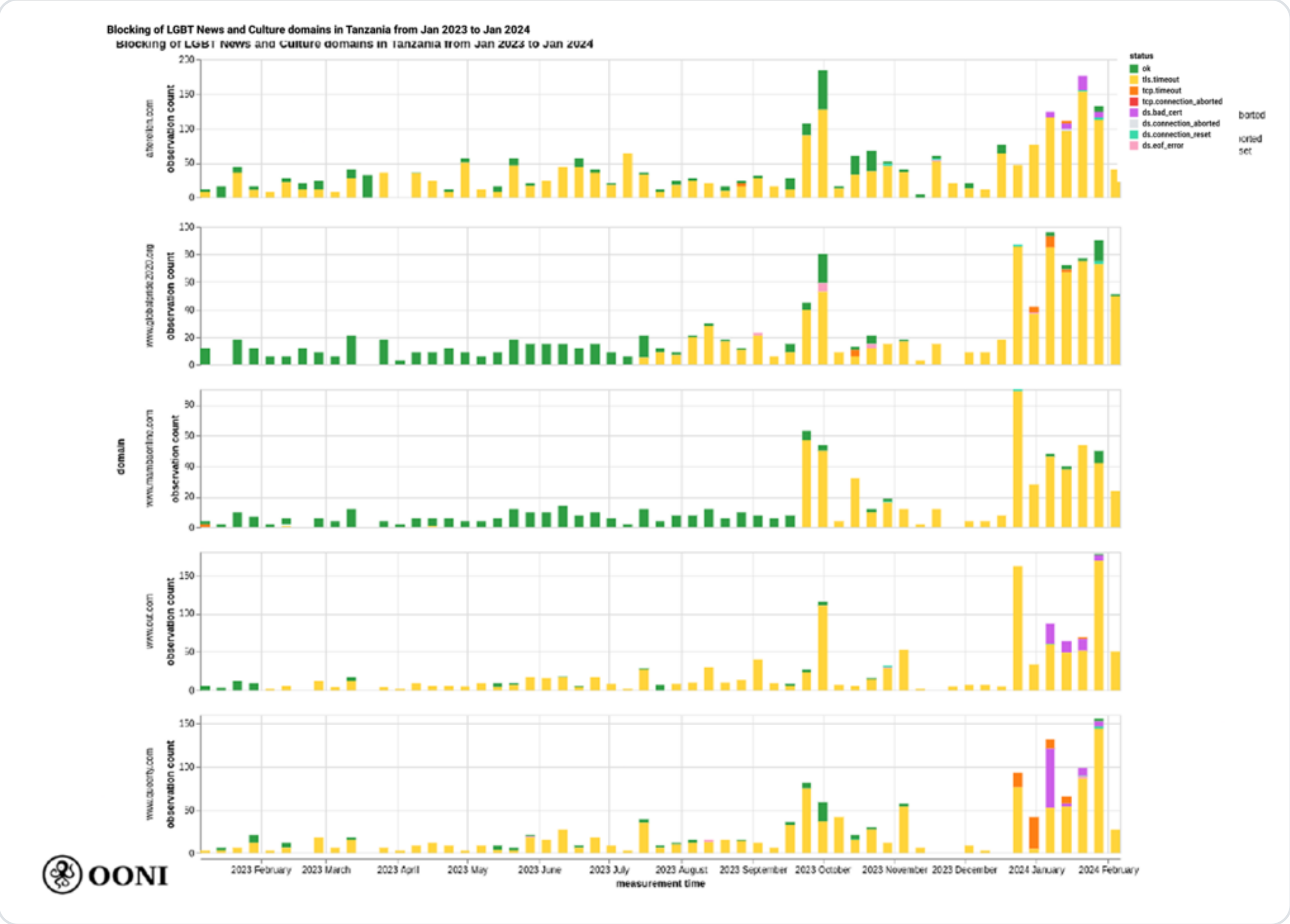


Chart: *Blocking of LGBTIQ news and culture domains in Tanzania between 1st January 2023 to 31st January 2024 (source: ooni/data tool).*

Similarly to the blocking of LGBTIQ social networking and human rights sites (discussed previously), we observe that the vast majority of anomalous measurements presented `tls.timeout` errors. In these cases, OONI data shows the timing out of the session after the ClientHello message during the TLS handshake, suggesting that access to these sites is blocked by means of TLS interference. The fact that we observe errors (`tls.timeout`) that are consistent with the testing of many other blocked domains increases our confidence in determining that access to these domains (shared through the above chart) was blocked in Tanzania during the testing period.

The blocked domains include MambaOnline (`www.mambaonline.com`), South Africa's leading LGBTQ+ news and lifestyle website, which has published an article discussing the closing down of HIV facilities in Tanzania and its impact on LGBT communities in the country. The blocked domains also include Global Pride 2020 (`www.globalpride2020.org`), which launched in April 2020 – in response to the COVID-19 pandemic – with the goal of bringing LGBTIQ communities worldwide together.

LGBTIQ suicide prevention

OONI data collected from Tanzania suggests that access to The Trevor Project (`www.thetrevorproject.org`) is blocked in Tanzania. Founded in 1998, The Trevor Project is a leading suicide prevention and crisis intervention nonprofit organization for LGBTQ+ young people. They provide a variety of services, including a toll-free telephone number where confidential assistance is provided by trained counselors, as well as an online social networking community for LGBTQ+ youth.

The blocking of `www.thetrevorproject.org` appears to have started on 7th February 2023, as OONI data provides more consistent signals of blocking thereafter. The following chart aggregates OONI measurement coverage from the OONI Probe testing of `www.thetrevorproject.org` on 15 networks in Tanzania between 1st January 2023 to 31st January 2024.

