Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom

Reethika Ramesh, Ram Sundara Raman, and Apurva Virkud, *University of Michigan;*
Alexandra Dirksen, *TU Braunschweig;* Armin Huremagic, *University of Michigan;*
David Fifield, *unaffiliated;* Dirk Rodenburg and Rod Hynes, *Psiphon;*
Doug Madory, *Kentik;* Roya Ensafi, *University of Michigan*

https://www.usenix.org/conference/usenixsecurity23/presentation/ramesh-network-responses

This paper is included in the Proceedings of the
32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Proceedings of the
32nd USENIX Security Symposium
is sponsored by USENIX.

Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom

Reethika Ramesh[†*] Ram Sundara Raman[†*] Apurva Virkud[†] Alexandra Dirksen[△]
Armin Huremagic[†] David Fifield Dirk Rodenburg[‡] Rod Hynes[‡] Doug Madory[◊] Roya Ensafi[†]

[†]*University of Michigan* [△]*TU Braunschweig* [‡]*Psiphon* [◊]*Kentik*

Abstract

Russia's invasion of Ukraine in February 2022 was followed by sanctions and restrictions: by Russia against its citizens, by Russia against the world, and by foreign actors against Russia. Reports suggested a torrent of increased censorship, geoblocking, and network events affecting Internet freedom.

This paper is an investigation into the network changes that occurred in the weeks following this escalation of hostilities. It is the result of a rapid mobilization of researchers and activists, examining the problem from multiple perspectives. We develop GeoInspector, and conduct measurements to identify different types of geoblocking, and synthesize data from nine independent data sources to understand and describe various network changes. Immediately after the invasion, more than 45% of Russian government domains tested blocked access from countries other than Russia and Kazakhstan; conversely, 444 foreign websites, including news and educational domains, geoblocked Russian users. We find significant increases in Russian censorship, especially of news and social media. We find evidence of the use of BGP withdrawals to implement restrictions, and we quantify the use of a new domestic certificate authority. Finally, we analyze data from circumvention tools, and investigate their usage and blocking. We hope that our findings showing the rapidly shifting landscape of Internet splintering serves as a cautionary tale, and encourages research and efforts to protect Internet freedom.

1 Introduction

Shutdowns, censorship, and restrictions on the flow of information are alarming reminders of the fragility of the Internet. They call for investigation into how we can strengthen the Internet and defend its freedom. A series of such events took place in February 2022, when Russia invaded parts of Ukraine in a major escalation of the longstanding Russo-Ukrainian War. [58]. What followed in the succeeding weeks was a hodgepodge of government reactions, sanctions, business withdrawals, and general confusion concerning the state of information controls. In Russia, the government's desire to control messaging about the invasion led it to increase censorship of alternative sources of information and limit the use of circumvention tools [51]. Isolation increased in both directions, with network resources in Russia being made unavailable from outside the country [35], and entities outside Russia cutting Russian users off from network access and business deals through sanctions and geoblocking, a phenomenon in which server operators intentionally deny access to users from particular regions [28, 54, 82].

There are significant challenges in studying and recording such an event: (1) Understanding multiple types of access restrictions like geoblocking, website censorship, changes in Internet infrastructure, and their compounding effects is a herculean task, requiring the collection and synthesis of diverse datasets; (2) Studying different forms of geoblocking requires the design and development of new measurement techniques and geographically distributed vantage points; and (3) Distinguishing between Internet restrictions such as censorship and geoblocking which have similar effects is difficult, and current censorship observatories are not equipped to make this distinction easily. Nevertheless, we are called to meet these challenges, in order to enable researchers and activists to engage advocacy groups in driving positive change, for example highlighting the harms of geoblocking and encouraging web services to avoid its use [1].

In this paper, we overcome each of these challenges by developing new measurement methods and synthesizing data from nine independent data sources—Open Observatory of Network Interference (OONI), Censored Planet, Route Views, Internet Outage Detection and Analysis (IODA), Censys, the Wayback Machine, Tor, Psiphon and IVPN—to characterize from multiple perspectives how decisions and reactions by powers in Russia and elsewhere affect the network and cause isolation [8, 9, 36, 39, 46, 64, 69, 79, 91].

We design, implement, and open-source our measurement tool, GeoInspector, for identifying geoblocking that is imple-

[*]Reethika Ramesh and Ram Sundara Raman contributed equally to this research.

mented on the DNS, TCP, and HTTP(S) protocols [7]. We overcome the difficult, error-prone challenge of differentiating between restrictions caused by geoblocking and local censorship in Russia, by developing a traceroute-like technique to determine the location of the blocking as well as developing specific HTTP signatures that confirm the presence of geoblocking. Considering Russia's history of decentralized censorship [71], we collect measurements from four diverse vantage points located in data center and residential networks in Russia (RU) and 15 geographically distributed vantage points in other countries. Additionally, we develop and run browser-based measurements to study the use of certificates issued by Russia's domestic Certificate Authority (CA) [77].

