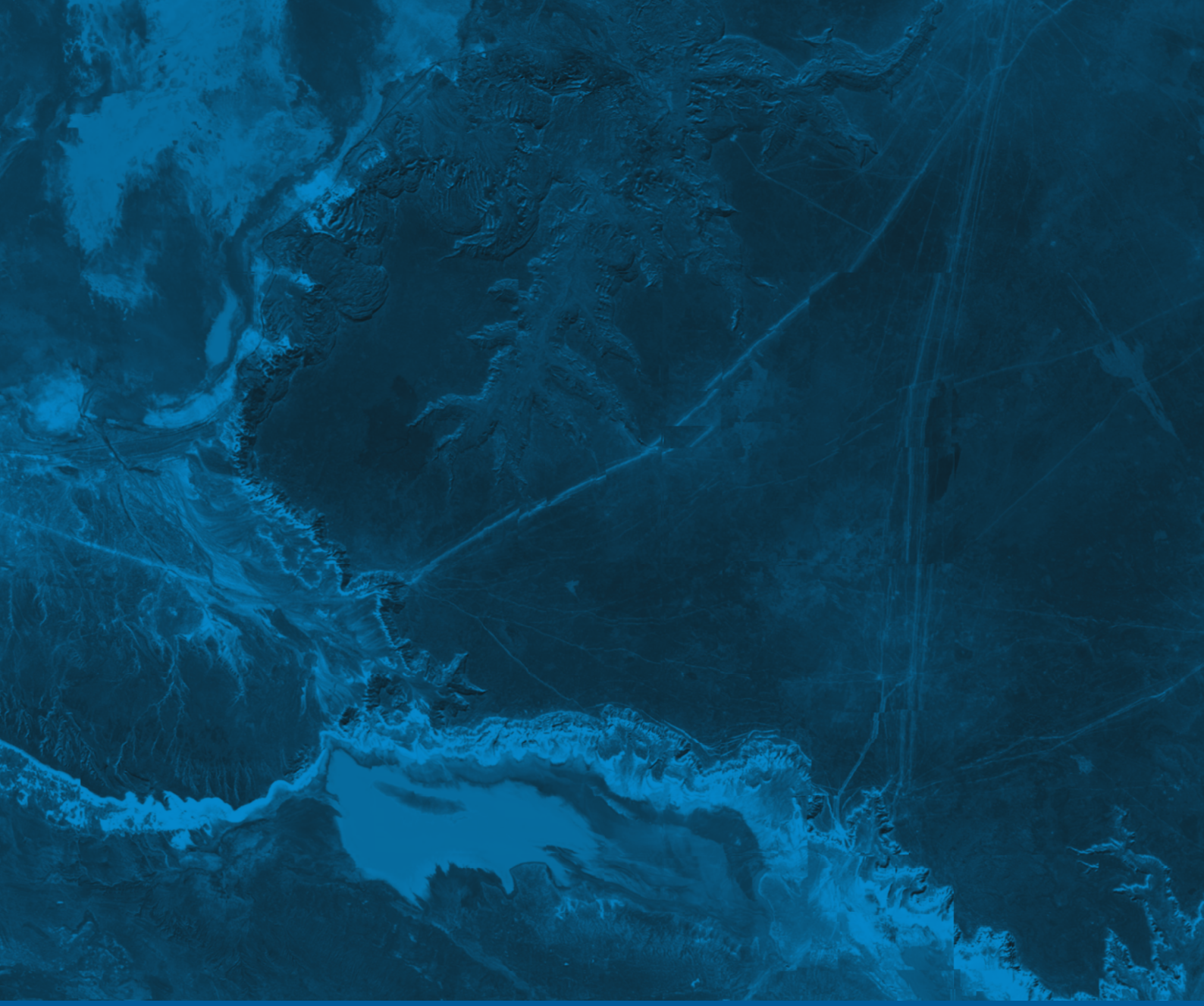


Kazakhstan:
TLS MITM attacks and blocking of news media, human rights, and circumvention tool sites

OONI
IFKZ INTERNET FREEDOM KAZAKHSTAN
EURASIAN DIGITAL FOUNDATION

In recent years, internet censorship in Kazakhstan has been reported quite extensively. As part of this study, OONI, Internet Freedom Kazakhstan (IFKZ), and Eurasian Digital Foundation collaborated to investigate internet censorship in Kazakhstan over the past year (between June 2023 to June 2024) through the analysis of empirical network measurement data.

In this report, we share OONI censorship measurement findings and relevant legal context. We found numerous news media, human rights, and circumvention tool websites blocked in Kazakhstan by means of TLS interference. We also found 7 distinct intermediate certificates signed by 4 distinct root CAs being used to carry out TLS man-in-the-middle (MITM) attacks, targeting at least 14 distinct domain names on at least 19 different networks in Kazakhstan. We share more details below.

Yelzhan Kabyshev (Head of Legal Practice, Eurasian Digital Foundation, Manager of the Human Rights Project, Internet Freedom Kazakhstan), Ruslan Daiyrbekov (Founder, Eurasian Digital Foundation), Vadim Melyakov (Analyst, Eurasian Digital Foundation, Specialist in International Relations), Igor Loskutov (Head of the Legal Department, InfoTech&Service LLP), Maria Xynou (OONI), Elizaveta Yachmeneva (OONI), Arturo Filastò (OONI), Mehul Gulati (OONI)

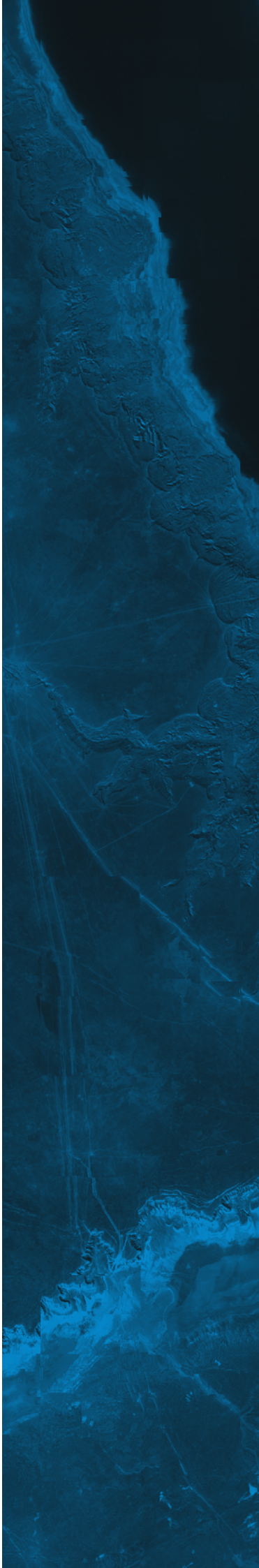
Layout Design: Ura Design

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

OONI

© 2024 Open Observatory of Network Interference (OONI)
Content available under a Creative Commons license.

Publication date: September 19, 2024
Last updated: October 15, 2024



Contents

Key Findings

Our analysis of OONI data collected from Kazakhstan over the past year (between 1st June 2023 to 1st June 2024) reveals the following:

- **TLS Man-In-The-Middle (MITM) attacks.** In OONI data collected from Kazakhstan between 2021 to 2024, we found 7 distinct intermediate certificates signed by 4 distinct root CAs being used to carry out TLS man-in-the-middle (MITM) attacks, targeting at least 14 distinct domain names on at least 19 different networks in Kazakhstan.

- **Blocking of at least 17 news media websites.** OONI data shows the blocking of:
  - Many Russian news media websites (such as the Russian TV Channel Tsargrad, Sputnik and Pogrom, the 360 Russian satellite TV channel, and the Ferghana Information Agency);
  - A few **Kyrgyz** news media websites (Kloop and Centralasia.media);
  - One international news website (Vice News).

- **Blocking of petition sites and of the Russian language edition of Amnesty International's website.** OONI data shows the targeted blocking of `amnesty.org.ru`, `www.change.org`, `www.ipetitions.com`, and `egov.press`. Meanwhile, Amnesty International's English language website was accessible in Kazakhstan, as were many other international human rights websites (such as Human Rights Watch).

- **Blocking of at least 73 circumvention tool websites.** OONI data shows the blocking of numerous censorship circumvention tool websites, including those of NordVPN, ExpressVPN, ProtonVPN, OpenVPN, TunnelBear, and Surfshark VPN. However, OONI data suggests that both Tor and Psiphon VPN were reachable in Kazakhstan during the analysis period.

The results of our analysis show that most ISPs in Kazakhstan appear to implement blocks by means of **TLS interference**, specifically by timing out the session after the Client Hello 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 Kazakhstan likely implement blocks in a coordinated manner (possibly through the use of Deep Packet Inspection technology). Coordination among ISPs in Kazakhstan is further suggested by the fact that we found the same certificate used by 19 distinct ISPs to implement TLS MITM attacks.

Introduction

Internet censorship in Kazakhstan has been reported quite extensively over the past few years. In 2019, for example, Reporters Without Borders (RSF) published an article condemning the blocking of news media websites and social media platforms in Kazakhstan amid opposition protests. Freedom House's Freedom on the Net 2023 report documented many more blocking cases in Kazakhstan, including the blocking of news media websites and censorship circumvention tools. Censored Planet published a research paper documenting large scale HTTPS interception in Kazakhstan, while OONI published a report on the throttling of news media websites during Kazakhstan's 2022 presidential election.

As part of our partnership, OONI, Internet Freedom Kazakhstan (IFKZ) and Eurasian Digital Foundation collaborated on investigating internet censorship in Kazakhstan over the last year. In this research, we investigate the aspects of internet regulation in Kazakhstan, including internet censorship. We analyze legislation focusing on limiting access to online content and its implementation. Specifically, we focus on the existing laws, and cases of social media, messengers, and website blockings. We also analyze cases of limiting access to VPN services, proxies and anonymizers which are interpreted exceptionally as circumvention tools by governmental entities.

This research aims to provide an extensive overview of the current state of internet censorship in Kazakhstan, including statistics on restrictions, case studies and examples from real practice, as well as analysis of legislation and its implementation. This research will be a useful resource for human rights defenders, journalists, researchers and other audiences interested in the state of freedom of speech and internet censorship in Kazakhstan.

Specifically, the research questions that guided this study include:

- Which **news media, human rights, political, and circumvention tool websites** are blocked in Kazakhstan?
    - Which techniques do ISPs in Kazakhstan use to implement the blocks? How does the blocking of websites vary across ISPs in Kazakhstan?
    - Which legal frameworks enable the implementation of internet censorship in Kazakhstan?
    - What is the impact of censorship on Kazakh news media organizations?

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 170 countries (including Kazakhstan), and network measurements collected by OONI Probe users are automatically published as open data in real-time. As part of this study, OONI analyzed OONI data collected from Kazakhstan to detect and characterize the blocking of websites.

Internet Freedom Kazakhstan (IFKZ) aims to ensure that the internet of Kazakhstan is free from any unlawful censorship or restrictions and to create a user-friendly digital environment with the possibility to exercise all human rights and freedoms. IFKZ focuses on enhancing transparency of governmental authorities in the ICT industry, introducing selectable access to unlawfully restricted resources, analyzing the legal grounds for restricting access to websites, and advocating for digital human rights and freedoms. As part of this study, IFKZ performed legal analysis and interviewed two Kazakh news media organizations (ProTenge and Medianet).

Our overarching research goal was to explore internet censorship in Kazakhstan, both through OONI network measurement and legal analysis. We aimed to determine whether it was possible to detect and characterize the blocking of websites in Kazakhstan (with a focus on news media, human rights, political and circumvention tool websites), while exploring whether the implementation of such blocks differed across ISPs in the country. Answering such questions can help with evaluating whether and to what extent internet users in Kazakhstan experience restrictions. Analyzing relevant legal frameworks provides important context for understanding the environment in which blocks are implemented.

We narrowed the scope of our study to websites that would potentially have the most impact if found blocked. Given past reports on the blocking of news media and circumvention tools, we limited our analysis to the testing of news media and censorship circumvention tool websites, while also analyzing the testing of political and human rights websites. We further limited OONI data analysis to measurements collected over the past year, between 1st June 2023 to 1st June 2024.

In the following sections, we share more details on the methods and findings of this study.

Methods

As part of this study, our goal was to explore internet censorship in Kazakhstan, both through OONI network measurement and legal analysis.

Specifically, the research questions that guided this study include:

- Which **news media, human rights, political, and circumvention tool websites** are blocked in Kazakhstan?
  - Which techniques do ISPs in Kazakhstan use to implement the blocks? How does the blocking of websites vary across ISPs in Kazakhstan?
  - Which legal frameworks enable the implementation of internet censorship in Kazakhstan?
  - What is the impact of censorship on Kazakh news media organizations?

We explored these questions through a combination of both qualitative and quantitative research methods. To investigate the blocking of websites, we analyzed OONI data collected from Kazakhstan over the last year. Specifically, we analyzed OONI Web Connectivity measurements (which pertain to the OONI Probe testing of websites) collected from Kazakhstan between 1st June 2023 to 1st June 2024. This analysis enabled us to detect the blocking of websites based on the specific censorship techniques adopted by ISPs in Kazakhstan to implement the blocks.

To understand the legal frameworks that govern the implementation of internet censorship in Kazakhstan, we carried out relevant legal analysis. To explore the impact of censorship, we interviewed two Kazakh news media organizations. We share more details on our methods below.

Legal analysis, interviews, and test list updates

As part of this study, Internet Freedom Kazakhstan (IFKZ) conducted qualitative research, providing relevant legal context, exploring the impact of censorship on a few Kazakh news media organizations, and informing which websites should be tested for censorship in Kazakhstan. Their research is based on data collected from different sources including official documents, interviews with media organizations and activists, as well as analysis of the legislation and cases of its implementation in Kazakhstan.

Specifically, IFKZ performed relevant legal analysis, updated the test list for Kazakhstan with websites of circumvention tools and media projects which may have been blocked in Kazakhstan according to the legislation norms described in the relevant section. IFKZ also interviewed two Kazakh news media organizations (ProTenge and Medianet) affected by DDOS attacks and social media account hacking to provide context about other types of censorship occurring in Kazakhstan, and the impact of such censorship.

As part of legal analysis, IFKZ provided an overview of existing regulation of online spaces and public information in Kazakhstan, including the relevant Articles of the Constitution, 'Mass Media Law' and 'On Communications' Law. IFKZ not only describe the content of these Articles and Laws, but they also explain how they were implemented through court decisions or with the resolution by the Ministry of Communications, along with related caveats when they are applied to online media and circumvention tools' websites. As an example, IFKZ describes the litigation case of the HideMyName project, whose website has been blocked in Kazakhstan since 2020. The appeal was not successful, however, it is very illustrative of how the described laws are applied in practice.

In the same legal section, IFKZ provides an overview of the publicly available data on the number of URLs and resources blocked in Kazakhstan according to different governmental bodies and argumentation of why these resources have been blocked. This data cannot be considered exhaustive as the legal requirement to list such resources in the Unified Registry of Internet resources hosting information prohibited in Kazakhstan has been lifted since 2022.

OONI data analysis

As part of this study, the Open Observatory of Network Interference (OONI) analyzed OONI network measurement data collected from Kazakhstan between **1st June 2023 to 1st June 2024**. Through this analysis, OONI aimed to examine whether news media, human rights, political, and circumvention tool websites (included in the Citizen Lab's Global and Kazakh test lists) were blocked during the analysis period, and whether the implementation of such blocks varied across networks in Kazakhstan.

Since 2012, 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 170 countries (including Kazakhstan), 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 Kazakhstan and numerous other countries (such as Russia, Iran, and Indonesia), we analyzed anomalous OONI measurements (with our OONI data analysis tool) to detect more subtle and advanced censorship techniques.

As part of this study, we analyzed OONI network measurement data collected from Kazakhstan between **1st June 2023 to 1st June 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 signs of blocking during the analysis period (therefore not warranting more advanced analysis, which is generally aimed towards understanding whether anomalies are false positives or signs of blocking). We excluded measurements from the testing of Signal because they were impacted by data quality issues over the past year.

Out of all Web Connectivity measurements collected from Kazakhstan over the last year, we further limited our analysis to domains (included in the Citizen Lab's Global and Kazakh test lists) that are annotated with the "News Media (NEWS)", "Human Rights Issues (HUMR)", "Political Criticism (POLR)", and "Anonymization and circumvention tools (ANON)" category codes in the Citizen Lab test lists. This enabled us to explore the blocking of news media, human rights, political, and circumvention tool websites, without analyzing all websites tested in Kazakhstan (which include a wide range of many different and unrelated to our research question websites).