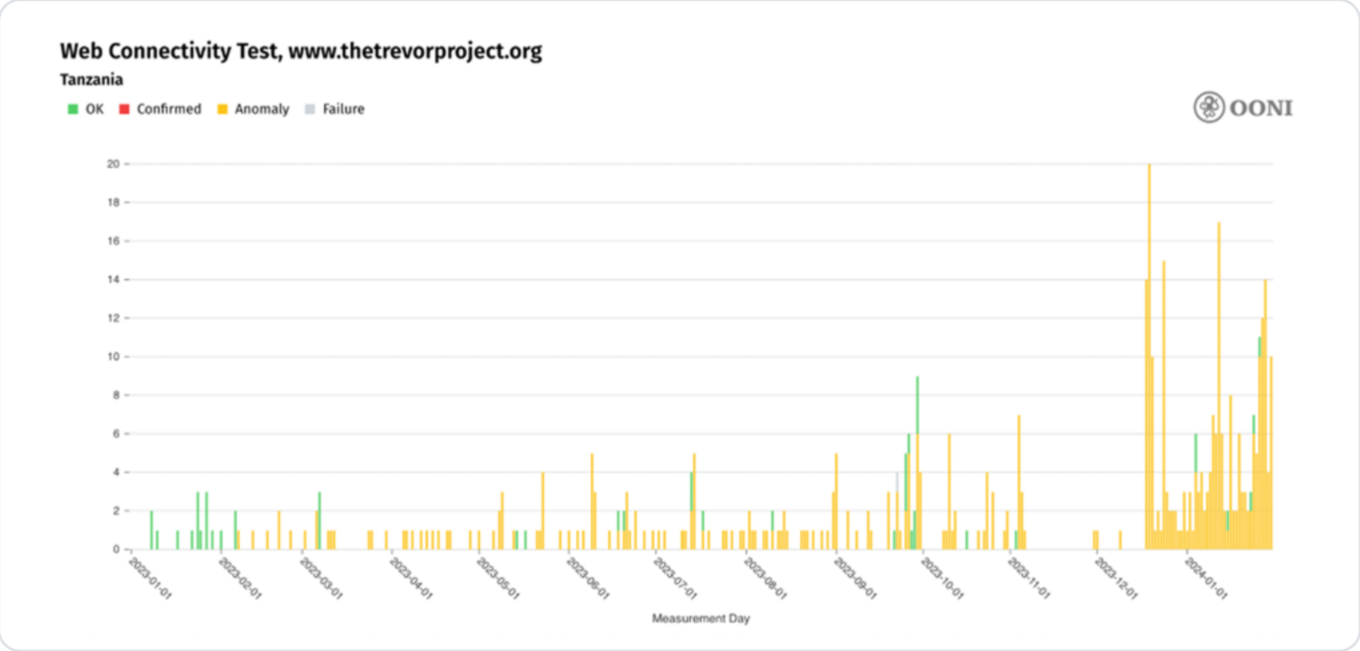


Chart: *OONI Probe testing of The Trevor Project (`www.thetrevorproject.org`) in Tanzania between 1st January 2023 to 31st January 2024 (source: OONI data).*

Throughout most of the testing period, the site received limited testing coverage from OONI Probe users in Tanzania, though we observe that most measurements from 7th February 2023 onwards started presenting anomalies (and, therefore, signs of potential blocking). We observed a spike in testing on 18th December 2023, and increased stable measurement coverage thereafter (which continued to present anomalies and signs of blocking).

We analyzed the anomalous measurements and found that the vast majority presented `tls.timeout` errors. Specifically, OONI data shows the timing out of the session after the ClientHello message during the TLS handshake, suggesting that access to `www.thetrevorproject.org` is blocked in Tanzania by means of TLS interference.

The following chart presents the results of our analysis, providing a per-ASN breakdown of the measurement coverage. We have limited the chart to the top 7 ASNs that presented the largest measurement coverage during the analysis period (to increase our confidence in the findings).