We find evidence of **geoblocking by Russian government domains forbidding access to foreign users**. 136 Russian government domains (25.09%) block access to all tested countries outside Russia, and a further 112 government domains (20.66%) cannot be accessed from tests outside Russia and Kazakhstan. We leverage public longitudinal data sources to show that most of this geoblocking is relatively new and begins after the start of the 2022 invasion. We document cases of foreign actors, especially **foreign news media outlets, educational organizations, and governments geoblocking Russian users** from their websites. We find 68 domains implement DNS-based, 90 implement TCP-based, and 286 employ HTTP-based geoblocking. Through our measurements, we also analyze the real-world deployment of certificates issued by Russia's new domestic CA that emerged as a response to western certificate authorities ceasing issuance of certificates to Russian Top Level Domains (TLDs) [17, 28, 34].

Through analysis of OONI and Censored Planet data, we show that overall blocking in major Autonomous Systems (ASes) increase in the weeks after the 2022 invasion, and highlight that specific **news media and social media communications domains such as BBC and Twitter are blocked completely** [100]. Combining insights from data published by IODA and Route Views, we observe some Russian networks attempting to implement geoblocking, protection from DDoS and censorship **using BGP routing changes and withdrawals**, including an attempt to hijack a Twitter prefix. Finally, we characterize the **action and reaction of censors and circumvention tools** both before and after the invasion, using data from Tor, Psiphon and VPNs.

Our investigation into network responses to Russia's invasion of Ukraine in 2022 highlights how the landscape of Internet censorship is rapidly shifting, as an array of private actors join a growing number of government actors in implementing online information controls. Our study is an example of a "rapid response" that mobilizes researchers from academia, Internet freedom groups, and industry partners to collaborate and highlight harmful trends to defend against actions that contribute to Internet splintering. However, due to the continuous and numerous occurrence of such events it is not feasible and sustainable to perform such coordinated and deep investigations at scale, without advances in current monitoring capabilities. The state of the art research into collecting censorship measurements is almost all aimed at detection of nation-state censorship of websites, which ignores the role that private actors play in censoring online content. We emphasize that censorship measurement platforms need to be equipped with techniques to differentiate the source of blocking and extend their monitoring beyond nation-states. We hope this work serves as a cautionary tale for Internet freedom researchers and activists, and encourages more research on Internet splintering and its growing threat.

2 Background on the Splinternet and Russia

The word "splinternet", as we use it, refers to an isolated network bubble brought about by various entities implementing blocking policies that ultimately cut off users from the global Internet or result in a heavily restricted and monitored connection to it [16, 95]. This splintering of the Internet has been a global concern in the past years and has been discussed in academic works [2, 55, 60]. In the past decade, we have witnessed new and increasingly bolder attempts at hindering user's access to the global Internet or providing unequal access to people from different regions. This has included actions implemented both by government censors, and service providers. The most notable examples are the large-scale HTTPS interception in Kazakhstan [83], censorship in Myanmar [65], throttling of Twitter in Russia [98], and content providers enabling geoblocking [60].

We hypothesize that the restrictions and censorship events following the 2022 invasion of Ukraine has exacerbated the growth of an isolated Internet bubble in Russia. Over the past decade, Russia has used several emerging censorship techniques such as using commoditized deep packet inspection technology to facilitate censorship [71], and using throttling to restrict the use of Twitter [98]. The implementation of regionalized information control techniques resulting in a splinternet would lead to vastly different Internet experiences for people from different regions. This could help foster a bubble of state-sponsored messaging around sensitive events.

In the rest of this paper, we highlight how the effect of splintering in networks in Russia was achieved both due to increased censorship by Russia and due to foreign Internet services applying sanctions to block Russian networks and deny service to Russian TLDs.

2.1 From a User's Perspective

Let us first consider the journey of a user in Russia on the modern Internet, shown in Figure 1, *keeping in mind various network locations where restrictions such as those illustrated in the paper could be applied*. The user begin the process on a desktop that is equipped with some browser software. Firstly, when the user tries to navigate to a website, a DNS

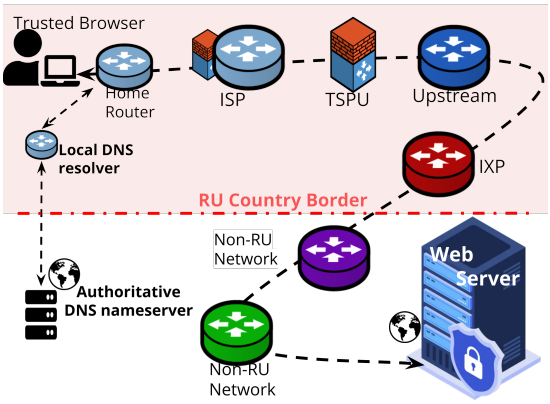


Figure 1: **Typical request to a website made from Russia.** The globe indicates where geoblocking can be implemented.