We aggregated anomalous Web Connectivity measurements collected from Kazakhstan 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 Kazakhstan (in this study, we found that "tls_timeout_error" 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). We further limited our analysis to the ASNs which received the largest measurement coverage and the strongest blocking signals. 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 Kazakhstan between 1st June 2023 to 1st June 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 Kazakhstan list (only including URLs relevant to Kazakhstan). As these lists are tested by OONI Probe users and there are bandwidth constraints, they are generally limited to around 1,000 URLs. Moreover, from these lists, we limited our analysis to URLs annotated as "News Media (NEWS)", "Human Rights Issues (HUMR)", "Political Criticism (POLR)", and "Anonymization and circumvention tools (ANON)" categories. As a result, the lists may exclude other websites which might be blocked in Kazakhstan, and the findings are limited to the testing of the URLs included in the "News Media (NEWS)", "Human Rights Issues (HUMR)", "Political Criticism (POLR)", and "Anonymization and circumvention tools (ANON)" categories of these lists. Given that the lists are community-curated, we acknowledge the bias in terms of which URLs are added to the lists, as well as the risk for the miscategorization of URLs.

- **Testing coverage of websites**

  Not all URLs included in test lists are measured equally across Kazakhstan over time. Whether OONI data is available for a particular website depends on whether, on which networks, and when an OONI Probe user in Kazakhstan 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 Kazakhstan, 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. Moreover, we limited the findings of this study to the ASNs which received the largest measurement coverage and which presented the strongest blocking signals during the analysis period. These include AS9198 (JSC Kazakhtelecom), AS21299 (Kar-Tel LLC), AS44477 (STARK INDUSTRIES SOLUTIONS LTD), AS206026 (Kar-Tel LLC), AS41798 (JSC Transtelecom), AS9009 (M247 Europe SRL).

- **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).

- **Interviews**

  In an attempt to explore the impact of censorship on news media organizations in Kazakhstan, we interviewed two Kazakh news media organizations (ProTenge and Medianet). Through these interviews, we aimed to complement the legal and OONI network measurement analysis with some qualitative data. However, we acknowledge that the findings from these two interviews do not provide a comprehensive or representative view on the impact of censorship on (most) news media organizations in Kazakhstan, as they mainly reflect insights from the two interviewed organizations. We encourage researchers to conduct a more comprehensive study on this (with a larger interview sample).

OONI Censorship Measurement Findings

As part of this study, we analyzed OONI data collected from Kazakhstan between **1st June 2023 to 1st June 2024**. Our analysis was limited to OONI Web Connectivity measurements pertaining to the testing of domains that are annotated with the "News Media (NEWS)", "Human Rights Issues (HUMR)", "Political Criticism (POLR)", and "Anonymization and circumvention tools (ANON)" category codes in the Global and Kazakh Citizen Lab test lists.

While many domains within the Citizen Lab test list categories that we analyzed (NEWS, POLR, HUMR, ANON) presented anomalies during the analysis period, we limited our findings to the domains that present the strongest signals of blocking. These include domains that received the largest measurement coverage during the analysis period, the largest volume of anomalies (in comparison to the overall measurement volume), and the largest and most consistent volume of failure types within anomalous measurements. We excluded domains that did not meet these criteria, as well as cases involving expired or otherwise dysfunctional domains.

Overall, we did not detect strong cases involving the blocking of political websites in Kazakhstan during the analysis period. More specifically, out of all the domains annotated as "Political Criticism (POLR)" from the Global and Kazakh Citizen Lab test lists, very few domains presented signals of blocking, but we excluded those cases from the findings because the domains had expired.

What we mainly found as part of OONI data analysis is the **blocking of 73 circumvention tool websites**, as well as the **blocking of 17 news media websites and several human rights websites**. In almost all cases, the blocks appear to be implemented by means of **TLS interference**, as OONI data shows that the TLS handshakes result in timeout errors after the Client Hello message. This is observed uniformly on all tested networks in Kazakhstan during the analysis period, providing a strong signal of blocking. It further suggests that ISPs in Kazakhstan implement censorship in a coordinated manner, perhaps through the use of Deep Packet Inspection (DPI) technology.

It's worth highlighting that we **found 7 distinct intermediate certificates signed by 4 distinct root CAs being used to carry out TLS man-in-the-middle (MITM) attacks**, targeting at least 14 distinct domain names on at least 19 different networks in Kazakhstan.

We share more details on the blocks in the following sections.

Blocking of news media websites

News media censorship in Kazakhstan has been reported over the past years. In 2021, for example, access to HOLA News – a Kazakh independent news website – was reportedly blocked temporarily (for 10 days) after reporting on the Pandora Papers offshore leaks. Amid Kazakhstan's 2022 snap presidential elections, several Russian and international news media websites were reportedly inaccessible. OONI data at the time suggested that access to such news media sites was throttled.

Last year, Kazakhstan reportedly blocked the website of the Russian TV Channel Tsargrad over extremist content and for "inciting hatred". A few months later (November 2023), Kazakhstan reportedly blocked Russia's Sputnik24 service over licensing issues. In January 2024, Kazakh television operator TVCOM stopped broadcasting several stations launched by Russian state-run Channel One to reportedly reduce the share of foreign news channels in Kazakhstan.

Our analysis of OONI data collected from Kazakhstan over the last year (between 1st June 2023 to 1st June 2024) shows the **blocking of the following 17 news media domains:**

- 360tv.ru
- astrakhan.sm.news
- centralasia.media
- cont.ws
- fergana.media
- holanews.kz
- kloop.kg
- kz.tsargrad.tv
- meduza.io
- newsland.com
- regnum.ru
- sputnikipogrom.com
- stanradar.com
- ukraina.ru
- www.kavkazcenter.com
- xakep.ru
- www.vice.com

Many of the above **blocked domains include Russian news media websites**, such as the (Kazakh language) website of the Russian TV Channel Tsargrad (which was reportedly blocked in Kazakhstan in August 2023), Sputnik and Pogrom (a socio-political online Russian nationalist publication that ran between 2012 to 2018), the 360 Russian satellite TV channel, the Ferghana Information Agency (a Russian media outlet covering news in Central Asia), and a Russian news website about Ukraine. Notably, the blocked Russian news media websites include Meduza, a Russian-language independent news website which was blocked in Russia following the invasion of Ukraine, and which remains blocked in Russia to date. The blocked websites also include the Kavkaz Center (a Chechen internet news agency), which is blocked in both Kazakhstan and Russia.

Apart from the blocking of Russian news media websites, OONI data also suggests that Kazakhstan **blocked access to a few Kyrgyz news media websites** as well. These include Kloop, one of the most popular news websites in Kyrgyzstan which is known for its journalism investigations. OONI data shows that access to Kloop is blocked in both Kazakhstan and Kyrgyzstan. Moreover, OONI data shows the blocking of Centralasia.media, a media organization based in Kyrgyzstan that covers news in Central Asia.

Vice News is the only international news media website that presented a strong signal of blocking in Kazakhstan based on our analysis. In fact, the OONI Probe testing of *www.vice.com* on multiple networks in Kazakhstan shows that almost all measurements were anomalous throughout the testing period. According to a Kazakh government website that provides information about blocking decisions, access to Vice News has been blocked in Kazakhstan since 2015 based on a court decision that determined that certain Vice News URLs spread terrorism and extremism related propaganda. These URLs point to a full-length video story (published by Vice in August 2014) about the Islamic State. Given that Vice News (like most websites these days) is hosted on HTTPS, ISPs in Kazakhstan cannot limit the block to a specific web page and therefore block the whole of `www.vice.com`.

All of the above news media domains presented a large volume of anomalies throughout the testing period (in comparison to the overall measurement volume), presenting an initial signal of blocking. This is illustrated through the following charts, which present an aggregate view of OONI measurements collected from the testing of the above 17 domains on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024.

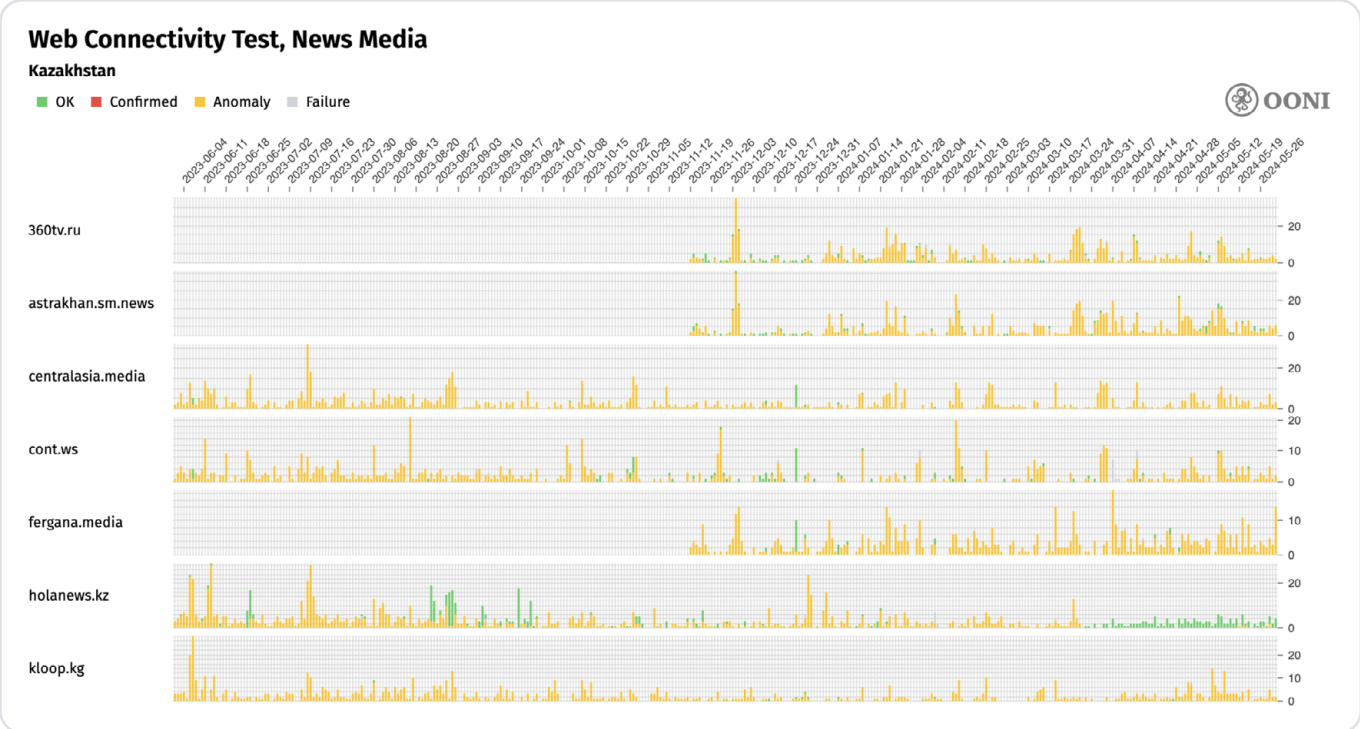


Chart: *OONI Probe testing of* `360tv.ru`, `astrakhan.sm.news`, `centralasia.media`, `cont.ws`, `fergana.media`, `holanews.kz`, *and* `kloop.kg` *on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

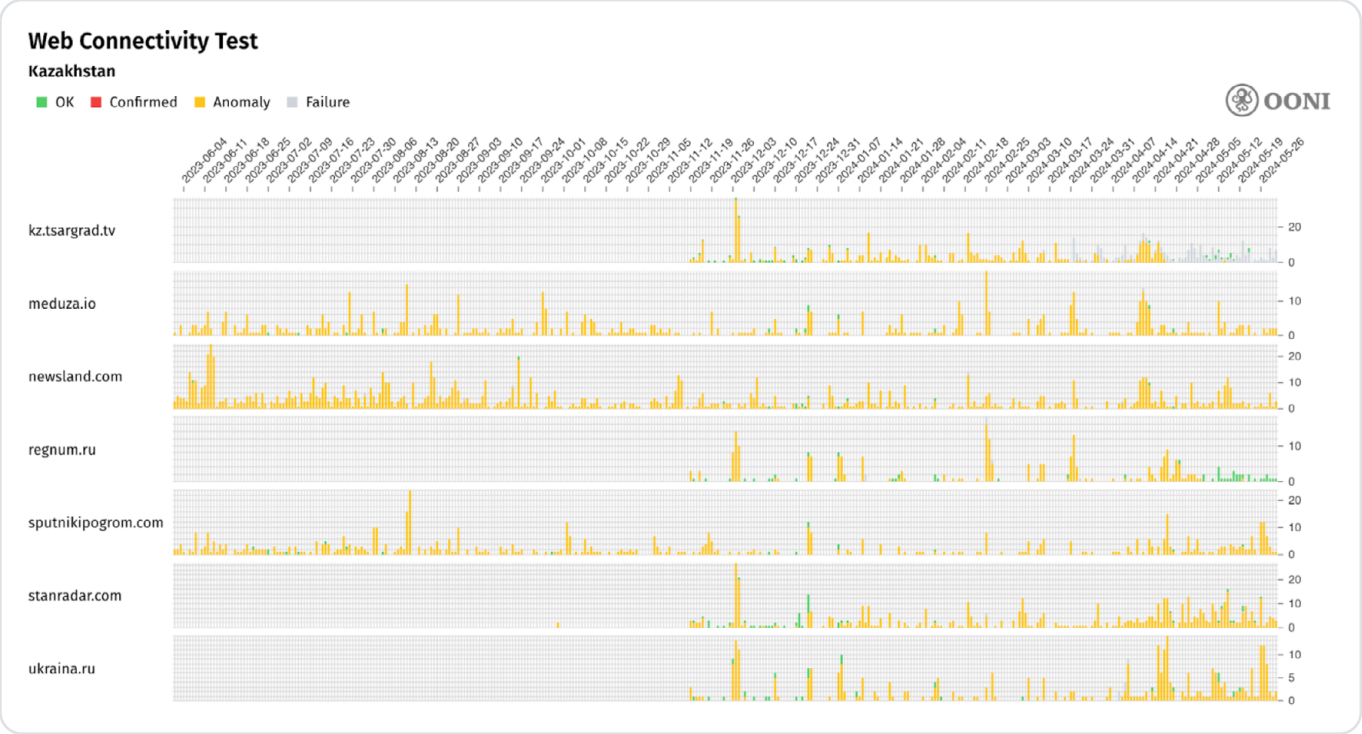


Chart: *OONI Probe testing of* `kz.tsargrad.tv`, `meduza.io`, `newsland.com`, `regnum.ru`, `sputnikipogrom.com`, `stanradar.com` *and* `ukraina.ru` *on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

Chart: *OONI Probe testing of* `www.kavkazcenter.com`, `xakep.ru` *and* `www.vice.com` *on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

From the above charts, it is evident that the vast majority of OONI measurements pertaining to the testing of these 17 news media domains presented anomalies throughout the analysis period. This suggests that access to these domains was blocked on tested networks in Kazakhstan. However, it's worth noting that the most recent measurements for `holanews.kz`, `xakep.ru` and `regnum.ru` were successful, suggesting that access may have recently been **unblocked** in Kazakhstan (at least on tested neworks).

While the persistent presence of anomalies provides a strong indicator of blocking, confirming and characterizing a block requires analyzing the reasons that caused the anomalies, while taking into account the factors that may have contributed towards false positives. To this end, we analyzed the anomalous measurements from these 17 domains to detect the specific failures that occurred during the experiments, which would enable us to understand at which point of the testing (e.g. DNS lookup, TLS handshake) the anomaly was triggered. We subsequently aggregated the failure types to evaluate whether and to what extent these failure types were consistent on each tested network throughout the analysis period, as a more consistent failure would serve as an indicator of a certain blocking technique and would provide a stronger signal of blocking.

As OONI Probe tests were performed on more than 30 ASNs in Kazakhstan during the analysis period (each with unequal measurement coverage), we limited our analysis to the ASNs that received both the largest measurement coverage throughout the analysis period (enabling us to trust those measurements more) and the strongest signals of blocking (i.e. most consistent failure types within anomalous measurements). These include AS9198 (JSC Kazakhtelecom), AS21299 (Kar-Tel LLC), AS44477 (STARK INDUSTRIES SOLUTIONS LTD), AS206026 (Kar-Tel LLC), AS41798 (JSC Transtelecom), AS9009 (M247 Europe SRL).

Based on this analysis, we produced the following chart.