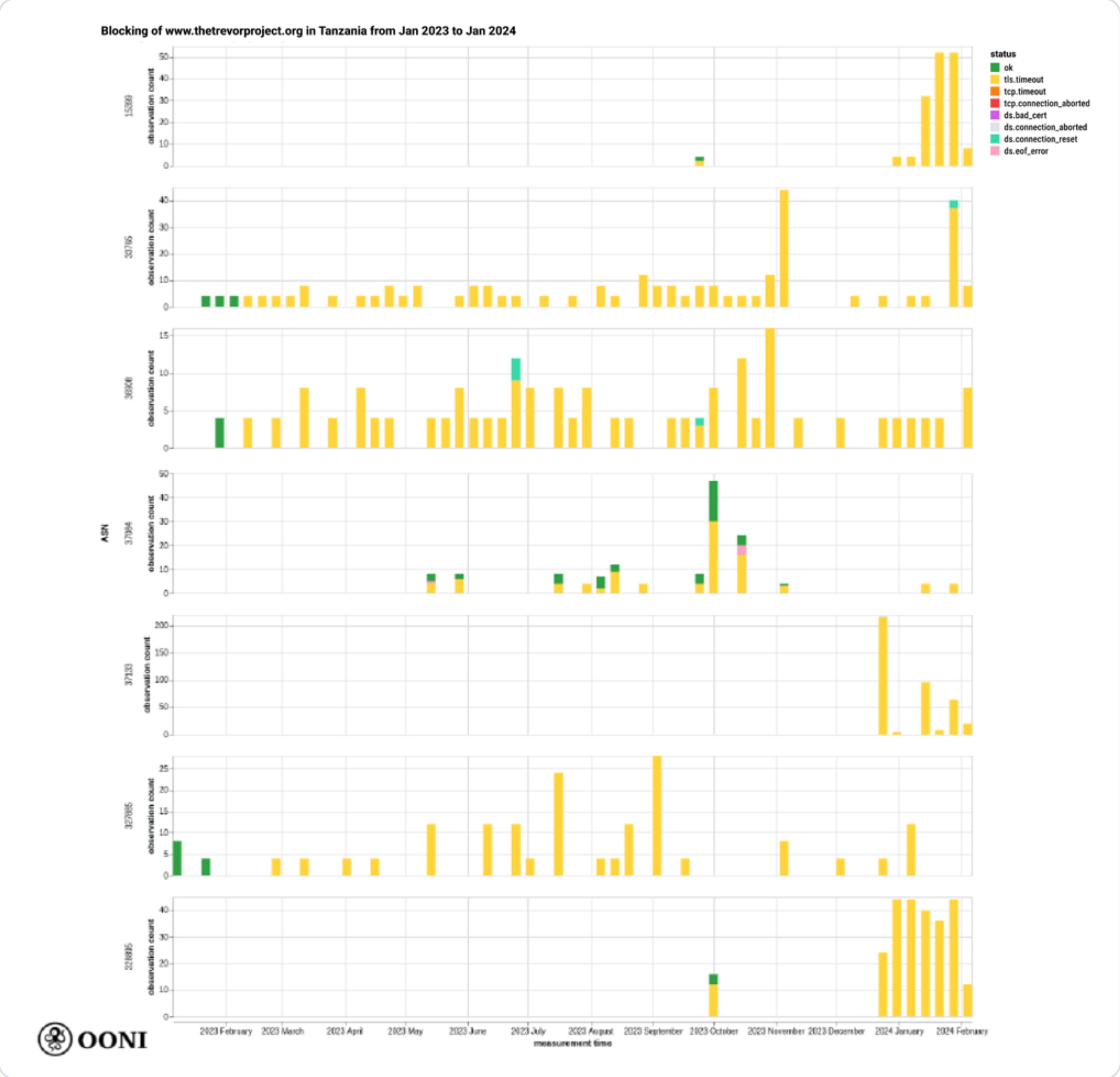


Chart: *Blocking of The Trevor Project (`www.thetrevorproject.org`) in Tanzania between 1st January 2023 to 31st January 2024 (source: ooni/data tool).*

As is evident from the above chart, the majority of measurements from the testing of `www.thetrevorproject.org` consistently presented `tls.timeout` errors on all 7 ASNs throughout most of the testing period. This suggests that different ISPs in Tanzania adopt the same blocking technique, possibly using similar (or the same) Deep Packet Inspection (DPI) technology to implement the blocks. Moreover, we observe that the timing of the block started at around the same time (between February 2023 to March 2023) on at least 3 ASNs. This further suggests coordinated blocking policies.

Overall, the blocking of `www.thetrevorproject.org` is probably part of a blocking order that likely entailed multiple LGTIQ-related domains, as suggested by the timing of the block (we started to observe `tls.timeout` errors on 7th February 2023, along with t1whe blocking of many other LGBTIQ-related domains, as discussed previously).

Blocking of websites that support human rights

Several websites that defend human rights through grants and petitions were also found blocked in Tanzania as part of our analysis. These include Change.org (the world's largest platform for social change, enabling users to create and sign petitions on a variety of social justice and human rights issues), Global Fund for Women (a non-profit foundation that funds gender justice movements), GlobalGiving (a non-profit organization that provides a global crowdfunding platform for grassroots charitable projects), and Open Society Foundations (the world's largest private funder of independent groups working for justice, democratic governance, and human rights).

Specifically, OONI data suggests that access to `www.change.org`, `www.globalfundforwomen.org`, `www.globalgiving.org`, and `www.opensocietyfoundations.org` were blocked in Tanzania during the analysis period. The following chart aggregates OONI measurement coverage from the OONI Probe testing of these domains on multiple networks in Tanzania between 1st January 2023 to 31st January 2024.