Measurement	**§**	**Public dataset used**		**Data Period**
Censorship in Russia	§4.1	Data from OONI [64] and Censored Planet [84]		May'21–May'22
Network Level	§4.3	BGP Data from [79]		Feb '21–May '22
Circumvention Tools	§6	Tor, Psiphon, VPNs		Dec '21–May '22
Tools Developed	**§**	**VPs**	**Test List**	**Data Period**
Geoblocking of RU Gov't Sites	§4.2	4 RU, 15 global	RU gov't domains [80]	Mar '22–April '22 and May 10 '22 (primary results)
Foreign Geoblocking	§5.1	4 RU, 15 global	Tranco Top 10k [68]	Mar '22–April '22 and May 10 '22 (primary results)
Russia Domestic CA	§5.2	Yandex, Chrome	3,722 signed domains [30]	April 8 '22

Table 1: **Measurement details:** Tools developed, vantage points and test lists, and the sources of public data.

query is made. When the IP for the domain in question is obtained, the browser makes a TCP connection, which can then be followed by a TLS handshake and HTTP requests and responses to exchange data. During the TLS handshake, the web server sends its certificate alongside the Server Hello. The browser on the user's machine validates that the certificate has been signed by a legitimate certificate authority, and allows further communication. If the user uses a compromised or state-approved browser, or has configured their browser to trust a particular CA, the user's connection could be intercepted by a machine-in-the-middle attack.

Secondly even if the browser and root certificate store are not compromised, the user's ISP could apply rules and block the user's connection based on internal policies, and censorship policies of their government. Next, filtering and censorship policies could be applied on the path by commoditized deep-packet inspectors. In Russia's case, there is evidence of TSPU devices ("Technical Measures to Combat Threats") installed on the path, typically close to the user, that carry out centrally coordinated censorship across multiple ISPs [96]. This sort of filtering can also happen further upstream by other providers or at Internet exchange points, but in Russia most of the censorship has been observed close to the user [71].

Next, the routing between networks is handled using Border Gateway Protocol (BGP) announcements. Network operators can use BGP to enforce censorship, by controlling and shaping how and whether ASes can access certain services. Using strategic BGP route withdrawals, connections to a large portion of networks can be censored or dropped instead of routing correctly, this practice is often also known as "blackholing". Finally, censorship and geoblocking policies can be applied by the server-side and by the DNS authoritative nameservers who could have a policy to not respond to requests coming from the IP address space of a certain country or network.

To overcome these restrictions, users may turn to using circumvention tools. These tools include anonymity-focused browsers like Tor [91], circumvention tools such as Psiphon [69], and VPNs that help users connect to services through an encrypted tunnel via a server typically located in uncensored networks [46]. These tools could even employ obfuscation techniques, peer-to-peer routing, and multi-hop routing to evade detection by the censors. However, governments try to prevent access to these tools by blocking the distribution of such tools and banning their use by law.

3 Overview

We provide an overview of how we organize and present our measurements and results. Table 1 indicates the structure of our paper, and the datasets we use in each study. Since we conduct our own measurements as well, we indicate the vantage points and test lists used in each.

In §4 we present the network actions that Russia has taken during their invasion of Ukraine. We expound on the increasing censorship events in Russia during this time and we analyze the geoblocking that Russian government domains employ. We also analyze different datasets to understand changes made at the BGP level in Russian networks. We emphasize that these actions lead to the rapid escalation of splintering.

In §5 we describe the actions taken by foreign entities that caused more isolation of Russian users, further escalating the splintering. We investigate popular foreign domains that geoblock Russian users and characterize their implementation. We emphasize that web services callously implementing such geoblocking ultimately harm users and Internet freedom as a whole. Further, we analyze how actions of western certificate authorities (CAs) led to the emergence of a domestic CA.

In §6 we highlight increased demand for circumvention tools, and how the tools reacted to intensified censorship. We show an increase in Psiphon users that correlates with censorship events, explain how various ways of accessing Tor were blocked, and study how VPN use increased many-fold during the invasion. Despite their availability, circumvention tools account for only a small fraction of users, indicating that many people still cannot connect to censored resources.