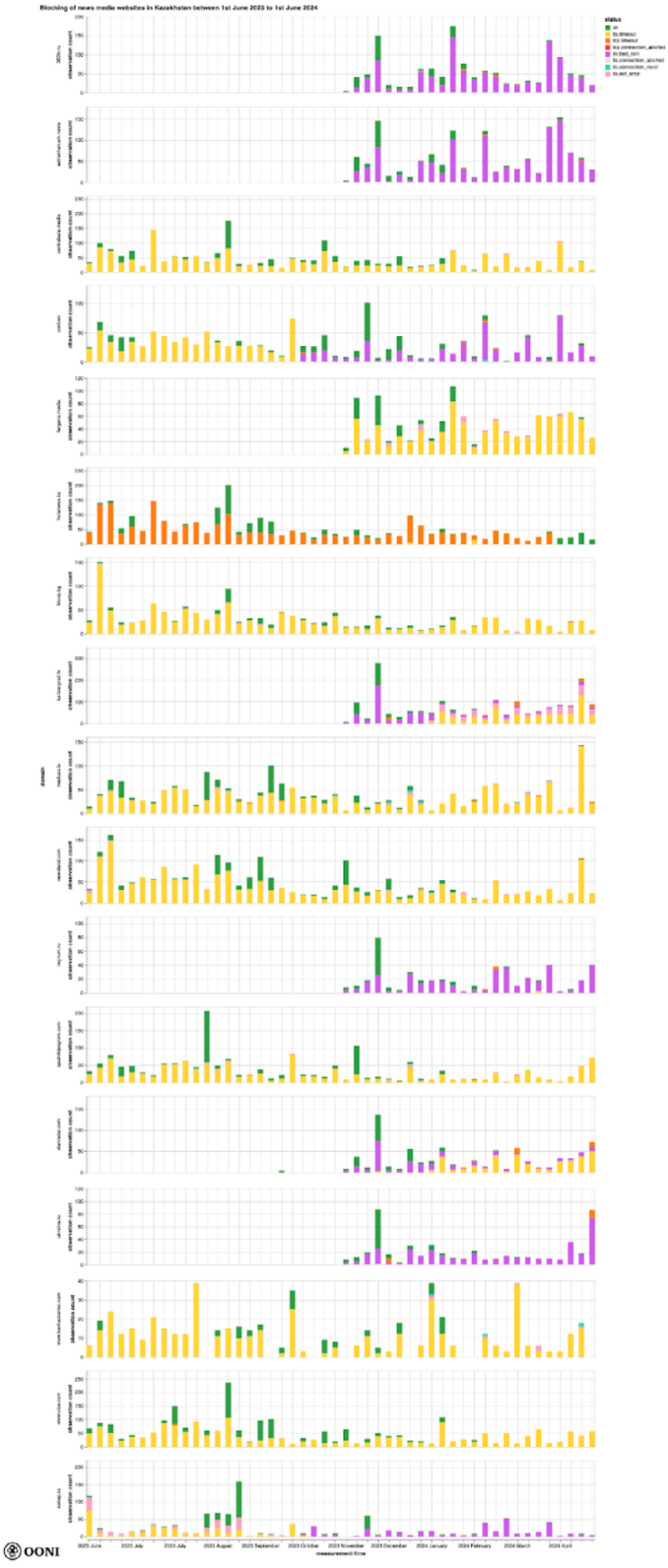


Chart: *OONI Probe testing of news media websites on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

As is evident, the majority of anomalous measurements from the OONI Probe testing of the above 17 news media domains in Kazakhstan presented signs of **TLS interference**. Specifically, OONI data shows that while DNS resolution returned consistent IPs and that it was possible to establish a connection to resolved IPs, the TLS handshake session timed out after the first Client Hello message (which is unencrypted), resulting in timeout errors. This consistent blocking technique – observed on multiple networks – gives us confidence in the findings, and suggests that ISPs in Kazakhstan may be using Deep Packet Inspection (DPI) technology to implement the blocks.

Image: *OONI measurement from the testing of* `kloop.kg` *in Kazakhstan on 14th May 2024 (source: OONI data).*

It's worth noting though that, for a few of the blocked news media domains (such as `360tv.ru`, `astrakhan.sm.news`, `ukraina.ru`, and `www.kavkazcenter.com`), we observe that ISPs in Kazakhstan returned **invalid TLS certificates**. This suggests the presence of TLS man-in-the-middle (MITM) attacks, which we discuss in more detail in a subsequent section of this report.

Blocking of Amnesty International and petition sites

Back in 2016, global petition platform Change.org was reportedly blocked in Kazakhstan for hosting a petition that called for the dismissal of then-prime minister Karim Massimov. Recent OONI data suggests that access to `www.change.org` remains blocked in Kazakhstan. But as part of our analysis, we also found other petition sites (`www.ipetitions.com` and `egov.press`) and the Russian language edition of Amnesty International's website blocked in Kazakhstan as well. According to Freedom House, petition websites were blocked in Kazakhstan to prevent campaigning.

Specifically, our analysis of OONI data collected from Kazakhstan over the last year (between 1st June 2023 to 1st June 2024) shows the **blocking of the following 4 human rights domains**:

- amnesty.org.ru
- egov.press
- www.change.org
- www.ipetitions.com

The above domains presented a large volume of anomalies throughout the testing period (in comparison to the overall measurement volume), presenting a signal of blocking. This is illustrated through the following chart, which presents an aggregate view of OONI measurements collected from the testing of the above 4 domains on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024.

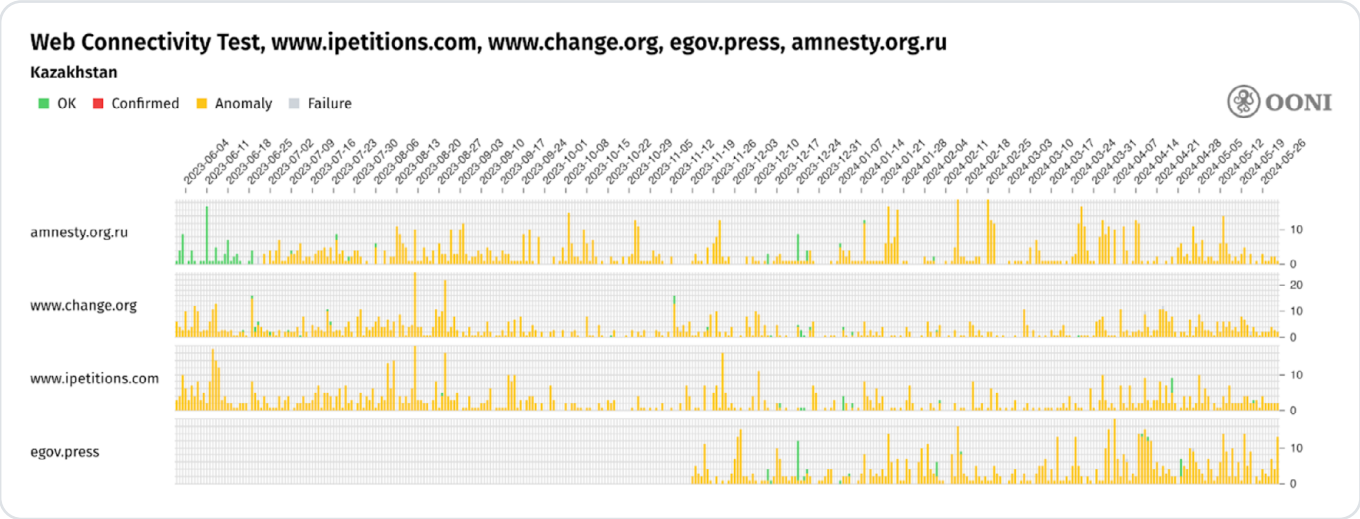


Chart: *OONI Probe testing of* amnesty.org.ru, egov.press, www.change.org *and* www.ipetitions.com *on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

From the above chart, it is evident that the vast majority of OONI measurements pertaining to the testing of these 4 human rights domains presented anomalies throughout the analysis period. This suggests that access to these domains was blocked on tested networks in Kazakhstan. Petition sites www.change.org and www.ipetitions.com presented anomalies throughout the entire analysis period, suggesting that their blocks were implemented before 1st June 2023 (the blocking of Change.org reportedly began in 2016). It's unclear when the blocking of egov.press began, given that the OONI Probe testing of this domain in Kazakhstan only started on 19th November 2023 (and most measurements thereafter presented anomalies).

However, the blocking of the Russian language edition of Amnesty International's website appears to have started during the analysis period of this study. Specifically, OONI data shows that while the testing of amnesty.org.ru in Kazakhstan was previously successful (showing that the site was accessible on tested networks), it mainly started presenting anomalies and signs of blocking from 30th June 2023 onwards. It's worth noting though that during the same analysis period, OONI data shows that Amnesty International's main, English language website was accessible (on tested networks) in Kazakhstan, as illustrated below.

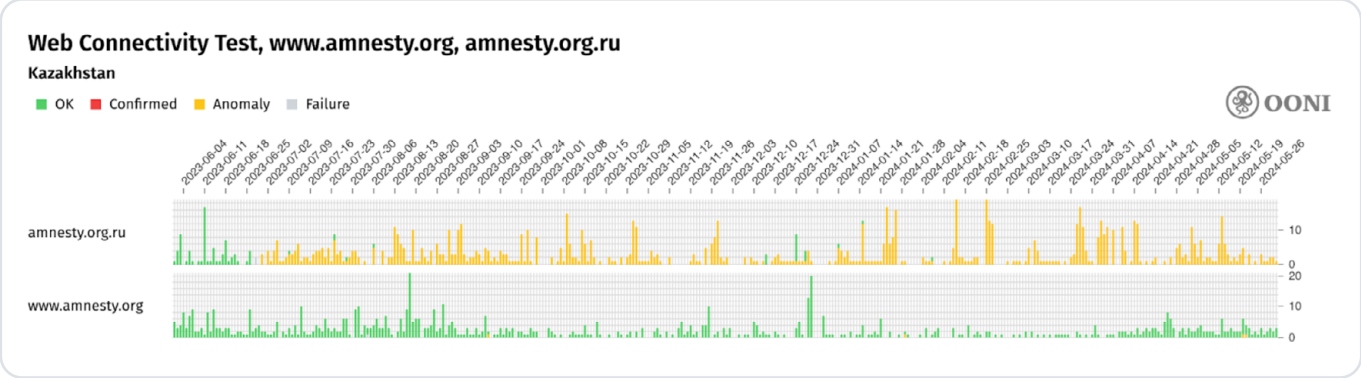


Chart: *OONI Probe testing of* `amnesty.org.ru` *and* `www.amnesty.org` *on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

The above comparison suggests that the Amnesty International block was targeted in nature, limited to censoring Russian language content which may have been more relevant for Kazakh audiences. The targeted blocking of (the Russian language edition of) Amnesty International's website is further suggested by the fact that OONI data shows that other international human rights websites (such as Human Rights Watch) were accessible in Kazakhstan during the analysis period.

Similarly to the blocking of news media websites (discussed previously), OONI data suggests that the blocking of these human rights websites is implemented by means of **TLS interference**, as we observe the timing out of the session after the Client Hello message during the TLS handshake. This is evident through the following chart, which aggregates the failure types observed in anomalous measurements.

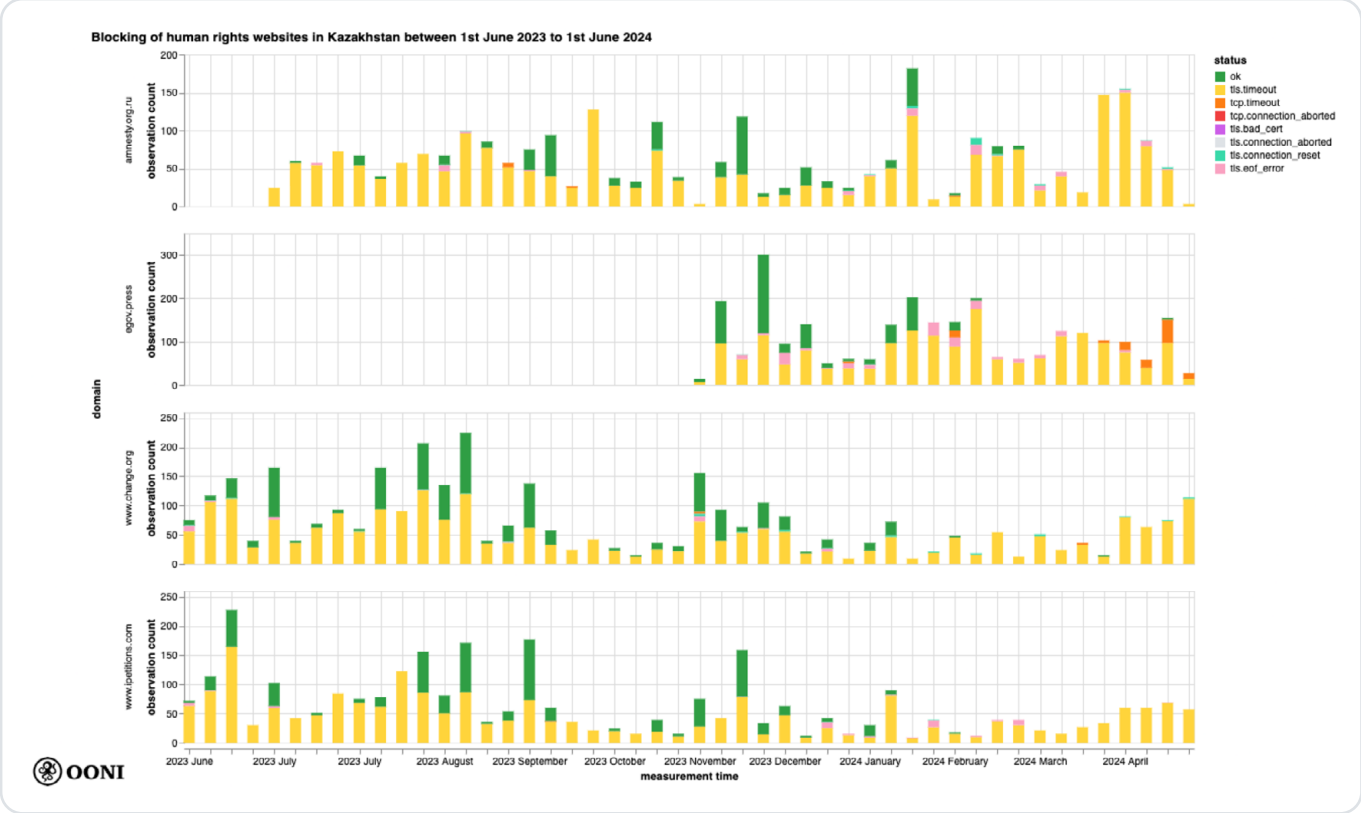


Chart: *OONI Probe testing of* `amnesty.org.ru`, `egov.press`, `www.change.org` *and* `www.ipetitions.com` *on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

As the TLS handshakes failed in the same way – resulting in the same timeout errors in the majority of measurements – we have a consistent signal which suggests that ISPs in Kazakhstan blocked access to the Russian language edition of Amnesty International's website and to several petition sites by means of TLS interference.

Blocking of circumvention tool websites

Circumventing internet censorship in Kazakhstan can potentially be challenging, as many censorship circumvention tool websites are blocked in the country. This is not too surprising, given that circumvention tools that provide access to materials blocked by court decisions and orders of state bodies are prohibited by law.

As part of our analysis, we detected the **blocking of 73 circumvention tool websites** in Kazakhstan. These include the following domains:

activpn.com
atlasvpn.com
belkavpn.com
borderlessvpn.io
browsec.com
cloudvpn.pro
disconnect.me
dotvpn.com
droidvpn.com
free-vpn.pro
fri-gate.org
getlantern.org
goosevpn.com
hide.me
hidemy.name
hit-tool.com
hola.org
i2p2.de
mac.eltima.com
mask-h2.icloud.com
mask.icloud.com
mrpvpn.com
mullvad.net
mybrowservpn.com
myvpn.run
netmap.su
nordvpn.com
openvpn.net
privateproxy.me
privatevpn.com
protonvpn.com
ringvpn.com
ru.vpnmentor.com
saturnvpn.com
speedify.com
strongvpn.com
supervpn.im
surfshark.com
ultravpn.com
usemyvpn.com
vpn.softok.info
vpnclientapp.com
vpnka.org
vpnki.ru
www.bananavpn.com
www.betternet.co
www.cyberghostvpn.com
www.expressvpn.com
www.gethotspotshield.com
www.gohotspotshield.com
www.hotspotshield.com
www.ivacy.com
www.keenow.com
www.netflixvpn.com
www.okayfreedom.com
www.pearlvpn.com
www.personalvpn.com
www.privateinternetaccess.com
www.privatevpn.biz
www.surfeasy.com
www.touchvpn.net
www.tunnelbear.com
www.urban-vpn.com
www.vpn.asia
www.vpnbook.com
www.vpngate.net
www.vpnmentor.com
www.vpnside.com
www.vpnuk.net
www.vyprvpn.com
zenmate.com
zenvpn.net
zoogvpn.com

Many more circumvention tool sites are potentially blocked in Kazakhstan, as the above list is limited to the domains that received the largest measurement coverage and the strongest blocking signals (based on our heuristics) during the analysis period.

Similarly to the blocking of news media and human rights websites (discussed previously), OONI data suggests that circumvention tool websites are blocked in Kazakhstan by means of **TLS interference** as well. Specifically, OONI data shows that while DNS resolution returned consistent IPs and it was possible to establish a connection to resolved IPs, we observed the timing out of the session after the Client Hello message during the TLS handshake. We consistently observe this pattern in the bulk of anomalous measurements pertaining to the testing of the above 73 domains. We illustrate this through the following chart (which we have limited to 18 of the above domains for readability purposes).