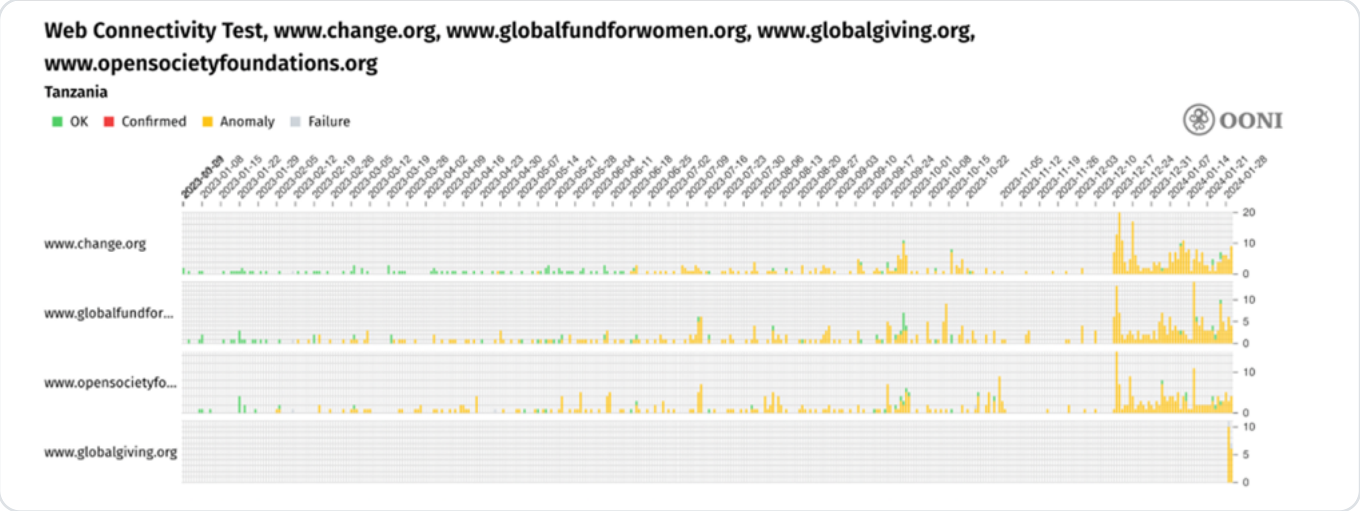


Chart: *OONI Probe testing of* `www.change.org`*,* `www.globalfundforwomen.org`*,* `www.globalgiving.org`*, and* `www.opensocietyfoundations.org` *in Tanzania between 1st January 2023 to 31st January 2024 (source: OONI data).*

While these domains received limited testing coverage throughout most of the analysis period (with a noticeable spike in measurement coverage from December 2023 onwards), it is evident from the above chart that most measurements presented anomalies (and, therefore, potential signals of blocking). In February 2023, OONI data shows that the testing of `www.globalfundforwomen.org` and `www.opensocietyfoundations.org` started to present anomalies, while the testing of `www.change.org` started to present signs of blocking on 29th April 2023. It's worth noting that the OONI Probe testing of `www.globalgiving.org` in Tanzania only started on 29th January 2024, resulting in very limited measurement coverage during the analysis period. Yet, all of those measurements presented anomalies, providing a signal of blocking.

Our analysis of these anomalous measurements reveals that the vast majority presented `tls.timeout` errors, as illustrated through the chart below.

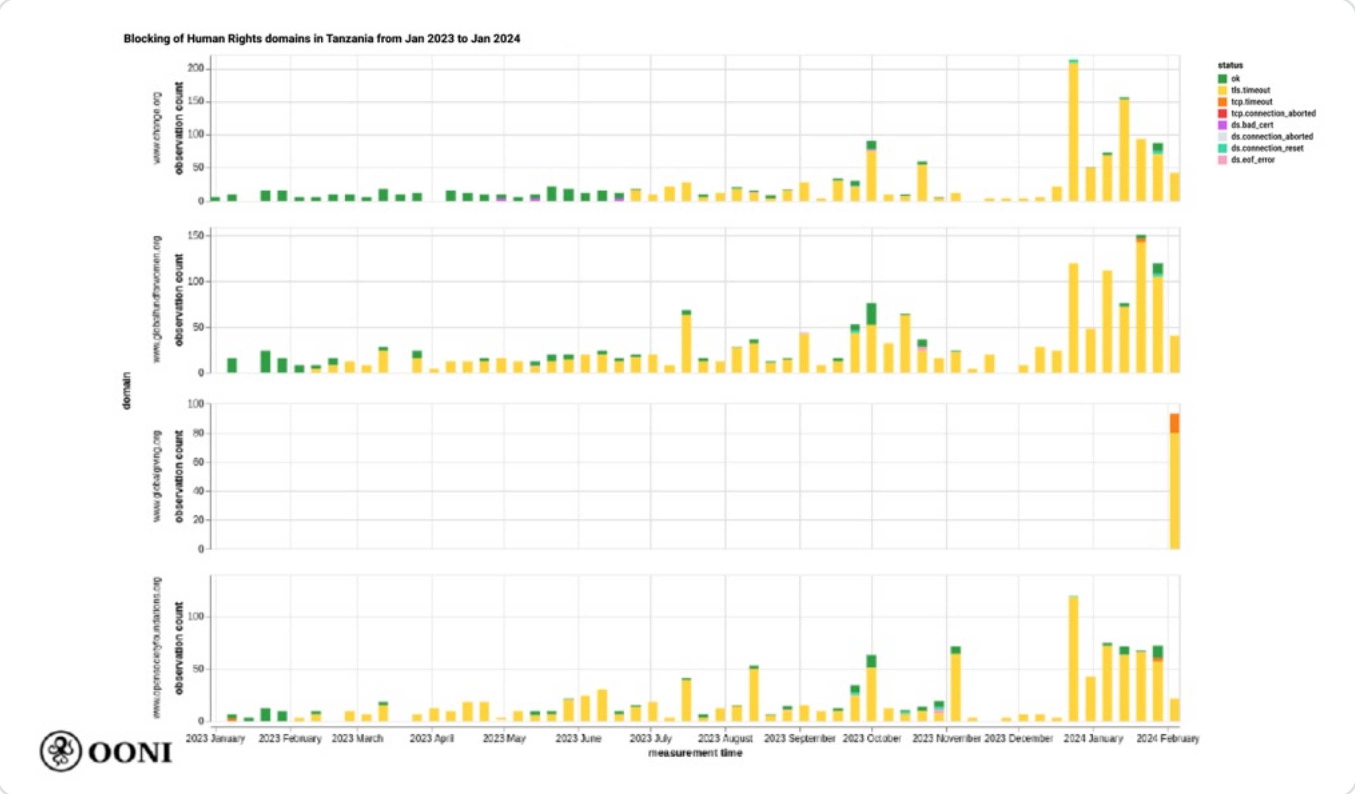


Chart: *Blocking of human rights websites in Tanzania between 1st January 2023 to 31st January 2024 (source: ooni/data tool).*

Specifically, OONI data shows that when the measurements presented anomalies, those anomalies were caused as a result of the timing out of the session after the ClientHello message during the TLS handshake. As we observe this in most anomalous measurements, there is a strong indication that access to `www.change.org`, `www.globalfundforwomen.org`, `www.globalgiving.org`, and `www.opensocietyfoundations.org` was blocked in Tanzania by means of TLS interference. This is consistent with the types of failures and means of blocking observed for other blocked websites in Tanzania (as discussed in previous sections of this report).