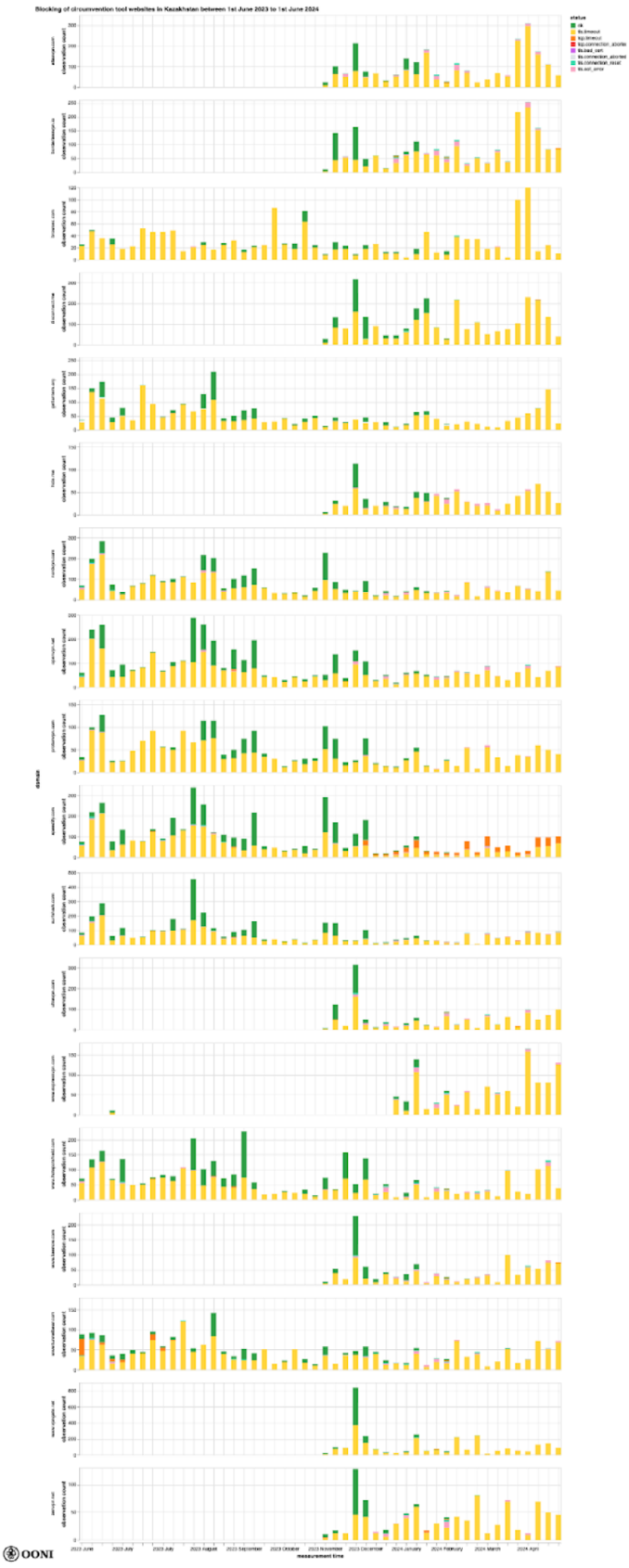


Chart: *OONI Probe testing of circumvention tool websites on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

This consistent pattern of TLS handshake timeout errors – observed on multiple networks in Kazakhstan – gives us confidence in the findings, and suggests that ISPs in Kazakhstan may be using Deep Packet Inspection (DPI) technology to implement the blocks.

The blocked domains include many popular circumvention sites, such as NordVPN, ExpressVPN, ProtonVPN, OpenVPN, TunnelBear, and Surfshark VPN. However, it's important to highlight that the blocking of a circumvention tool website does not necessarily mean that access to their VPN is blocked as well, nor that such a block is always effective – particularly since several circumvention tools have built-in techniques designed to evade blocks.

As OONI Probe mainly includes experiments designed to measure the reachability of two circumvention tools (Tor and Psiphon), it remains unclear to us whether the VPNs of the aforementioned (blocked) domains are blocked as well. It's worth noting though that during the analysis period, OONI data suggests that both Tor and Psiphon VPN were reachable (on tested networks) in Kazakhstan, as illustrated below.

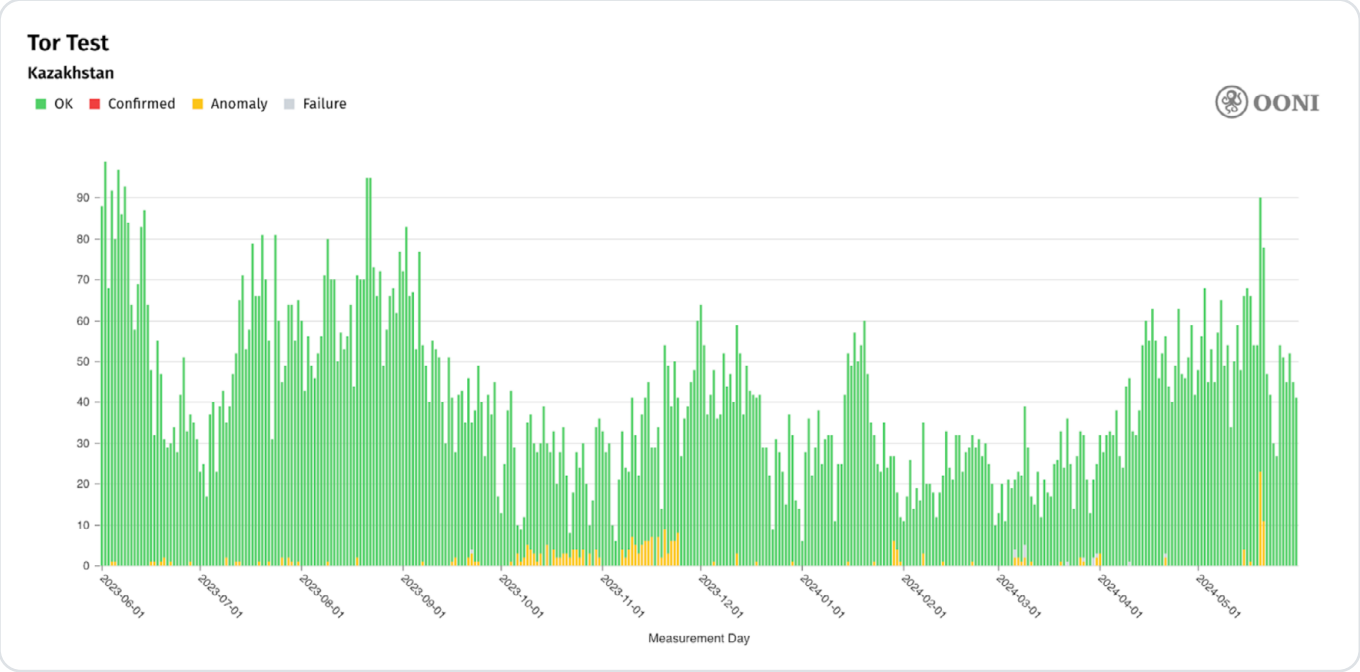


Chart: *OONI Probe testing of Tor on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

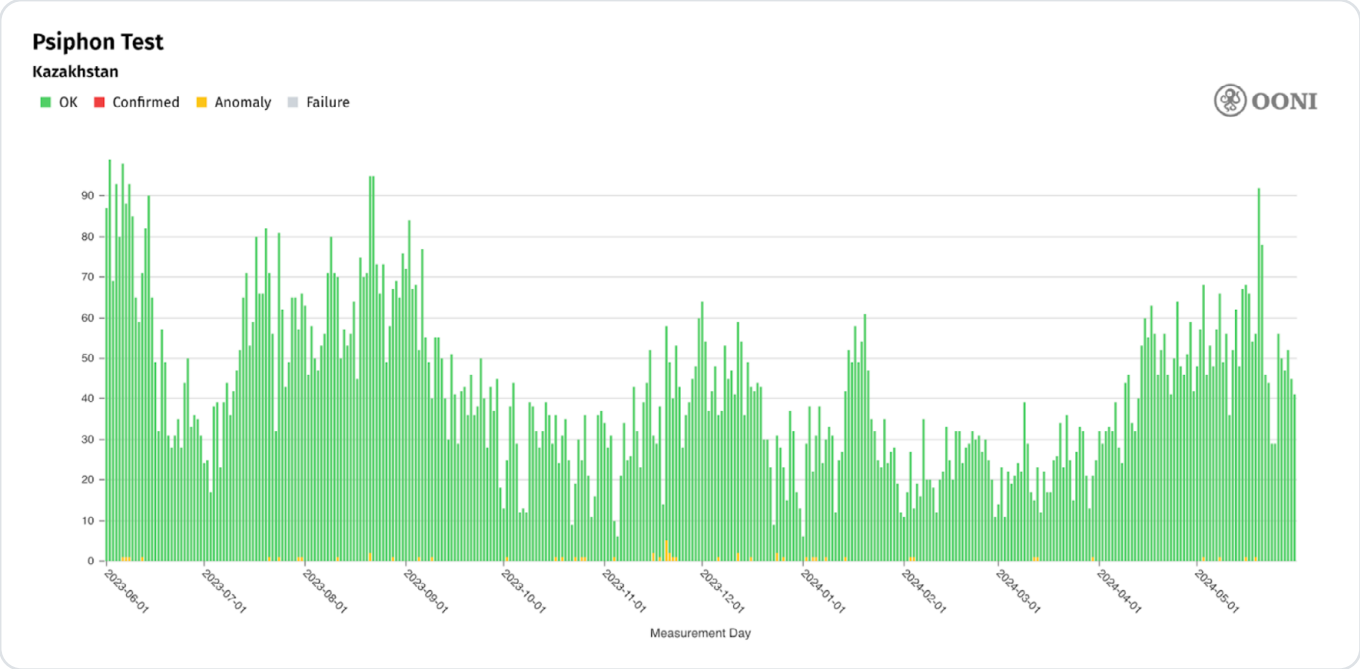


Chart: *OONI Probe testing of Psiphon VPN on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

The above charts suggest that internet users in Kazakhstan might be able to circumvent internet censorship through the use of Tor or Psiphon VPN. OONI data also shows that the Tor Project and Psiphon websites were accessible on tested networks in Kazakhstan during the analysis period, as illustrated below.

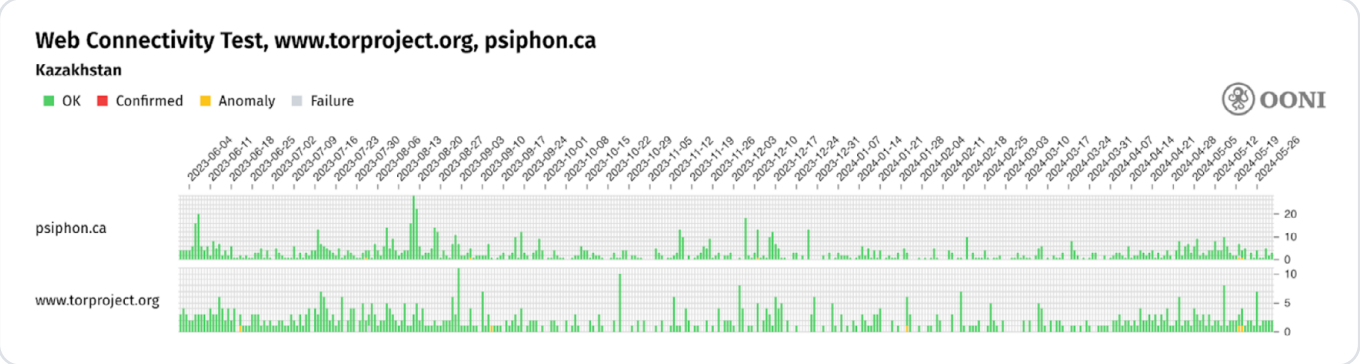


Chart: *OONI Probe testing of* `www.torproject.org` *and* `psiphon.ca` *on multiple networks in Kazakhstan between 1st June 2023 to 1st June 2024 (source: OONI data).*

TLS Man-In-The-Middle (MITM) attacks

Normally most web traffic is made secure using TLS, which is a technology that ensures your connection to a particular server is encrypted. When a government deploys a TLS man-in-the-middle (MITM) attack, they are able to not only block access to the service, but to also break the encryption. This allows them to gain access to the content of the communication of the user to the site or service, bypassing the layer of encryption. This will only work if a user has installed on their computer the government mandated root certificate authority, which is what browsers use to verify if the certificate presented by the server is issued by a known trusted authority.

According to Internet Freedom Kazakhstan, a security certificate with MITM technology was proposed for implementation in Kazakhstan in 2016, and the relevant amendments to the Law "On Communications" were adopted. In December 2020, during the cyber exercises Information Security Nur-Sultan-2020, users in Kazakhstan were sent SMS messages with information about installing a security certificate to maintain access to foreign internet resources. Government agencies claimed that this method is used exclusively to block prohibited content, including terrorist and extremist materials. It was also reported that the use of a security certificate is legal and necessary to protect the country from cyberattacks and combat prohibited content.

Ramil Bektemirov, a representative of JSC State Technical Service, at a briefing on the exercises held in Astana in 2020, answered a question about the use of MITM technology in a security certificate:

> *"The [MITM] technology is indeed used in the solution. This technology is used not only by us, but also by leading manufacturers of network protection equipment. They include functionality in this solution in order to inspect traffic. We understand that now 70% of our traffic is encrypted. And in order to inspect it, to see prohibited content that will need to be blocked, without this technology it is impossible".*

Kazakhstan has been known to use at least 4 different root CAs, which we summarize in the following table:

Common Name	Not Valid Before	Not Valid After	Links
НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ	Jul 27 04:47:00 2015 GMT	Jul 27 04:47:00 2020 GMT	mozilla.dev.security.policy thread • mozilla bug
Qaznet Trust Network	Feb 2 05:41:00 2016 GMT	Feb 2 05:41:00 2046 GMT	net4people bbs thread • censoredplanet report • archive.org cert • mozilla bug • mozilla blog post
Information Security Certification Authority CA	Feb 28 04:08:03 2020 GMT	Feb 28 04:08:03 2040 GMT	net4people bbs thread • censoredplanet post • archive.org cert • mozilla bug • mozilla blog post
Information Security Certification Authority	Feb 28 06:16:40 2020 GMT	Feb 28 06:16:40 2050 GMT	net4people bbs thread • ntc.party thread • crt.sh cert #1 • crt.sh cert #2 • crt.sh cert #3 • crt.sh cert #4 • mozilla bug

As part of our analysis, we found evidence in OONI data that Kazakhstan's government mandated root certificate authority was being used to implement TLS man-in-the-middle (MITM) attacks targeting a set of domains.

Specifically, OONI data from Kazakhstan shows that the following 14 domains were targeted by TLS MITM attacks:

360tv.ru
astrakhan.sm.news
compromat.ru
cont.ws
knews.kg
kz.tsargrad.tv
regnum.ru
rutracker.org
sproot.it
stanradar.com
ukraina.ru
www.for.kg
www.pinterest.com
xakep.ru

We are able to conclude that this is indeed a TLS MITM and not just DNS tampering leading to a page which contains an invalid certificate, since we were able to establish that the IP returned as part of DNS resolution is DNS consistent (in comparison to the IP returned from control measurements).

In previous years, TLS MITM attacks in Kazakhstan were reported in news outlets and at the time, Mozilla took actions to explicitly block that particular root CA from working in their browser.

At least 7 more root CAs with common name Information Security Certification Authority exist:

- https://crt.sh/?id=4833570779
- https://crt.sh/?id=4739909320
- https://crt.sh/?id=4633597326
- https://crt.sh/?id=3967758934
- https://crt.sh/?id=12281942153
- https://crt.sh/?id=11106964945
- https://crt.sh/?id=14682080594

In order to identify which was used to sign the intermediates seen in OONI measurements we ran this script.

In OONI data collected from Kazakhstan between 2021 to 2024, we found **7 distinct intermediate certificates** signed by **4 distinct root CAs** being used to carry out the TLS MITM. Each of these certificates has a relatively short duration period of validity of 75 days. This means that in order for the certificate chain to continue functioning properly, they would have to re-emit a new intermediate from their root CA at least every 74 days.

The root CAs we found used to sign intermediates in OONI data – while different from that previously reported by Censored Planet in 2019 and which, at the time, was added to the OneCRL list for revoking untrusted root CAs – are also present in the OneCRL list for Mozilla. The fact that they are part of the OneCRL for Mozilla means that their use is ineffective when accessed from a Firefox browser.

The following list summarizes the intermediates seen in OONI measurements and the relevant root CA used to sign them:

```
Fingerprint: c0e15a945595372030f0d45938ebb6081bb39fb5
Serial: 542829070264121061358597976201233251364726286334
Not valid before: 2021-06-18 12:54:34
Not valid after: 2021-09-01 12:54:34
Issuer: C=KZ,O=ISCA,CN=Information Security Certification Authority
Root CA Cert: https://crt.sh/?d=4739909320
Root CA Fingerprint: fabda72fa1f620c160420a496194b61f82a01b4a
Root CA Serial: 212762436239719553268722926518842178639864163027
Root CA Not valid before: 2020-02-28 06:46:02
Root CA Not valid after: 2040-02-28 06:46:02
```

OONI measurement

```
Fingerprint: 90f9aa29195ecbfbf2c943ab1d5102f3ec84a68c
Serial: 600636309019776433832878055409971857043873967144
Not valid before: 2021-08-19 12:39:14
Not valid after: 2021-11-02 12:39:14
Issuer: C=KZ,O=ISCA,CN=Information Security Certification Authority
Root CA Unknown
```

OONI measurement

```
Fingerprint: 8634ecaefb5d02463d2a9ce42178001154752561
Serial: 29369719831636072981245391652063645800889204772 8
Not valid before: 2023-08-09 06:33:35
Not valid after: 2023-10-23 06:33:35
Issuer: C=KZ,O=ISCA,CN=Information Security Certification Authority
Root CA Cert: https://crt.sh/?d=11106964945
Root CA Fingerprint: ea5d093c312e1a516937e153c06c2d82127b47d6
Root CA Serial: 394571478723635638549382697435194886177070445336
Root CA Not valid before: 2020-02-28 05:39:51
Root CA Not valid after: 2050-02-28 05:39:51
```

OONI measurement

```
Fingerprint: cb074692a22395fa615a89a86d877c9abc034867
Serial: 203432698505598047390349427507107109607746033885
Not valid before: 2023-11-02 09:03:07
Not valid after: 2024-01-16 09:03:07
Issuer: C=KZ,O=ISCA,CN=Information Security Certification Authority
Root CA Cert: https://crt.sh/?d=11106964945
Root CA Fingerprint: ea5d093c312e1a516937e153c06c2d82127b47d6
Root CA Serial: 394571478723635638549382697435194886177070445336
Root CA Not valid before: 2020-02-28 05:39:51
Root CA Not valid after: 2050-02-28 05:39:51
```

OONI measurement

```
Fingerprint: dfcd9dcb64edd86e333ad6247e2deda7dcf10ebd
Serial: 62182944575324169161449529886085187860306891706O
Not valid before: 2023-11-28 11:24:53
Not valid after: 2024-02-11 11:24:53
Issuer: C=KZ,O=ISCA,CN=Information Security Certification Authority
Root CA Cert: https://crt.sh/?d=12281942153
Root CA Fingerprint: 1375ebdcf56359aae0423e861ac8fc6231511ce6
Root CA Serial: 285540385527369649610289916863209926796774245522
Root CA Not valid before: 2020-02-28 06:16:40
Root CA Not valid after: 2050-02-28 06:16:40
```

OONI measurement

```
Fingerprint: 5d54c6afa4fd4685359875595565ae9f8caab914
Serial: 499633659418679795571951434192241531137344178316
Not valid before: 2024-03-20 05:50:15
Not valid after: 2024-06-03 05:50:15
Issuer: C=KZ,O=ISCA,CN=Information Security Certification Authority
Root CA Unknown
```

OONI measurement

```
Fingerprint: 76e9f2a52c149586be8f389d8a71ac41d3f423d1
Serial: 414124517712191942334357388114692622770498879745
Not valid before: 2024-08-23 10:46:59
Not valid after: 2024-11-06 10:46:59
Issuer: C=KZ,O=ISCA,CN=Information Security Certification Authority
Root CA Cert: https://crt.sh/?d=14682080594
Root CA Fingerprint: bfd7f531eca8e3d65b4738167b160b7a95a8d894
Root CA Serial: 6181551062104020837407701706100174036169357512S0
Root CA Not valid before: 2020-02-28 07:04:41
Root CA Not valid after: 2050-02-28 07:04:41
```

OONI measurement

While these are all technically different root CAs, we are considering them all part of the same incident in the table at the beginning of this section labeled as “Information Security Certification Authority” since they all share the same common name.

The root CAs seem to all share a very close issuance time, which seems to suggest that they may have all been generated in batch at some point in time to then rotate them over time as they get included inside of CRL lists.

Regarding the validity times of the intermediate certificates, it’s quite apparent that there is a gap in between the renewal of the certificates. Based on OONI data, we were able to confirm that even if internet users in Kazakhstan were to have installed the root certificate, as directed by the government, they would still have received certificate validation errors between 2nd November 2011 and 9th August 2023. Shorter windows of invalidity for the certificate can be observed between 23rd October 2023 and 28th November 2023, and then between 11th February 2024 and 20th March 2024.

What can be seen from the chart below is that these intermediate certificates were spotted in the wild and **being used to perform MITM even during periods of certificate invalidity**.

tls_end_entity_certificate_not_valid_before	tls_end_entity_certificate_not_valid_after	measurement_start_time	
2021-06-18 12:54:34+00:00	2021-09-01 12:54:34+00:00	2021-07-07 00:00:00+00:00	5
		2021-07-14 00:00:00+00:00	1
		2021-07-21 00:00:00+00:00	4
		2021-08-04 00:00:00+00:00	2
		2021-08-11 00:00:00+00:00	1
2021-08-19 12:39:14+00:00	2021-11-02 12:39:14+00:00	2021-08-18 00:00:00+00:00	1
		2021-08-25 00:00:00+00:00	2
		2021-09-01 00:00:00+00:00	4
		2021-09-08 00:00:00+00:00	1
		2021-09-15 00:00:00+00:00	2
		2021-09-22 00:00:00+00:00	4
		2022-04-13 00:00:00+00:00	2
		2022-04-20 00:00:00+00:00	1
2023-08-09 06:33:35+00:00	2023-10-23 06:33:35+00:00	2023-10-11 00:00:00+00:00	8
		2023-10-18 00:00:00+00:00	12
		2023-10-25 00:00:00+00:00	25
		2023-11-01 00:00:00+00:00	29
		2023-11-08 00:00:00+00:00	8
2023-11-02 09:03:07+00:00	2024-01-16 09:03:07+00:00	2023-11-15 00:00:00+00:00	68
		2023-11-22 00:00:00+00:00	127
		2023-11-29 00:00:00+00:00	505
		2023-12-06 00:00:00+00:00	3
2023-11-28 11:24:53+00:00	2024-02-11 11:24:53+00:00	2023-12-06 00:00:00+00:00	47
		2023-12-13 00:00:00+00:00	68
		2023-12-20 00:00:00+00:00	14
		2023-12-27 00:00:00+00:00	120
		2024-01-03 00:00:00+00:00	190
		2024-01-10 00:00:00+00:00	126
		2024-01-17 00:00:00+00:00	105
		2024-01-24 00:00:00+00:00	168
		2024-01-31 00:00:00+00:00	82
		2024-02-07 00:00:00+00:00	83
		2024-02-14 00:00:00+00:00	164
		2024-02-21 00:00:00+00:00	171
		2024-02-28 00:00:00+00:00	46
		2024-03-06 00:00:00+00:00	81
		2024-03-13 00:00:00+00:00	118
2024-03-20 05:50:15+00:00	2024-06-03 05:50:15+00:00	2024-03-20 00:00:00+00:00	157
		2024-03-27 00:00:00+00:00	131
		2024-04-03 00:00:00+00:00	185
		2024-04-10 00:00:00+00:00	168
		2024-04-17 00:00:00+00:00	134
		2024-04-24 00:00:00+00:00	176
		2024-05-01 00:00:00+00:00	23

This suggests that if users were to attempt to visit the sites affected by the MITM and had installed the root CA, they would still be getting an error.

It's unclear to us why they went through the hassle of telling users to install the root CA, but then failed to keep the intermediates up to date in order to effectively carry out a MITM attack, even when users were fully compliant with government orders. We can only speculate that this is either due to some misconfiguration in the periodic renewal task (although for the first certificate we see the time window of invalidity is almost 2 years), or that for 3 times they forgot to renew their certificates on time.

Based on OONI data, we were able to confirm that this root CA was being used to sign intermediate certificates that were then being used to carry out MITM attacks targeting users in Kazakhstan on at least 19 different networks and at least 14 distinct domain names.

Specifically, we found evidence of a TLS MITM on the following 19 networks:

- Uplink LLC (AS8200)
- TimeWeb Ltd. (AS9123)
- JSC Kazakhtelecom (AS9198)
- "Mobile Business Solution" MBS LLP (AS15736)
- Kar-Tel LLC (AS21299)
- Kcell JSC (AS29355)
- Mobile Telecom-Service LLP (AS29555)
- Jusan Mobile JSC (AS35104)
- JSC Alma Telecommunications (AS39824)
- BTcom Infocommunications Ltd. (AS41124)
- JSC Transtelecom (AS41798)
- OBIT-telecommunications, LLC (AS43370)
- SMARTNET TOO (AS43994)
- STARK INDUSTRIES SOLUTIONS LTD (AS44477)
- ForteBank JSC. (AS48502)
- Mobile Telecom-Service LLP (AS48503)
- PS Internet Company LLP (AS48716)
- JSC Kazakhtelecom (AS50482)
- Kar-Tel LLC (AS206026)

The fact that so many distinct ISPs are implementing the MITM using the same certificate seems to suggest a high level of coordination amongst distinct providers and a fairly high level of compliance.

Legal environment

Absolute freedom of expression is not allowed in Kazakhstan. However, Article 5 of the Constitution of the Republic of Kazakhstan proclaims that: 'Ideological and political diversity shall be recognised in the Republic of Kazakhstan'. At the same time, the exercise of human and civil rights and freedoms must not violate the rights and freedoms of other persons, or infringe on the constitutional order and public morality. Propaganda or agitation for a violent change in the constitutional order, violation of the integrity of the Republic, undermining the security of the state, war, social, racial, national, religious, class and tribal superiority, as well as the cult of cruelty and violence are not allowed (Articles 12, 20 of the Constitution of the Republic of Kazakhstan).

Article 20 of the Constitution of the Republic of Kazakhstan guarantees freedom of speech: *'Everyone has the right to freely **receive and share information** by any means not prohibited by law. Censorship is prohibited.'* The constitutional right guaranteed by Paragraph 2 of Article 20 of the Constitution is realized within the limits and in accordance with the procedure determined by laws and is not included in the list of rights and freedoms established by Paragraph 3 of Article 39 of the Primary Law, which are not subject to restriction in any cases. Under Article 39, Paragraph 1, of the Constitution, the right to freedom of expression may be restricted by laws to the extent necessary to **protect the constitutional order, public order, human rights and freedoms, public health and public morals.**

The only legal definition of censorship is given in the Law of the Republic of Kazakhstan from 23 July 1999 No. 451-I 'On Mass Media':

> *"censorship is the **prior approval** of messages and materials by the mass media with state bodies, officials and other organisations at their request or on other grounds for the purpose of restricting or banning the dissemination of messages and materials or parts thereof".*

This definition, firstly, attributes a possible restriction or ban on the dissemination of messages and materials **exclusively to the activities of the mass media**, and secondly, refers to a ban on **prior approval**, not a restriction or ban on already published materials and messages.

It seems more relevant to interpret censorship in a broader sense, for example, according to the definition given in Wikipedia: "Censorship is the suppression of speech, public communication, or other information. This may be done on the basis that such material is considered objectionable, harmful, sensitive, or 'inconvenient'. Censorship can be conducted by governments, private institutions."

In this context, the legislation in Kazakhstan provides state bodies with broad powers to supervise the dissemination of information, including on the Internet. Thus, the Law of the Republic of Kazakhstan dated 23 July 1999 No. 451-I 'On Mass Media' (hereinafter – Mass Media Law) contains the concept of **media monitoring** – the process of collecting media sources and analyzing them for compliance with the legislation of the Republic of Kazakhstan. In accordance with legislative acts, a number of state bodies share these similar functions.

At the same time, the issue of limiting or restricting **access to illegal information**, i.e. information contrary to the laws of the Republic of Kazakhstan, inevitably arises.

What information is considered illegal in Kazakhstan can be illustrated by the example provided on the official website of the Ministry of Information and Public Development of the Republic of Kazakhstan 'Share a complaint about Internet content'. This page invites all interested citizens to report Internet resources distributing information violating the legislation of the Republic of Kazakhstan to the authorized body, represented by the Information Committee of the Ministry of Information and Public Development of the Republic of Kazakhstan. Based on the shared reports, the Ministry will carry out all necessary measures to suspend the spread of illegal information on the territory of the country.

At the same time, the Ministry distinguishes the following types of illegal information:

1. **Propaganda of suicide;**
2. **Propaganda of drugs, psychotropic substances, their analogues and precursors;**
3. **Propaganda or agitation of cruelty and violence, social, racial, national, religious, class and tribal superiority;**
4. **Demonstration of film and video products of pornographic and special sexual and erotic nature;**
5. **Conducting election campaigning;**
6. **Propaganda or agitation for violent change of the constitution;**
7. **Violation of the integrity of the Republic of Kazakhstan;**
8. **Propaganda of extremism or terrorism;**
9. **Publication of materials and dissemination of information aimed at inciting interethnic and inter-confessional hatred;**
10. **Online casinos;**
11. **Unfair, inaccurate advertising;**
12. **Others.**

Review of Internet regulation and legislation focused on access to information

According to the Law of the Republic of Kazakhstan dated 16 November 2015 No. 401-V 'On Access to Information': "***information*** *– information about people, objects, facts, events, occurrences and processes recorded in any form"*. This study focuses on information recorded in a form that allows sharing it on the Internet.

In accordance with the definitions given in the Law of the Republic of Kazakhstan dated 24 November 2015 No. 418-V 'On Informatisation', the **Internet** is a worldwide system of united telecommunications networks and computing resources for the transmission of electronic **information resources**. **Electronic information resources** are information in digital form contained on electronic media and in the **objects of informatisation**. In this context, we are primarily interested in such an object of information as an **Internet resource**. An **Internet resource** is **information** (in text, graphic, audiovisual or other form) placed on **hardware or software** having a unique network address and (or) domain name and **functioning on the Internet**.

Under the Mass Media Law, **any Internet resource may be recognised as a mass media outlet**. The new law 'On Mass Media' unites online publications and news agencies into a single term 'Internet outlet'. Internet publications will be considered a type of mass media and will be subject to registration in accordance with the law.

However, there are two procedures for limiting or suspending access to information on Internet resources.

The first one addresses online media. An Internet resource, the information and communication infrastructure of which is located in the territory of the Republic of Kazakhstan, may undergo the procedure of registration with the authorized body (currently the Ministry of Culture and Information of the Republic of Kazakhstan). In this case, it acquires the status of an **online media**.

Limitation of access or suspension of the publication or limitation of the distribution of information of online media is possible by **the decision of the media's owner or a court**.

The dissemination of information by foreign Internet resources that violates the Constitution of the Republic of Kazakhstan and the norms of the Mass Media Law shall be subject to judicial suspension of access to the said Internet resources in the territory of the Republic of Kazakhstan.

The enforcement of a court decision on suspension when the media outlet is an Internet resource shall entail a ban on the use of a domain name with the same or duplicate name for a period not exceeding three months. A court decision on termination, when the mass media outlet is an Internet resource, shall entail cancellation of domain name registration and a ban on the use of a domain name with the same or duplicate name, the registration of which was canceled by the court decision, for a period of one year.

The activity of all other Internet resources may be suspended **without a court decision** by authorized state bodies (their competence will be discussed further below).

According to the Mass Media Law, suspension is allowed for a period not exceeding three months. Grounds for suspension include:

- propaganda or agitation of the cult of cruelty and violence,
- propaganda or agitation of social, racial, national, religious, class and tribal superiority,
- disclosure of information constituting state secrets or other secrets protected by law,
- dissemination of information advocating suicide,
- propaganda of drugs, psychotropic substances, their analogues and precursors,
- dissemination of television, radio programmes, television, radio channels,
- demonstration of pornographic and special-sex film and video productions,
- use of mass media to violate the conditions of election campaigning,
- carrying out activities by foreigners, stateless persons, foreign legal entities and international organisations that hinder and (or) promote the nomination and election of candidates, political parties that have nominated a party list, achieving a certain result in the elections,
- campaigning during the period of its prohibition,
- forcing to participate or refuse to participate in a strike,
- violation of the legislation of the Republic of Kazakhstan on the right for organising and holding peaceful assemblies,
- on copyright and related rights on the Internet,
- violation of the requirements for updating the registration of the service.

Grounds for termination are:

- propaganda or agitation for violent change of the constitution,
- violation of the integrity of the Republic of Kazakhstan,
- undermining the security of the state,
- propaganda of war,
- propaganda of extremism or terrorism,
- publication of materials and dissemination of information aimed at inciting interethnic and inter-confessional hatred,
- failure to eliminate the reasons for the suspension of a media outlet, or
- failure to eliminate the reasons that previously served as the basis for the suspension of the Internet resource within the established period of time.