While the exact motivation for these blocks is quite unclear to us, it is worth mentioning that GlobalGiving previously hosted a crowdfunding project in support of LGBT Voice Tanzania (which promotes LGBTIQ human rights in Tanzania), which we also found to be blocked in the country. Similarly, GlobalGiving currently hosts an active crowdfunding project in defense of LGBTQIA rights in Tanzania (also linked with LGBT Voice Tanzania). In light of the restrictive environment for LGBTIQ rights and the blocking of numerous LGBTIQ websites in Tanzania (as discussed previously), it is possible that the blocking of GlobalGiving may have been motivated by an attempt to limit support towards causes that the government does not approve. Similarly, the blocking of Change.org, Global Fund for Women, and Open Society Foundations may have had similar motivations. The targeted nature of these blocks is further suggested by the fact that many other human rights websites, such as those of Human Rights Watch and Amnesty International, were (mostly) found accessible during the analysis period.

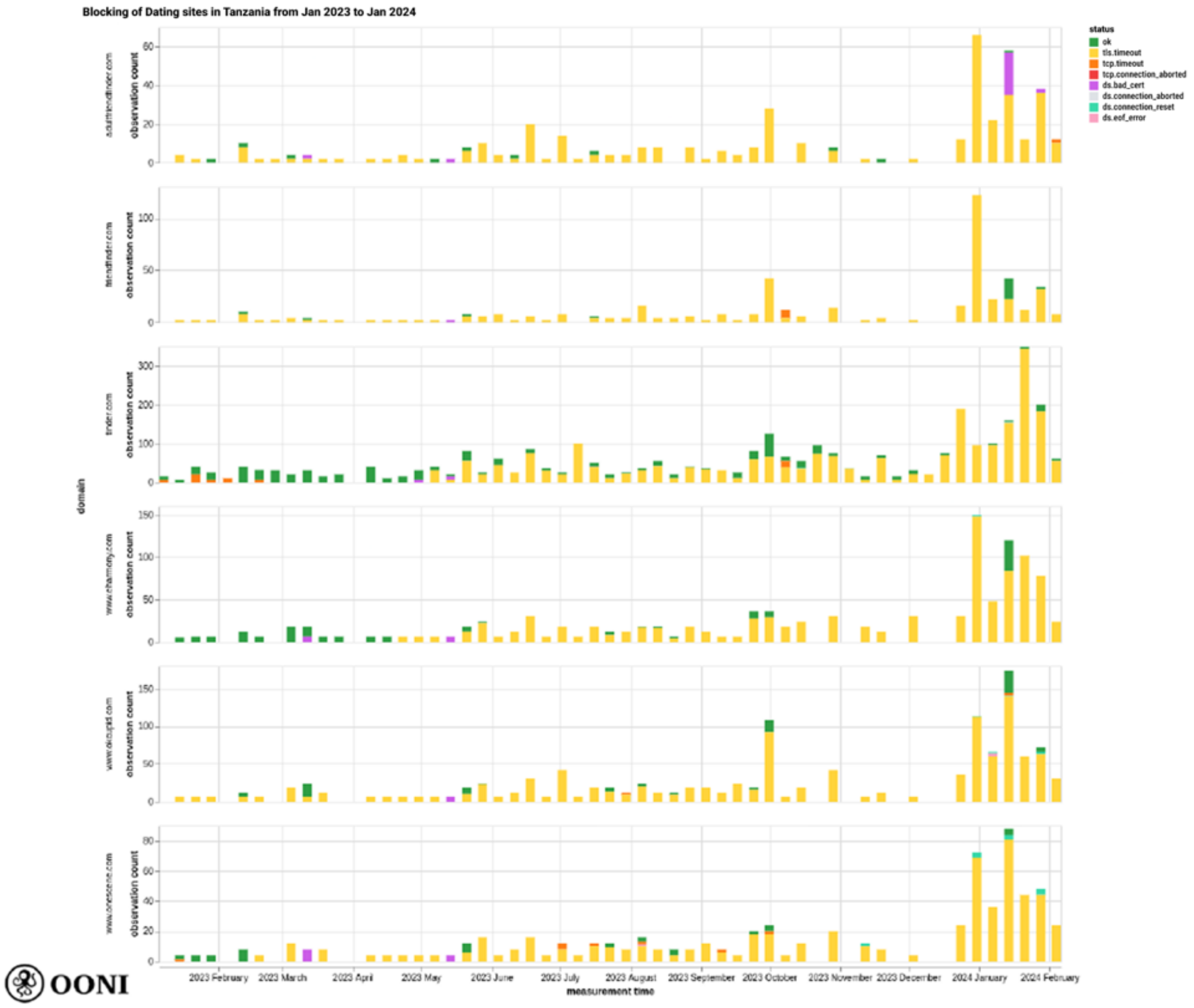


Chart: *Blocking of online dating websites in Tanzania between 1st January 2023 to 31st January 2024 (source: ooni/data tool).*

Our analysis shows that (similarly to the blocking of other websites identified as part of this study) the vast majority of measurements presented timeout errors during the TLS handshake, suggesting that access to these dating websites is blocked by means of TLS interference. It's worth noting that while we observe signs of TLS interference for most domains starting from the beginning of the analysis period (between January 2023 to February 2023), we mainly start to observe TLS handshake timeout errors on 19th April 2023 for `www.eharmony.com`, and on 5th May 2023 for `tinder.com`. While the blocking of the other domains may have started before the analysis period, the blocking of eHarmony and Tinder is mainly visible in OONI data from April/May 2023 onwards.