It is also prohibited to use the media to commit **criminal and administrative offenses**, which also covers the prohibitions contained in the Mass Media Law:

- prohibition of advertisement of alcoholic beverages, products imitating alcoholic beverages, tobacco and tobacco products;
- prohibition of activities of a financial (investment) pyramid scheme,
- placement of information on vacancies for employment containing requirements of a discriminatory nature in the field of labor,
- placement of information on goods (jobs, services) with an indication of price (tariffs, rates, rates) not in tenge,
- publication of personal and biometric data, including information about his/her/their parents and other legal representatives,
- publication of other information allowing identification of the person,
- publication of information about the child who suffered as a result of illegal action (or inaction);
- publication of information about minors suspected and (or) accused of committing administrative and (or) criminal offenses, cyberbullying.

The elements of administrative and criminal offenses in which Internet resources can be used to commit the offenses are much broader. Therefore, it seems unnecessary to specify all of them in the Mass Media Law.

In case of suspension or termination of a media outlet identified as an Internet resource, authorized state bodies, or owners of Internet resources shall suspend or terminate the media or distribution of the products of the media outlet in the territory of the Republic of Kazakhstan.

Also, according to Paragraph 7 of Article 35 of the Law of the Republic of Kazakhstan dated 24 November 2015 No. 418-V 'On Informatisation':

> *"In case of dissemination of information prohibited by an enforceable court decision or laws of the Republic of Kazakhstan via telecommunication networks, or access to which has been temporarily suspended by an instruction on the elimination of violations of the law by the Prosecutor General of the Republic of Kazakhstan, or his deputies, an authorized body, authorized bodies, owners or owners of Internet resources are obliged to take immediate measures to restrict access to prohibited information".*

Judicial and extrajudicial procedure for suspension and termination of access to Internet resources

According to the current legislation of the Republic of Kazakhstan, **any information published on any Internet platform** may be reviewed by Kazakhstan's authorized state bodies for compliance with national legislation.

Article 41-1 of the Law of the Republic of Kazakhstan dated 5 July 2004 No. 567-II 'On Communications' generally prohibits access to Internet resources and (or) information published on them in order to access information prohibited by an enforceable **court decision** or the **laws of the Republic of Kazakhstan**. However, it does not specify whether the court order is required to recognise information as illegal, or simply the presence of the fact of prohibition in the laws of the Republic of Kazakhstan is sufficient.

As for the judicial procedure, there may be a general procedure, when an authorized body or prosecutor's office applies with a statement of claim to terminate access to an Internet resource.

When determining the jurisdiction of cases on the recognition of products of foreign media distributed in the territory of Kazakhstan, containing information contrary to the legislative acts of the Republic, as illegal, the jurisdiction will be determined at the **location of the applicant**.

In addition, it should be noted that according to Article 466 of the Civil Law Code of the Republic of Kazakhstan, the courts of the Republic of Kazakhstan also consider cases with the participation of foreign citizens in cases where:

1) the management body, branch or representative office of the foreign person is located in the territory of the Republic of Kazakhstan;
2) the defendant has property in the territory of the Republic of Kazakhstan;

[...]

6) the claim arises from a contract under which full or partial performance must take place or has taken place in the territory of the Republic of Kazakhstan;

[...]

9) **in a case on protection of honour, dignity and business reputation, the plaintiff is a resident of the Republic of Kazakhstan;**
10) in a case for the protection of the privacy rights, including compensation for losses and (or) compensation for moral damage, the plaintiff is a resident of the Republic of Kazakhstan.

Also, the termination of access to Internet resources may be carried out through the special proceedings, i.e. without the presence of the defendant.

The Code of Civil Procedure of the Republic of Kazakhstan of 31 October 2015, No. 377-V, Chapter 47, allows the recognition of **information materials imported, published, produced and/or distributed in the territory of the Republic of Kazakhstan as extremist or terrorist**. A prosecutor shall file an application with the court at the place where such materials are found, stating that the information materials contain signs and (or) appeals to extremism or terrorism. The court, having recognised information materials imported, published, produced and (or) distributed in the territory of the Republic of Kazakhstan as extremist or terrorist, shall issue a decision to ban the import, publication, production and (or) distribution of information materials in the territory of the Republic of Kazakhstan.

Chapter 48 of the Code of Civil Procedure of 31 October 2015, No. 377-V, allows application-based proceedings to declare the production of **a foreign media outlet distributed in the territory of the Republic of Kazakhstan** containing information contrary to the laws of the Republic of Kazakhstan illegal. The application shall be filed by citizens and legal entities whose legitimate interests have been affected by the products of a foreign media outlet, or by a prosecutor, or by an authorized body with the court, in writing or in the form of an electronic document at the location of the applicant. The court, having recognised that the production of a foreign media outlet distributed in the territory of the Republic of Kazakhstan contains information contrary to the laws of the Republic of Kazakhstan and therefore is illegal, shall issue a decision to suspend or stop the distribution of the production of the foreign media outlet in the territory of the Republic of Kazakhstan. The court judgment is sent to the relevant State body. Thus, in this case we are talking about foreign media, which includes, as mentioned above, Internet resources. However, the Kazakhstan legislation does not establish criteria for classifying mass media, including Internet resources, as foreign.

In addition, access to Internet resources and (or) information posted on them may be blocked without a court decision on the basis of Article 41-1 of the Law of the Republic of Kazakhstan dated 5 July 2004 No. 567-II 'On Communications'. This article states that in cases when networks and (or) means of communication are used for criminal purposes detrimental to the interests of the individual, society and the state, as well as for the dissemination of information that violates the legislation of the Republic of Kazakhstan on elections, contains calls for extremist and terrorist activities, mass riots, or for participation in mass (public) events held in violation of the established law, promoting sexual exploitation of minors and child pornography for the purposes of cyberbullying in relation to a child, containing advertisements of electronic casinos, internet casinos, as well as advertisements of gambling and (or) betting organized and conducted by a person who does not have the right to engage in gambling activities in the Republic of Kazakhstan, the Prosecutor General of the Republic of Kazakhstan or his deputies shall make a submission to the national security authorities of the Republic of Kazakhstan on taking measures to temporarily suspend the operation of networks and (or) means of communication, provision of communication services.

In cases where information prohibited or otherwise restricted by **judicial acts or laws of the Republic of Kazakhstan that have entered into legal force**, or access to which has been temporarily suspended by a submission of the **Prosecutor General of the Republic of Kazakhstan or his deputies** to eliminate legal violations, telecommunications operators and (or) owners and (or) legal representatives of online platforms, and (or) a state technical service, upon the order of the authorized authority, are obliged to take immediate measures to restrict access to prohibited information.

Also, in cases that cannot be delayed and may lead to the commission of grave and especially grave crimes, as well as crimes prepared and committed by a criminal group, the **Chairman of the National Security Committee of the Republic of Kazakhstan, his deputies or heads of territorial bodies of the National Security Committee of the Republic of Kazakhstan**, or persons working in their stead, have the right to suspend access to Internet resources and (or) information posted on them for the **benefit of all subjects of operational and investigative activity**, followed by notification of authorized bodies in the field of communications, the media and the Office of the Procurator-General of the Republic of Kazakhstan within twenty-four hours.

Joint Order of the Chairman of the National Security Committee of the Republic of Kazakhstan dated 15 February 2017 № 5/for official use, Minister of Information and Communications of the Republic of Kazakhstan dated 2 March 2017 № 82 for official use, Minister of Finance of the Republic of Kazakhstan dated 15 March 2017 № 168 for official use, Minister of Defence of the Republic of Kazakhstan dated 9 March 2017 № 49/44 for official use, Head of the State Protection Service of the Republic of Kazakhstan dated 10 March 2017 № 11-58 for official use, Chairman of the Agency of the Republic of Kazakhstan for Public Service and Counteraction to Corruption dated 3 March 2017 № 3 Director of the Foreign Intelligence Service of the Republic of Kazakhstan 'Syrbar' dated 22 February 2017 № 4, Minister of Internal Affairs of the Republic of Kazakhstan dated 28 February 2017 № 41 for official use 'On Approval of the Rules for Suspension of Networks and (or) means of communication, provision of communication services, access to Internet resources and (or) information placed on them' has the 'For Official Use' stamp.

Government Decree No. 347 from 13 April 2005 approved a list of State bodies which, in conjunction with an authorized body, have the right to suspend the operation of communications networks and facilities in the event of a threat or emergency of a social, natural or man-made nature or the introduction of a state of emergency:

1. General Prosecutor's Office of the Republic of Kazakhstan.
2. The National Security Committee of the Republic of Kazakhstan.
3. Ministry of Internal Affairs of the Republic of Kazakhstan.
4. Ministry of Defence of the Republic of Kazakhstan.
5. Ministry of Emergency Situations of the Republic of Kazakhstan.

The national security authorities of the Republic of Kazakhstan and (or) the authorised body in the field of mass media shall, within one hour of receipt of a submission on the elimination of legal violation, send an instruction to telecommunications operators, owners and (or) legal representatives of online platforms and (or) to the state technical service to take measures for its implementation.

Telecom operators, owners and (or) legal representatives of online platforms and (or) state technical service:

1. Upon receipt from the authorized body related to mass media and (or) from the national security bodies of the Republic of Kazakhstan of an instruction to take measures to implement the submission or decision specified in paragraphs 1, 1-1 and 1-2 of this Article, shall be obliged to implement it within no more than two hours by temporarily suspending the operation of networks and (or) means of communication, provision of communication services, access to Internet resources and (or) information posted on them, unless otherwise established by the laws of the Republic of Kazakhstan;

2. Assist the national security bodies of the Republic of Kazakhstan and law enforcement agencies of the Republic of Kazakhstan in identifying a person using networks and (or) means of communication for criminal purposes detrimental to the interests of the individual, society and the state, as well as for dissemination of information that violates the election legislation of the Republic of Kazakhstan, containing calls for extremist and terrorist activities, mass riots, as well as for participation in mass (public) events held in violation of the legislation of the Republic of Kazakhstan.

Special state bodies of the Republic of Kazakhstan and law enforcement agencies of the Republic of Kazakhstan shall, within the limits of their competence, take operational-search, counter-intelligence and criminal procedural measures to identify and bring to justice the person who disseminated prohibited information.

The authorized body in the industry of mass media shall send a notice to the person who disseminated the information referred to in paragraph 1 of this Article with a requirement to take measures to remove it within six hours of receipt of the notice.

If a person who uses networks and (or) means of communication for criminal purposes damaging the interests of an individual, society and the state, or for dissemination of information violating the election legislation of the Republic of Kazakhstan, for sharing calls for extremist and terrorist activities, mass riots, or participation in mass (public) events held in violation of the established law, for the purpose of cyberbullying against a child, has deleted it, he/she shall send a notification about it to the authorized agency of the Republic of Kazakhstan.

Upon receipt of the notification specified in Paragraph 4 of this Article and verification of its accuracy, the authorized body in the field of mass media shall instruct telecommunications operators and/or owners and/or legal representatives of online platforms and/or the state technical service to cancel the prescription specified in Paragraphs 1-1 and 2 of this Article and resume access to the Internet resource in accordance with the procedure determined by the authorized body in industry of mass media.

Telecom operators and/or owners and/or legal representatives of online platforms, and/or the state technical service, upon receipt of the instruction specified in Paragraph 5 of this Article from the authorized body in the industry of mass media, is obliged to execute it immediately.

Order No. 409 of the Minister of Information and Public Development of the Republic of Kazakhstan, dated 27 September 2022 established the Rules of interaction of state bodies on issues of **compliance with the requirements of the legislation of the Republic of Kazakhstan for telecommunications networks**. It should be noted here that in fact the rules do not refer to compliance with requirements, but to the detection of violations: 'State bodies shall form and send to the authorized body a list of employees, including subordinate organizations, who within their competence **identify and keep records of materials** distributed in telecommunications networks and add **Internet resources and URLs** containing information violating the legislation of the Republic of Kazakhstan, into the information system according to the format'.

When sending a notification, the public authority must ensure that the information entered into the information system is lawful and justified, as well as screenshots of the identified materials confirming their unlawfulness.

The Rules do not clarify **how many employees should be involved in identifying where exactly on the Internet they should search or which methods they should use to search for prohibited information**, but only mention that this 'shall be carried out **within their competence**'.

However, their competence is also questionable. There is no mention of any joint work in the Rules – according to the notifications received from the state authorities, it is up to the Ministry of Culture and Information of the Republic of Kazakhstan, likely on the basis of some additional knowledge of its employees, to confirm or not to confirm the fact of illegality of the information.

The Order No. 84 of the Minister of Information and Public Development of the Republic of Kazakhstan, dated 29 April 2019 introduces the **Methods of media monitoring in the territory of the Republic of Kazakhstan**. According to these Methods, monitoring of media distributed in the territory of the Republic of Kazakhstan is conducted by an authorized body in the media, television and radio broadcasting industry in order to **identify and record violations of the legislation of the Republic of Kazakhstan**. The object of monitoring includes Internet resources and online publications.

Carrying out media monitoring, according to these Methods, includes the following stages:

1. Viewing (or listening) of the media resources, identification, recording and collection of violations;
2. Legal analysis and generalization of reports on violations in the media;
3. Additional analysis of the identified cases of law violation, conducted by the authorized body.

Based on the results of monitoring, the following information is indicated: for online publications, news agencies and Internet resources – the name of the owner of the online publication, news agency, Internet resource, legal address, IP address of the Internet resource, if available – official email address. If it is impossible to establish information about the owner of the Internet resource, the authorized body shall send a notice to the hosting provider on whose server it is placed.

In order to carry out technical and methodological support of media monitoring, the authorized body, per budget legislation, contracts an organization performing work on technical and methodological support of monitoring (hereinafter referred to as the organization).

The authorized body, with methodological and technical support, including by obtaining **information from the organization**, lists violations of the law of the Republic of Kazakhstan identified through the monitoring of media products, as well as those **reported by the state bodies**, or through the **appeals from individuals and legal entities, or through the requests from officials** sent to the authorized body. That is, back in 2019, it was assumed that some reports of the presence of illegal information should come from state bodies to the Ministry of Information and Social Development of the Republic of Kazakhstan should be received, but now it has been fixed in a mandatory manner.

The Letter of the Committee for Communications No. 30-30-7/2454-I, by Informatisation and Information of the Ministry of Investment and Development of the Republic of Kazakhstan, dated 18 April 2016 clarifies that the organization is the Republican State Enterprise on the right of economic management **'Centre for Analysis and Information'** established following the Resolution of the Government of the Republic of Kazakhstan dated 9 July 2012 No. 925.

The organization monitors the mass media for compliance with: the Constitution of the Republic of Kazakhstan, the Constitutional Laws of the Republic of Kazakhstan 'On State Symbols of the Republic of Kazakhstan', 'On the First President of the Republic of Kazakhstan – Leader of the Nation', 'On the President of the Republic of Kazakhstan', the Code of the Republic of Kazakhstan 'On People's Health and Health Care System', the Laws of the Republic of Kazakhstan 'On Mass Media', 'On Television and Radio Broadcasting', 'On Advertising', 'On Culture', 'On Countering Terrorism', 'On Countering Extremism', 'On National Security of the Republic of Kazakhstan', 'On the Rights of the Child in the Republic of Kazakhstan', and 'On the Rights of the Child in the Republic of Kazakhstan'.

The process of monitoring Internet resources is carried out by reviewing Internet resources using search engines, keywords and word combinations according to search directions. Monitoring of Internet resources is a daily review of the content of Internet resources for compliance with the norms of international law and the law of the Republic of Kazakhstan. If the organization identifies violations of the law, the dissemination of illegal material is recorded (screenshots, recording of videos, etc.).

Regulation of social networks, messengers and influencers (bloggers)

The main document in this area is the Law of the Republic of Kazakhstan dated 10 July 2023 No. 18-VIII 'On Online Platforms and Online Advertising'. It is focused explicitly on ensuring the transparency of the online platforms, the security of the digital space of the Republic of Kazakhstan and the **prevention of illegal content publication**.

In accordance with the law, an **online platform** is an Internet resource and (or) software operating on the Internet, and (or) instant messaging service designed for receiving, producing and (or) posting, and (or) distributing, and (or) storing content on an online platform by a user of through an account created by him, a public community, except for an Internet resource and (or) software operating on the Internet, and (or) instant messaging service designed for financial services and e-commerce.

An instant messaging service is a software designed and / or used by users of an online platform to exchange or transmit instant messages to specifically identified person(s) in real-time using telecommunications networks, excluding software designed to provide financial services and e-commerce.

The main problem of this law is that the legislators have attempted to establish the legal status of social networks and messengers such as Facebook, WhatsApp, and Telegram, which are actually used by Kazakhstan citizens, but are **located in foreign jurisdictions** that are not subject to Kazakhstan's laws.

In this regard, it is unclear what measures and legal regulation should be applied to these companies by the legislator to regulate their activities within the required framework? It is not clear what the frameworks are too. Authorised state bodies understand that the only real means of regulation is the so-called 'switch' by means of which access to these networks can be temporarily suspended through Kazakhstani providers. However, the 'switch' would only work for those network users who do not know how to use various anonymisers, VPNs, proxies, etc. Since such actions are condemned by the international community, the Kazakhstan authorities often deny blocking in every possible way, explaining the lack of access by purely technical issues. Until recently, there were no known precedents when at the republican level legal claims were made against the owners of social networks or when suspensions of access to them were legally justified. However, on 22 April 2024, on the sidelines of the Majilis, the Minister of Culture and Information Aida Balaeva spoke about the possibility of blocking the TikTok services.

At the same time, during the discussion in Parliament of a bill to combat gambling addiction, MP Irina Smirnova drew attention to the fact that online gambling broadcasts have recently intensified on TikTok. Vice-Minister of Culture and Information Kanat Iskakov clarified that the number of online casinos and online lotteries has indeed increased dramatically in recent years. The Ministry is working in several directions on this issue.

> *'Firstly, we are working with online platforms, in particular with TikTok. And the administration of online platforms assists in this respect. The second direction is where we independently block websites, applications, and URLs. The thing is that they are generated daily, for example, we remove 150 of them during one day, and then they are generated hourly, new ones are created. So the issue here is that we do not have the capacity sometimes to close as many as possible. Sometimes they are created dozens of times more than we remove,'* said Kanat Iskakov.

The deputy minister noted that such content is often generated from abroad and because of that it is **very difficult to find the authors and initiators of such fraudulent schemes**.'

According to the Law of the Republic of Kazakhstan dated 10 July 2023 No. 18-VIII 'On Online Platforms and Online Advertising', in order to work in the territory of the Republic of Kazakhstan, owners and (or) other legal representatives of online platforms, whose average daily access to online platforms during a month is more than one hundred thousand users located in the territory of the Republic of Kazakhstan, shall appoint their legal representative to interact with the authorized body.

However, to date, nothing is known about such representatives and their work with the user complaints, nor about the fulfillment of the legal requirement to translate the interface and user agreement into Kazakh.

How the criterion of one hundred thousand users was calculated and what is the methodology of counting users located on the territory of the Republic of Kazakhstan – was not reported.

The second problem is that it is not clear with whom the Kazakhstan authorities should deal, should they enter into public relations through the regulation of social networks and messengers? Are they going to recognise the **authors of individual pages** as independent media or are they going to try to find those who moderate for the **entire social network**? After all, a common problem of social networks is that on the one hand, they try to present themselves as a purely technological platform, only allowing others to post information, in order not to be responsible for the content. On the other hand, we have recently seen a lot of examples of quite **active moderation policies**, with thousands of posts and accounts being deleted en masse for certain political reasons and views.

In fact, the Law of the RK dated 10 July 2023 No. 18-VIII 'On Online Platforms and Online Advertising' introduces a certain system of voluntary censorship, referred to therein as moderation. According to it, owners and (or) legal representatives of online platforms are obliged to take measures to counteract the spread of illegal content in the territory of the Republic of Kazakhstan. It is separately stipulated that the owner of an online platform must ensure moderation of content in the Kazakh language in order to prevent violation of the law of the Republic of Kazakhstan.

The clause about distribution on the territory of the Republic of Kazakhstan, obviously means that illegal content should not be visible in Kazakhstan, but can be accessed from the territory of other states, through anonymizers, etc.

The Law obliges owners of online platforms to take measures to improve content moderation systems and artificial intelligence algorithms; ensure the safety of minors on the online platform; counter the placement and distribution of illegal content in the territory of the Republic of Kazakhstan; and interact with state authorities of the Republic of Kazakhstan. The owner of the online platform shall annually post a report that includes the following information on content moderation: an indication of illegal content removed by automated moderation systems, the number of received prescriptions of the authorized body, user reports and decisions made on them.

Also, owners and (or) legal representatives of online platforms are obliged to:

- Take measures to counteract the distribution of unlawful content on the territory of the Republic of Kazakhstan;
- React to the request of the authorized body within twenty-four hours after its receipt;
- Ensure the execution of judicial acts that have entered into legal force;
- Ensure the receipt and implementation of instructions and decisions of state bodies by taking measures established by Article 41-1 of the Law of the Republic of Kazakhstan 'On Communications';
- Immediately notify the law enforcement authorities of the Republic of Kazakhstan in case of detection of unlawful content that entails a threat to the life or safety of a person and a citizen;
- Inform the authorized body on measures to counteract illegal content;
- Provide information on users requested by the authorized body on the basis of judicial acts, requests from law enforcement or special state bodies of the Republic of Kazakhstan;
- Suspend the activity of accounts in the territory of the Republic of Kazakhstan that post and distribute illegal content, information recognised as cyberbullying against a child, according to an instruction from the authorized body.

According to the Law, unlawful content includes: an appeal, propaganda or agitation for a violent change in the constitution, violation of the integrity of the Republic of Kazakhstan, undermining the security of the state, war, social, racial, national, religious, class and tribal superiority, the cult of cruelty and violence, suicide, pornography, drugs, psychotropic substances, their analogues and

precursors, the idea of separatism, fraud, information contributing to the violation of inter-ethnic and inter-confessional harmony as well as statements questioning the statehood and territorial integrity of the Republic of Kazakhstan, information revealing state secrets or other secrets protected by law, and other information prohibited by the laws of the Republic of Kazakhstan.

Here again, we would want to highlight the wording of '**other information prohibited by the laws of the Republic of Kazakhstan**'. This wording opens up a wide range of interpretation possibilities, and it is unclear how foreign platforms should know about all the information prohibited by the laws of the Republic of Kazakhstan. Even the Letter of the General Prosecutor's Office of the Republic of Kazakhstan dated 2 June 2014 No. 2-010732-14-29487 states:

> *'We consider it extremely difficult to draw up any document that would make it possible to identify all possible cases of media use for criminal purposes on the basis of pre-established uniform rules and criteria. The media representatives/employees should be responsible for independently identifying such cases on the basis of criminal legislation and law enforcement practice'.*

According to the Law of the Republic of Kazakhstan dated 10 July 2023 No. 18-VIII 'On Online Platforms and Online Advertising', the suspension, termination of posting and distribution of unlawful content is carried out in accordance with Article 41-1 of the Law of the Republic of Kazakhstan 'On Communications'. The owner and (or) legal representative of an online platform shall, within twenty-four hours after receiving the instruction of the authorized body, take measures to remove the information recognised as cyberbullying against a child.

It is also stated that if the owners and (or) legal representatives of online platforms carry out activities of online platforms in the territory of the Republic of Kazakhstan without complying with the requirements established by law, the authorized body has the right to restrict their activities in the territory of the Republic of Kazakhstan in accordance with the laws of the Republic of Kazakhstan. However, the laws of the Republic of Kazakhstan do not contain a definition of what exactly 'restriction of activities in the territory of the Republic of Kazakhstan' means. So far, there have been no precedents in Kazakhstan for restricting, suspending or terminating access to social networks, individual pages or accounts. Although there have been court decisions to do so, apparently they proved to be technically unenforceable.

The Letter of the Ministry of Culture and Information of the Republic of Kazakhstan dated 30 April 2024 No. ZhT-2024-03763178 informs that:

> *'As of today, online platforms 'TikTok' and 'VKontakte' have appointed their legal representatives in the territory of the Republic of Kazakhstan. Thus, today the use of the interface with the function of selecting the Kazakh language is available in online platforms such as: 'OK', "TikTok", "YouTube", "Telegram", "VK". However, this function is not available on the following online platforms: 'Facebook', 'Instagram', 'Mail.ru'.*

However, the authorized body evaded answering the questions: *'is information on the average monthly number of users on the territory of the Republic of Kazakhstan for the last six months of operation of the online platform placed in public access?'.*

The practice of restricting access to online content

This section reviews the legal aspects and blocking techniques in the Republic of Kazakhstan, analyzes data on the number of blocked sites and URL links in recent years, and provides comments and reports from various government agencies.

Restriction statistics

In the Letter of JSC 'State Technical Service' dated 17 April 2024 № ЖТ-2023-03723136 it is informed that according to article 41-1 of the Law of the Republic of Kazakhstan 'On Communications' in cases of dissemination through the telecommunication network of information prohibited or otherwise restricted for dissemination by judicial acts or laws of the Republic of Kazakhstan that have entered into legal force, as well as access to which has been temporarily suspended by the submission of the Prosecutor General of the Republic of Kazakhstan or his deputies, Joint Stock Company GTS (Governmental Technical Service) shall take immediate measures to restrict access to prohibited information upon the order of the authorized mass media body.

To date, the following materials have been blocked by court decisions and orders of the authorized agency:

- in 2022 – 14447 Internet resources and URL links;
- in 2023 – 16472 Internet resources and URL links;
- in the first quarter of 2024 – 7,230 Internet resources and URL links.

The Financial Monitoring Agency of the Republic of Kazakhstan provides the following data on the websites and accounts blocking for the period from 1 January to 31 March 2024:

With signs of a financial pyramid	Online casinos	Cryptocurrencies	Total number of blocked websites and accounts
2 062	1 365	1 083	**4 510**

The Letter of the Minister of Internal Affairs of the Republic of Kazakhstan dated 29 April 2024 No. 1-3-3-6-43/1289//DZ-131 informs that: 'Over the last 3 years alone, more than 51,000 different illegal resources have been identified and blocked on the Internet, including those with signs of fraud and pyramid schemes'.

However, in the response of the Ministry of Internal Affairs of the Republic of Kazakhstan from 27 April 2024, No. ZhT-2024-03722998 to the enquiry about 'what work has been done to limit access to Internet resources with content prohibited by the law of the Republic of Kazakhstan or court decisions and what are the statistics of termination or suspension of access to such Internet resources for the entire time of work', the Ministry preferred to evade the exact figures, saying:

> *'The Ministry of Internal Affairs, within its competence, monitors the Internet to identify illegal Internet resources (pornographic materials, cults of cruelty and violence, suicide, manufacture and sale of weapons, drugs, psychotropic substances, explosives, etc.).*
>
> *Where Internet resources are located on foreign websites, a link to them is sent for blocking to an authorized body (the Ministry of Culture and Information of the Republic of Kazakhstan – hereinafter referred to as the MCI). In terms of obtaining statistical information on blocking illegal content, we recommend contacting the authorized body (MCI)'.*

The Prosecutor General's Office was similarly evasive in answering the same question.

The Letter of the Ministry of Culture and Information of the Republic of Kazakhstan dated 26 April 2024 No. ZhT-2024-03723009 states:

> *'As part of control over compliance with the requirements of the laws of the Republic of Kazakhstan, the Ministry constantly monitors media products, including Internet resources and social networks for violations of the laws of the Republic of Kazakhstan. One of the main tools to counteract the spread of destructive information on the Internet is the monitoring of Internet resources and social networks. The monitoring of mass media in the territory of the Republic of Kazakhstan is regulated by the Law of the Republic of Kazakhstan 'On Mass Media', as well as the Legislation on Monitoring of Mass Media distributed in the territory of the Republic of Kazakhstan, as well as the methodology for its calculation (Order of the Minister of Information and Public Development of the Republic of Kazakhstan No. 84 of 29 April 2019). The Ministry conducts monitoring on a 24/7 basis. Once a violation is identified, a notice requiring the elimination of the violation is sent to media owners, in cases of ignoring the notice, access to materials and Internet resources is terminated by court decision or through the pre-trial blocking procedure established by paragraph 1-1 of Article 41-1 of the Law of the Republic of Kazakhstan 'On Communications'.*

When qualifying a violation of the law of the Republic of Kazakhstan as entailing criminal liability, the authorized body shall send the case to the state body, whose competence includes consideration of cases on this type of violation, with the attachment of materials of the revealed violation.

This approach is generic and applicable to all cases of dissemination of information prohibited by the laws of the Republic of Kazakhstan via the telecommunications network.

The steps for suspending access to Internet resources containing violations of the laws of the Republic of Kazakhstan are described in the Law of the Republic of Kazakhstan 'On Communications'. In accordance with subparagraph 1-1 of Article 41-1 of the Law 'On Communications', if information prohibited by an enforceable court decision or the laws of the Republic of Kazakhstan is disseminated through a telecommunications network, telecommunications operators and (or) the state technical service, upon the recommendation of the Prosecutor General or his deputies, as well as the order of the authorized information authority, are obliged to take immediate measures to restrict access to the prohibited information.

Thus, there are currently 3 legal grounds for restricting access to Internet resources:

1. court decision;
2. requirement of the Prosecutor General or his deputies;
3. a recommendation of the authorized body in the field of information (currently the Ministry of Culture and Information of the Republic of Kazakhstan).

In this case, the Ministry, as a body within the Government of the Republic of Kazakhstan, has the right, in cases described in subparagraph 1-1 of Article 41-1 of the Law 'On Communications', to take immediate measures to restrict access to prohibited information.

For the entire period of work (as of 22 April 2024), the Ministry shared 17,693 reports in respect of **821,405** facts of violations, of which 219 reports shared 1,100 facts of violation in regards to activities prohibited by the courts of the Republic of Kazakhstan.

The Letter of the Prime Minister of the Republic of Kazakhstan dated 16 May 2024 № 16-07/1945 dz 'On measures taken with regard to fake news spreading illegal content' states the following:

> *'The media and social networks are regularly monitored to prevent and detect the dissemination of fake information. In the process of monitoring, 41 cases of dissemination of fake and incorrect information were identified and reported on by the authorised bodies. Six primary sources of fake information were identified. Notices were sent to the owners of online platforms demanding the removal of unlawful materials, as well as to the Ministry of Internal Affairs for consideration of bringing the owners to administrative responsibility. Most of the fake information was related to the distribution of fake newsletters in messengers. Twenty-nine persons were brought to administrative responsibility for posting fake information (6 were arrested, pre-trial investigations were initiated in 2 cases, and the rest were fined). In addition, 92 unlawful publications were sent to the Office of the Procurator-General for legal evaluation, and preventive talks were held with users of social networks who had published such materials. Meetings are also held regularly with the editors-in-chief of the media to coordinate information coverage of the flood situation. The Government has strengthened its efforts to monitor and identify fake information in the media and social networks. The Ministry of Culture and Information, together with the Office of the Procurator-General, is conducting an awareness-raising campaign on the spread of fake information, and is circulating information materials on criminal liability for spreading fakes.'*

The Authorized Information Body continues to monitor the media and social networks in order to prevent and detect the dissemination of '**NEGATIVE INFORMATION**'.

What is interesting in this case is the emphasis on negative information rather than illegal information.

In conclusion, it should be recalled that during the adoption of the Law of the Republic of Kazakhstan of 3 May 2022, No. 118-VII 'On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on the Protection of the Rights of the Child, Education, Information and Informatisation', the provision on the **Unified Register of Internet resources** hosting information prohibited or otherwise restricted for dissemination by the laws of the Republic of Kazakhstan or by judicial acts that have entered into legal force, as well as access to which has been temporarily suspended, was excluded from its draft.

Undoubtedly, if such a register existed in Kazakhstan, it would be possible to draw an exhaustive picture, but for now, we have to work with scattered and contradictory reports from government agencies, which do not give a complete picture of the state of affairs in this area.

Interviews with media representatives

As part of this study, IFKZ conducted interviews with members of media organizations who have experienced website blockings and the hacking of their social media and messenger accounts.

Facing cyber attacks: ProTenge's experience

ProTenge does not have its own website; the team uses Instagram and Telegram to distribute media articles. At the end of 2023, ProTenge faced the problem of account hacking.

Q: **When and how did you find out that access to your account was blocked?**

A: They [unidentified persons, hackers] did it four times, they started in December, finished in January and plus there were more than two cyberattacks on the Telegram channel, that is one of the reasons why we work exclusively on social networks, because it is much easier to block websites. Even the case with Kursiv is a prime example, and with us, after they saw that we were calmly restoring access to accounts, they stopped these cyberattacks. In other words, our strategy of publishing only on social networks so far justifies itself.

Q: **Why was access to your account blocked? Have you received an official explanation?**

A: No, we have not received an explanation from Instagram. However, we contacted human rights organizations in Europe, through which we were able to restore access. I am sure that if we had broken the rules, we would not have been able to restore the account. The restoration process took between 3 and 24 hours, indicating that Instagram did not find any violations of community rules from our side. Of course, such attacks on social media accounts are common, and human rights defenders assist journalists and activists in restoring access. There was a wave of such attacks in December, but now they have become less frequent, which indicates that they haven't been very effective.