Blocking of Clubhouse and 4chan

As of 13th August 2023, OONI data suggests that Tanzania started blocking access to Clubhouse – a social networking app based on audio-chat for thematic discussions. We previously reported on this block. Our analysis for this study suggests that 4chan (which hosts boards dedicated to a wide variety of topics) was blocked in Tanzania throughout the analysis period as well.

We produced the following chart based on our analysis of OONI measurements collected from the testing of `www.clubhouse.com`, `www.joinclubhouse.com`, and `www.4chan.org` in Tanzania between January 2023 to January 2024. The chart provides a weekly aggregation of measurements (collected from multiple networks in Tanzania) with annotations of results.

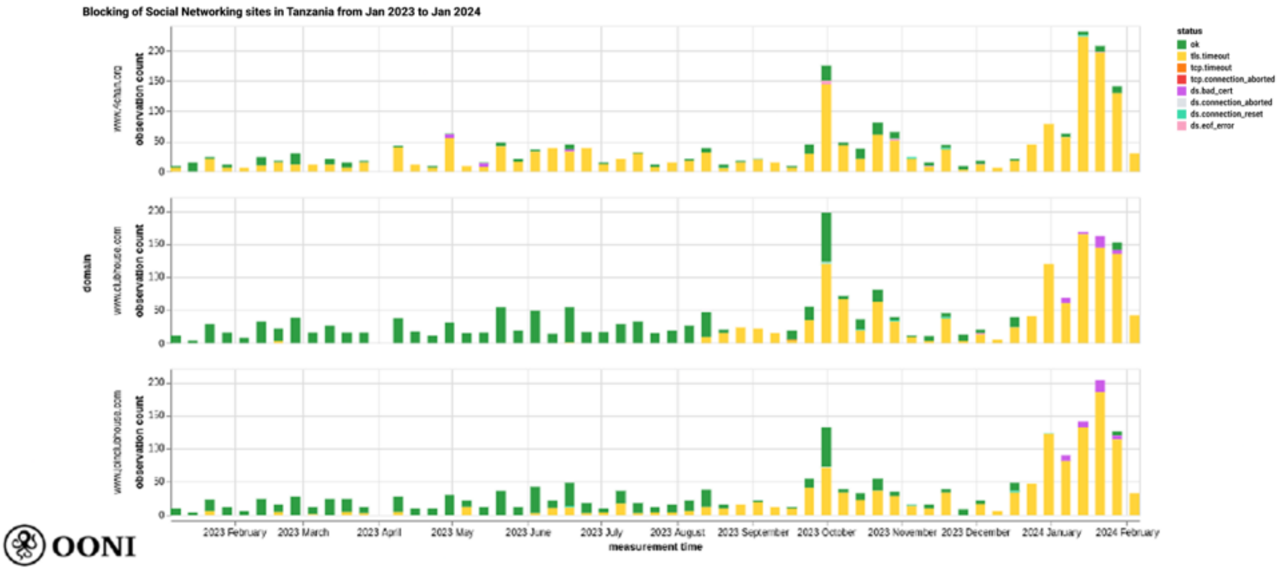


***Chart:** OONI Probe testing of Clubhouse and 4chan in Tanzania between 1st January 2023 to 31st January 2024 (source: ooni/data tool).*

While the testing of `www.4chan.org` presented anomalies throughout the analysis period (the spike in anomalies began in November 2022), we observe that the testing of `www.clubhouse.com` presented the first signs of TLS interference on 13th August 2023. However, we observe the first TLS handshake timeout errors for `www.joinclubhouse.com` (which now redirects to `www.clubhouse.com`) on 18th January 2023, suggesting that some ISPs in Tanzania may have started interfering with access to Clubhouse earlier than August 2023. For all 3 domains, we have a more consistent signal from October 2023, when the measurement coverage increased and more consistently presented signs of TLS interference. Similarly to other blocked websites reported in this study, we observe the timing out of the session after the ClientHello message during the TLS handshake.

It's worth highlighting that other (popular) social networking sites (such as those of Facebook, Instagram, and Twitter/X) and instant messaging apps (such as WhatsApp and Facebook Messenger) did not present significant signals of blocking throughout the analysis period (though we reported on the blocking of such social media platforms during Tanzania's 2020 general elections), and they appeared to be mostly accessible on tested networks (the anomalous measurements during this period appear to be false positives based on our analysis). This suggests that the blocking of Clubhouse and 4chan may have been targeted in an attempt to stifle specific thematic discussions by groups using those platforms.

Blocking of ProtonVPN

In October 2023, the Tanzania Communications Regulatory Authority (TCRA) reportedly started requiring users in Tanzania to report their use of Virtual Private Networks (VPNs). To use a VPN, users in Tanzania are now required to fill out a form to report to TCRA the VPNs that they use, providing information that includes their individual IP addresses. The Authority clarified that they have not restricted the use of VPNs, but it remains unclear to us if the new requirement has resulted in a drop in VPN use in Tanzania.