We have received no explanation from the state authorities either. Together with other journalists, we submitted statements to the law enforcement authorities not in the hope of an investigation, but as a preventive measure after the cyberattacks and subsequent physical attacks on Vadim Nikolayevich Boreyko, Samal Ybraeva and Gulnara Bashkenova. This was important to document the situation. The cyberattacks ended, and administrative prosecution of me and Askhat Niyazov began. I saw a certain chain of events in this.

To be honest, the cyberattacks on social networks without Instagram's assistance are difficult to investigate. We have collected a lot of information and found that such a scheme is widely used, for example, by the Saudi Arabian authorities to block the accounts of journalists who criticize the government. Russia has also acted against accounts condemning the invasion of Ukraine, having developed a policy in this aspect.

Q: **How did the blocking of your account affect your work? What economic loss did you suffer because of the blocking of your account?**

A: We had several active advertising contracts at the time, and we couldn't work them off. Between $3,000 and $5,000 I think

Q: **Do you expect your resources to be blocked in the future? What do you think the possible restriction will be related to?**

A: What is important here is the technology used to find vulnerabilities in social networks such as Instagram and Facebook. There are two strategies: either a complete blocking of these social networks, similar to the measures adopted in the Russian Federation, or a continuation of the search for and exploitation of new vulnerabilities. It is difficult to predict which scenario will work. It will largely depend on the socio-political situation in the country. After the Sadykov case, it became clear in which direction actions would move and at what speed.

Q: **Have you taken any steps to protect your accounts from future blocking?**

A: We have taken all possible measures. We consulted a number of experts, both local and people outside the country. And everything that could be done at this stage, we have done. But you as a cyber security expert know that, there is nothing unhackable, there is only a question of cost. In general, we have done everything on our part to make it as expensive as possible.

Q: **What changes do you think could prevent similar blockings in the future?**

A: To prevent this from happening, we should hold fair elections in the country and become a democratic country where human rights are respected. Then the law enforcement agencies will not use these methods against journalists.

Q:	**What advice do you have for other website/account owners who may encounter similar problems in the future?**
A:	It is important to contact organizations specializing in cybersecurity for human rights defenders and journalists. It is important to seek their assistance to complete a cybersecurity audit using the resources available. Their recommendations should be strictly followed. That's all I can advise on this issue. Do not store digital data that you do not wish to disclose. Any information that you have in your possession, in any form or medium, can be made public at any time. Even cloud-stored data can be at risk. Always consider your actions from a publication-readiness perspective to avoid unwanted consequences. This is a basic rule of thumb, especially given the many instances where sensitive information has become publicly available despite its intended confidentiality.

Blocking and DDoS attack on a media website: Medianet's experience

In recent years, independent media in Kazakhstan have faced various forms of pressure, including website blockings. Medianet, an international center for journalism, was no exception. During the interview, Medet Yesimkhanov, editor-in-chief at Factcheck.kz (an online media by MediaNet), spoke about his experiences, actions and future plans in relation to such incidents. The interview was focused on the reasons for blocking, response measures and possible changes in policy and legislation that could prevent such incidents in the future.

Q:	**When and how did you find out that access to your site was blocked? Were you notified in advance?**
A:	Our website is thankfully not blocked right now. However, we experienced difficulties in accessing the site recently – on 19th June. At that time, a check by our IT specialists showed high activity of bots. Similar events occur every few months. One of the most memorable cases of the last year and a half is the DDoS attack that occurred on the night of 14-15th March 2023. Then we managed to restore access, but throughout the night and the following days we were still in the 'code red' mode, if I may put it this way. And, of course, we cannot but remember the Internet outage in January 2022, when almost all media outlets, including us, did not have access to their own resources. There were no warnings at the time, we learnt about the blockage when we were unable to access the site, and then it was announced at the official level.

Q: **What have you done when your website was blocked? For example, did you create an alternative domain or encourage your audience to use a VPN?**

A: Given that there was a full internet outage in January 2022, we did not make any appeals. There were colleagues in the newsroom who were out of the country at the time, and they took over the management of the website and social media. Otherwise, the website has not ever 'been down' for an extended period of time – we have been able to resolve the problem in a fairly short time. We usually let our readers know what's going on and ask for patience while we try to fix the situation. If in the future we encounter prolonged website blocking (e.g., half a day or more), we may consider longer-term solutions.

Q: **Do you expect your resources to be blocked in the future? What do you think the possible restriction will be related to?**

A: We do not rule out such a scenario, as independent media in Kazakhstan have been subjected to pressure many times. And only last year we have seen cyberattacks on some popular resources. The restriction, in the case of the media, is almost always related to their direct activity -- that is, the publication of materials.

Q: **Have you taken any steps to protect your site from future blocking?**

A: Our specialists work hard to ensure that the website is protected from various attacks. We also take into account the scenario of blocking access to the website for a long or indefinite period of time and keep in mind several possible solutions. But we don't want to talk about them in advance, especially since we haven't had any such incidents so far.

Q: **What changes (in policy, legislation) do you think could prevent such blockings in the future?**

A: Firstly, internet shutdowns should be prohibited by law, as they violate fundamental human rights. In addition, it would be good if government agencies assisted in investigating cyber attacks. Finally, journalists should be protected, not persecuted. Unfortunately, we have seen freedom of speech and press freedom only shrink in recent years.

Q: **What advice do you have for other site owners who may encounter similar problems in the future?**

A: Have a good team of experts who can find solutions, as well as provide options to continue to maintain the services even during a prolonged blocking.

Restriction of VPNs, proxies and anonymizers

In Kazakhstan, circumvention tools that provide access to materials blocked by court decisions and orders of state bodies are prohibited by law.

Paragraphs 1-3 of Article 41-1 of the Law 'On Communications' state the following:

> *'Operation of communication networks and (or) means of communication, provision of communication services, access to Internet resources and (or) information placed on them for the purpose of access to information prohibited by an enforceable court decision or laws of the Republic of Kazakhstan shall be prohibited'.*

This norm was amended in 2017, but the practice of restrictions in Kazakhstan had been in place before. A Kazakh court decision of 10 September 2014 banned circumvention tool websites: *'Prohibit the operation of networks and (or) means of communication used for the purpose of circumventing the technical capabilities of telecommunications operators used to stop the distribution of foreign media products in Kazakhstan'.*

Restriction statistics

According to the Internet Freedom project, which analyzes the list of blocked URLs, this is the statistics of restrictions on the basis of 'Violation of the norms of the Law of RK "On Communications" (anonymisers, proxy-servers of TOR type, VPN-servers, etc.)' by year:

Year	URLs
2018	**62**
2019	**27**
2020	**152**
2021	**10**
2022	**16**
2023	**1**
Total	**268**

Due to the blocking of social networks and media during the elections and the implementation of Qaznet Trust Network's national security certificate, Kazakhstan became one of the top countries in terms of VPNs usage growth in 2019. According to the 'Global Mobile VPN Report 2019' in 2019, Kazakhstan ranked third in terms of the growing number of downloads with 4.1 million downloads (+210%) compared to the last 12 months (October 2017 – September 2018):

> *'May-June 2019, Kazakhstan: 111% climb resulting from multiple short-lived social media blocks and a brief total internet shutdown, surrounding national election unrest. A further 93% spike in June is likely due to continued protests and a root certificate distributed by the government, found to be used for mass-surveillance.'*

According to the Top10VPN, the demand for VPN services in Kazakhstan on 5 January 2022, when the protests took place, increased by 3405% compared to the average daily rate of the previous 30 days.

Thus, given the direct legislative ban on such technologies, in practice they are popular among users in Kazakhstan.

Case study: Attempt to unblock a VPN domain

On 14 July 2020, the Ministry of Information restricted access to almost 150 URLs related to VPN services, including hidemy.name, owned by 'hidemy.network Ltd.' company. Hidemy.name was not notified of this restriction.

To justify the blocking, the Ministry presented a document called 'monitoring analysis' with cropped screenshots that do not allow third parties to understand the date and time when the monitoring has started. The screenshot presented by the Ministry shows the website of Kavkaz-Centre, which has been banned since 2011, but due to the fact that this website publishes the date and time on the home page, it allows to determine the date of monitoring as 20 January 2023. This document cannot be accepted for consideration – evidence from 2020 is required.

The Ministry did not provide proof of notification to the resource administrator, noting that the manager responsible for the notification is no longer employed by the government agency and all accounts have been blocked.

On 7 March 2023, the representative of the VPN, the law firm Digital Rights Center Qazaqstan, filed a lawsuit to the Specialized Interdistrict Administrative Court of Astana demanding to unblock the URL links pertaining to the company's services.

On 24 March 2023, Judge Aubakirov N.E. made a ruling to return the lawsuit, stating that 'hidemy.network Ltd.' should have challenged the prescription within 1 year. However, the company could not do so, as it had no information about the prescription, having received it only in December 2023.

Specialized inter-district administrative court of Astana and the Judicial Board on administrative cases of the court of Astana in their rulings on refusal to consider the filed lawsuit refer to the fact that the term for filing a lawsuit has expired. Thus, they refer to paragraph 5 of Article 136 of the Administrative Procedural Code:

> *'A person who did not participate in the administrative procedure, whose rights, freedoms and legitimate interests are affected by an administrative act, has the right to file a lawsuit in court within one month from the date when the person learnt or could have learnt about the adoption of the administrative act,* ***but not later than one year from the date of its adoption.****'*

The trick of this article is that a state body (in this case, the Ministry of Culture) makes a decision to block access and does not notify the website's administrators about it, as it happened with hidemy.name. The VPN service did not know that it was blocked in Kazakhstan as early as 14 July 2020, but only found out about it only in autumn 2022.

Arguments that the VPN client administrators were not informed have not been accepted by the courts, citing this clause of this Article of the Administrative Procedural Code.

Not agreeing with the determinations of the lower judges, a petition was filed with the Supreme Court to review the judicial acts, with Judge Baimakhanov S.U. presiding over the judicial panel, with Judges Alzhanov G.U. and Umraliev E.D. on the panel.

On 9th November 2023, a court hearing was held in the Supreme Court of the Republic of Kazakhstan, which took no more than 10 minutes, in the case of unblocking the VPN client site hidemy.name. Below is the question that the panel of the Supreme Court asked in order to make its final decision on the case:

Supreme Court, *'Does the website administrator see that there are no requests from the KZ segment to his site?'.*

Response from a VPN client representative: *'To find out that a service is unavailable in a particular country, you need metrics [to measure availability], and there are separate services that determine availability based on requests from servers in different jurisdictions'.*

Response of the representative of the Ministry of Culture: *'We work with the Autonomous Organisation "Governmental Technical Service" (GTS), which directly fulfills the technical tasks of blocking. When we consulted with them, [they said that] the owner sees all the flows. If the website was blocked on the territory of Kazakhstan, the flow is reduced'.*

Supreme Court: *'So the Claimant knew that something had gone wrong in Kazakhstan and users had stopped using its service from the moment it was blocked by GTS, traffic had dropped and they should have known immediately. The question is removed.'*

The issue may seem simple at first glance, but in practice it is much more complex. All jurisdictions around the world require the use of specialized monitoring tools to check the availability of a website from different geographical locations. Such tools are usually paid and provide data on a number of accessibility parameters, including response time, code status, bugs, download speed and other indicators.

In addition, there are issues of accessibility of the website through different networks of telecom operators. For example, there may be cases when the website is available through the networks of Kazakhtelecom JSC, but is not available through Beeline. In such situations, it is necessary to conduct repeated measurements to confirm the reliability of the data.

Performing accessibility audits requires not only the appropriate tools, but also qualified people, both internal and external, who are able to use the tools and analyze the collected data. Depending on the complexity and scope of the task, different skills and qualifications may be required, such as knowledge of network protocols, web technologies, programming, assistive technologies, accessibility standards and other competences.

Thus, we believe that administrators of websites and services are not obliged to ensure that their resources are available in all jurisdictions of the world, as this requires significant financial costs. In addition, Kazakhstan has an authorized state body, the Ministry of Culture and Information, which is responsible for interacting with and informing foreign websites, but in practice this function is not always realized.

In addition, the Supreme Court justifies its decision by saying that it is possible to open some pornographic and terrorist websites using a VPN.

> *'The defendant's representative, on the contrary, believes that the courts justifiably returned the claim, and therefore asked to leave the contested court rulings in force and the cassation appeal without satisfaction. He also explained that during the consideration of the plaintiff's complaint it was repeatedly established that using 'VPN hidemy.name' it was possible to get access to the Internet resource kavkazcenter.com, which is banned on the basis of the decision of the Saryarka district court of Astana № 2-2014/2011 of 20 April 2011, for propaganda of terrorism. In addition, with the use of 'VPN hidemy.name', the Internet resource* `https://rt.pornhub.com` *with pornographic materials, restricted by the order of the authorized body, was opened. It was in this connection that access to the Internet resource* `https://hidemy.name` *was restricted in the territory of the Republic of Kazakhstan on the basis of an order issued by the authorized body'.*

Does it make sense to block circumvention tools?

It is practically impossible to completely restrict access to all circumvention tools, unless one moves to radical measures of widespread blocking. VPN services, proxy servers and anonymizers can be distributed via websites, cloud storage, app stores such as AppStore, Google Play Market, Windows Marketplace, browser extension and plug-in shops, social networks and messengers. Moreover, if necessary, you can change the configuration directly on the device by specifying the appropriate IP address and password.

An analysis of the usage and restrictions of VPNs, proxies and anonymizers in Kazakhstan shows that legislative measures aimed at blocking these technologies often contradict social and technological realities. Despite the official ban, such services remain in demand among users, especially in the context of political instability and increased Internet censorship.

Conclusion

Our network measurement findings corroborate previous reports on the blocking of news media websites, petition sites, and circumvention tool sites in Kazakhstan. Specifically, as part of our analysis, we found **17 news media websites** (including Vice News, a few Kyrgyz news media sites, and many Russian news media sites), the Russian language edition of Amnesty International's website, several **petition sites** (`www.change.org`, `www.ipetitions.com`, and `egov.press`), and **73 circumvention tool websites** (including NordVPN, ExpressVPN, ProtonVPN, OpenVPN, TunnelBear, and Surfshark VPN) blocked in Kazakhstan between June 2023 to June 2024.

Petition websites were reportedly blocked in Kazakhstan several years ago in a government attempt to prevent campaigning. The ongoing blocking of petition sites in Kazakhstan raises concerns. Meanwhile, the blocking of the Russian language edition of Amnesty International's website appears to be targeted in nature, given the fact that Amnesty International's English language website was accessible in Kazakhstan – as were many other international human rights websites (such as Human Rights Watch).

News media censorship (as identified through the blocking of news media websites in this study) in Kazakhstan might be aimed towards securing information sovereignty. The Decree of the President of the Republic of Kazakhstan No. 145 dated March 20, 2023 approved the Information Doctrine of the Republic of Kazakhstan, which contains controversial concepts (such as "true information security", "ideological sovereignty", "main ideological vector", "destructive, manipulative and false content", "false narratives") which may influence the regulation of online content and censorship decisions.

Circumventing internet censorship in Kazakhstan can potentially be challenging, as OONI data shows the extensive blocking of numerous circumvention tool websites. It's worth noting though that some circumvention tools (Tor and Psiphon VPN) were found reachable in Kazakhstan during the analysis period, suggesting that internet users in Kazakhstan might be able to circumvent internet censorship through the use of Tor or Psiphon VPN.

The results of our analysis show that most ISPs in Kazakhstan appear to implement blocks by means of **TLS interference**, specifically by timing out the session after the Client Hello message during the TLS handshake. This suggests the potential use of Deep Packet Inspection (DPI) technology to detect (and block access to) hostnames (likely included in some blocklist) that are specified in the (unencrypted) Client Hello message of TLS handshakes. As the timing of the blocks and the types of URLs blocked are (mostly) consistent across networks, ISPs in Kazakhstan likely implement blocks in a coordinated manner (based on government orders).

Notably, through OONI data collected from Kazakhstan between 2021 to 2024, we found **7 distinct intermediate certificates signed by 4 distinct root CAs being used to carry out TLS man-in-the-middle (MITM) attacks, targeting at least 14 distinct domain names on at least 19 different networks in Kazakhstan**. We found that these intermediate certificates were even being used to perform MITM attacks during periods of certificate invalidity. This raises concerns because such practices weaken the online privacy and security of internet users in Kazakhstan.

We found TLS MITM attacks on at least 19 networks by only analyzing OONI data collected from Kazakhstan between June 2023 to June 2024. As OONI data from Kazakhstan spans from 2017 to date, with new measurements published every day, we encourage researchers to analyze OONI data to investigate the scale of TLS MITM attacks in Kazakhstan further.

Acknowledgements

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

We also thank David Fifield for sharing input that informed the update of the TLS MITM section of this report.

Kazakhstan: TLS MITM attacks and blocking of news media, human rights, and circumvention tool sites

Publication date: September 19, 2024
Last updated: October 15, 2024

OONI

IFKZ INTERNET FREEDOM KAZAKHSTAN

EURASIAN DIGITAL FOUNDATION