We checked OONI data to see if we could detect signals of VPN blocking in Tanzania. Most OONI data collected from Tanzania during the analysis period (between January 2023 to January 2024) did not provide strong signals of VPN blocking, seemingly corroborating TCRA's claim that they would not restrict the use of VPNs. However, it's worth noting that OONI data mainly involves the testing of VPN websites, while Psiphon and Tor are the main circumvention tools that are measured for reachability (neither of which presented strong signs of blocking during the analysis period). Moreover, relevant OONI measurement coverage is significantly reduced and limited from 18th June 2023 onwards, limiting our ability to detect signs of VPN blocks.

Only a few of the tested VPN domains presented a large volume of anomalies during the analysis period. These include the domains of Secure VPN (`securevpn.im`) and ProtonVPN (`protonvpn.com` and `api.protonvpn.ch`). However, the anomalous measurements from the testing of `securevpn.im` have been excluded from the findings, because the testing of this domain failed globally during the same period (between mid-March 2023 to mid-June 2023), seemingly because there was an issue with the domain's IP address during that period.

OONI data only indicates that access to ProtonVPN was blocked in Tanzania during the analysis period. Specifically, OONI data shows that most measurements from the testing of `protonvpn.com` and `api.protonvpn.ch` presented anomalies, as illustrated below.

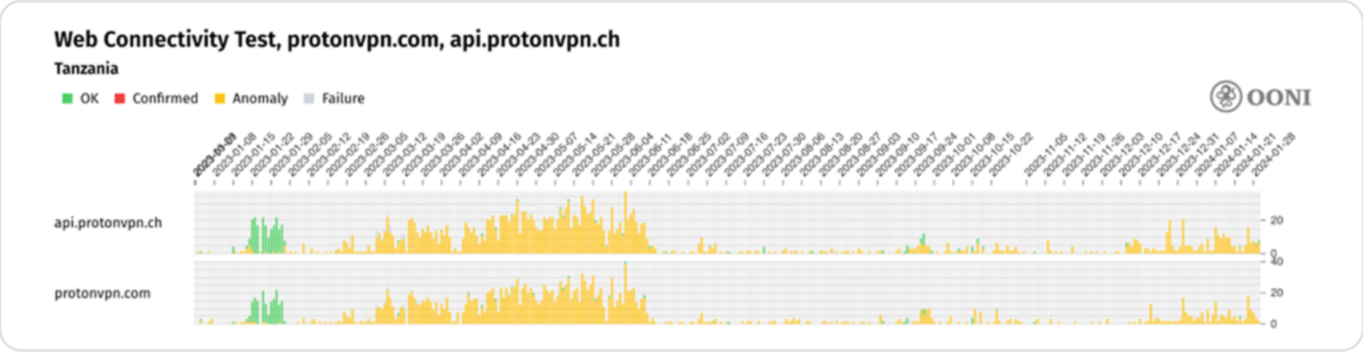


***Chart:** OONI Probe testing of ProtonVPN (`protonvpn.com` and `api.protonvpn.ch`) in Tanzania between 1st January 2023 to 31st January 2024 (source: OONI data).*

Within the analysis period, we start to observe anomalies in early January 2023 (and relevant measurements had also been presenting anomalies since at least August 2022), but we have a stronger signal from March 2023 onwards (when the measurement volume increased). Throughout the testing period, we observe that most measurements presented anomalies, providing a signal of blocking. Interestingly, the above chart shows very similar and consistent measurement results in the testing of both `protonvpn.com` and `api.protonvpn.ch`, suggesting that access to both ProtonVPN's website and app was blocked in Tanzania.

Our analysis of ProtonVPN (`protonvpn.com` and `api.protonvpn.ch`) measurements shows consistent failures with those observed in the blocking of other URLs discussed as part of this study. Specifically, most anomalous measurements presented signs of **TLS interference**, as OONI data shows the timing out of the session after the ClientHello message during the TLS handshake.

We produced the following chart based on our analysis, illustrating that TLS handshake timeout errors are observed in most measurements collected from the testing of `protonvpn.com` on multiple networks in Tanzania.

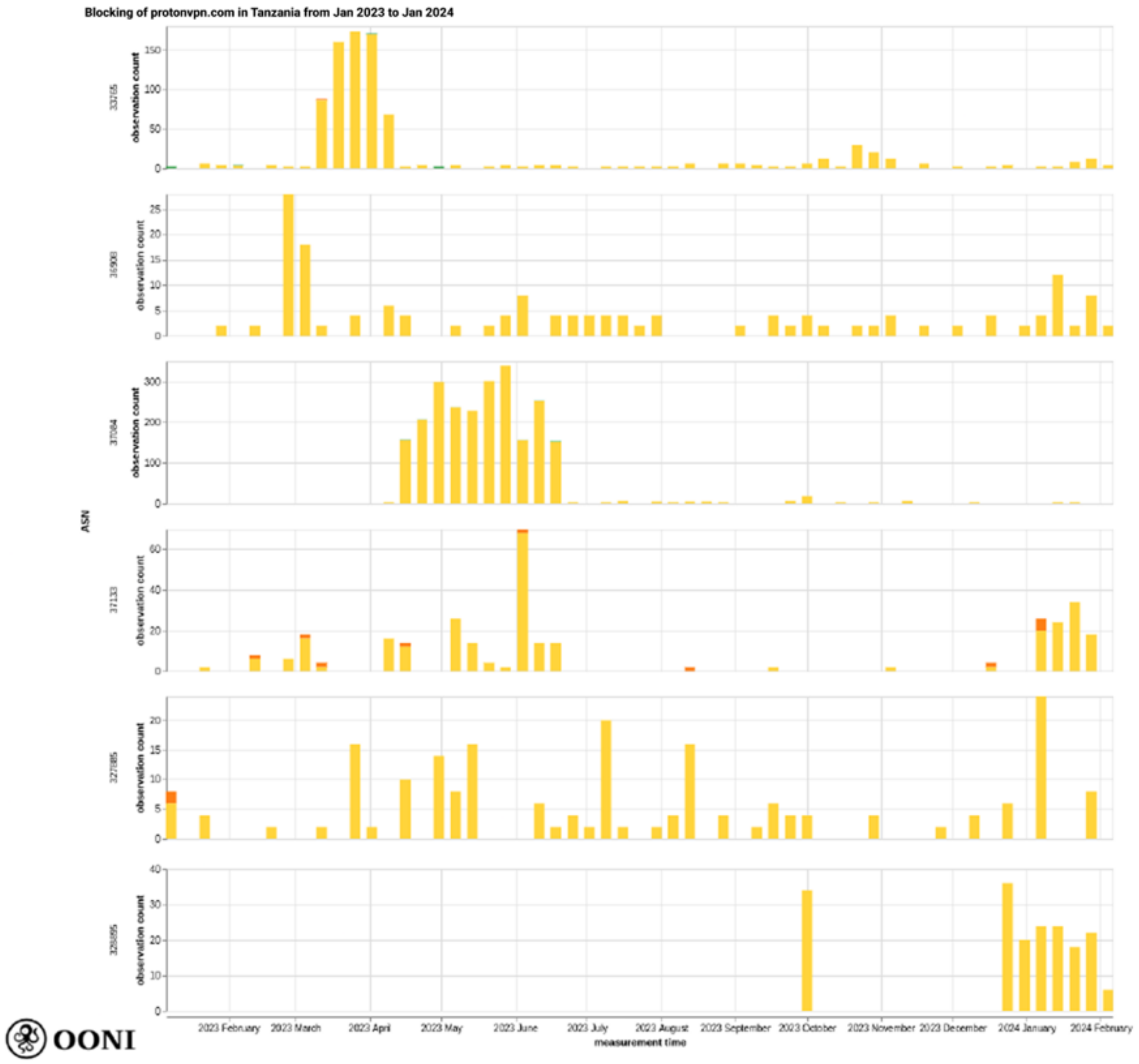


Chart: *Per ASN breakdown of OONI measurement coverage from the testing of ProtonVPN (`protonvpn.com`) in Tanzania between 1st January 2023 to 31st January 2024 (source: ooni/data tool).*

We have limited the above chart to the ASNs which received the largest measurement coverage during the analysis period. As is evident, we observe the same TLS handshake timeout errors in almost all measurements collected from the testing of `protonvpn.com` on (at least) six ASNs between January 2023 to January 2024. This not only provides a strong signal of blocking, but also suggests that ISPs in Tanzania implement blocks using the same censorship techniques (similarly to the findings for other blocked URLs, as discussed previously in this study).

In response to a Twitter/X thread (mentioning the blocking of ProtonVPN in Tanzania), Proton mentioned that users can try switching between all the different connection protocols available in the app settings to circumvent the block.

Conclusion

Over the past year (between January 2023 to January 2024), OONI data collected from Tanzania shows a surge in blocks in comparison to previous years. The results of our analysis show that most ISPs in Tanzania appear to implement blocks by means of **TLS interference**, specifically by timing out the session after the ClientHello message during the TLS handshake. This suggests the potential use of Deep Packet Inspection (DPI) technology. As the timing of the blocks and the types of URLs blocked are (mostly) consistent across networks, ISPs in Tanzania likely implement blocks in a coordinated manner (based on government orders).

Even though we found many different websites blocked in Tanzania over the past year, our findings suggest that these blocks are mostly targeted in nature. Many of the blocks identified in this study involve **LGBTIQ websites**, which correlates with the escalating discrimination and crackdown on LGBTIQ communities in Tanzania in recent years. The blocking of a wide range of LGBTIQ websites – including LGBTIQ social networks, sites that defend LGBTIQ rights, LGBTIQ news and culture, and an LGBTIQ suicide prevention site – suggests an intensification of government attempts to stifle LGBTIQ communities in Tanzania.

Most social media platforms were found accessible in Tanzania throughout the analysis period, while only Clubhouse and 4chan were found blocked. This suggests that these blocks may have been targeted in an attempt to stifle specific thematic discussions by groups using those platforms. Quite similarly, many human rights websites (such as those of Human Rights Watch and Amnesty International) were (mostly) accessible in Tanzania over the last year, while OONI data shows the blocking of Change.org, Global Fund for Women, GlobalGiving and Open Society Foundations. These blocks may have been motivated by an attempt to limit support towards causes that the government does not approve (further suggesting the targeted nature of the blocks).

Meanwhile, the Tanzania Communications Regulatory Authority (TCRA) recently started requiring users in Tanzania to report their use of VPNs. We found that most tested VPN websites are still accessible in Tanzania, and that only ProtonVPN was blocked over the last year. This suggests that while users in Tanzania are now required to report their use of VPNs, the use of VPNs is not widely restricted (through blocks).

Yet, the new VPN reporting requirement raises the question of whether it will result in less VPN use in Tanzania and, by extension, less censorship circumvention. And if it results in less censorship circumvention, it raises the question of what impact the blocks (identified through this study) would have on LGBTIQ communities and other human rights movements in Tanzania. We encourage researchers to explore these questions through future studies.

Acknowledgements

We thank OONI Probe users in Tanzania for contributing measurements, supporting this study.

Photos by Qim Manifester (page 8) Peter Mitchell (page 17) on Unsplash.