3.1 Ethics

Data-driven investigations into censorship, especially ones, like ours, that respond to a sudden crisis, are crucial to monitoring overreach by authorities. Journalists, advocacy groups, and users need precise understanding of what exactly is being blocked in the network, which investigations like ours provide. Progress in anti-censorship research requires empirical, measurement-driven understanding of censorship practices. Our results advance transparency and accountability regarding Internet restrictions while minimizing risk in data collection and publication. The benefits of publishing this work far outweigh the minimal risks. We contacted our Institutional Research Board (IRB) and received "Not Regulated" determination. Considering the nature of our study, we went beyond just consulting the IRB and took the below considerations.

Community efforts, panel discussions, and prior work from the FOCI and Internet measurement communities [24, 47, 63, 64, 84, 101] have established best practices and ethical standards for safety in research, drawing from the principle of beneficence from the Menlo report [19]. Our study is in line with these norms. In the investigation of geoblocking, we used one residential machine in RU, and 18 datacenter VPs in commercial hosting facilities. Our approach mirrors previous work conducting similar measurements in Russia, China, and Myanmar [63, 65, 71, 96]. The residential VP is operated by a colleague with a decade of experience working on censorship and measurement in Russia, who knowingly and voluntarily consented to the measurements. We acknowledge the potential risks of doing censorship research in Russia, but note that there has never been punitive action taken by the Russian government against a project like ours. In renting VPSes, we used the name and university email address of one of the authors, and strove not to subject VPS operators to more risk than they face in the ordinary course of business. From the VPSes we tested only popular websites, with no emphasis on ones likely to be censored. Our measurement results do not reveal sensitive or identifying information from the VPSes.

We collaborate with and obtain data from OONI, Censored Planet, IODA, Route Views, Psiphon, Tor, and IVPN, who have extensive experience working with the Internet freedom community, and their own ethics and privacy rules to govern research projects and data publication. These datasets do not include any sensitive information [39, 46, 69, 79, 91].

4 Russia's Actions Escalating the Splintering

The government of Russia has a long history of implementing network censorship. Since the invasion, however, its censorship practices have escalated even further. Russia has started using increasingly powerful methods to protect its Internet "sovereignty" in the face of attacks and sanctions against it. Here we present a trend of increasing restrictions, including censorship, geoblocking, and withdrawal of BGP routes.

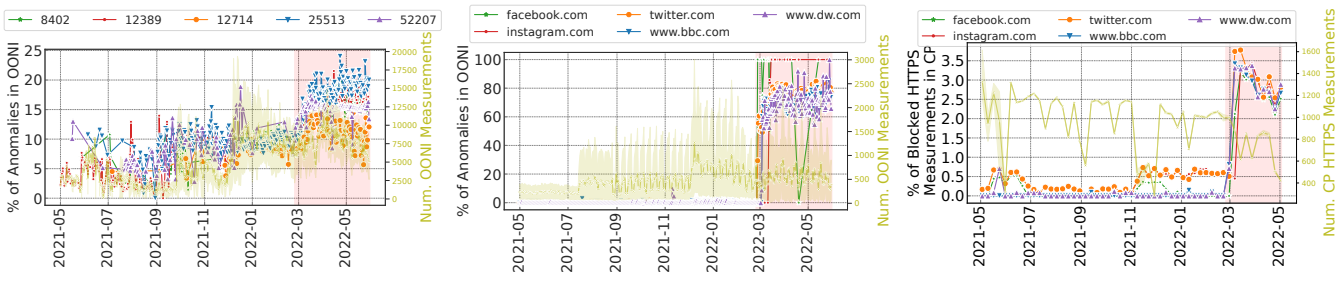
4.1 Censorship in Russia

We characterize changes in censorship of websites around the time of the 2022 invasion by analyzing public data from preexisting censorship measurement platforms. A benefit of using established platforms is that they collected measurements both before and after the invasion. Our analysis uses data from two such platforms, OONI [64] and Censored Planet [84]. **These two platforms are complementary; together they give us a more complete picture of Internet censorship in Russia before and after the invasion.** Together, OONI and Censored Planet collected measurements in 1,074 ASes in Russia between May 2021 and May 2022 (783 ASes in Russia just between January 2022 and May 2022 period).

OONI uses direct network measurement. Volunteers run OONI's open-source data collection software, *OONI Probe*, in about 160 countries every month. OONI Probe runs a variety of tests designed to detect network interference and censorship, and publishes the resulting data on the OONI website [64]. OONI has written its own reports about blocking in Russia, one at the start [100] and one a year later with Roskomsvoboda [78]. We analyze measurements from OONI's Web Connectivity test collected in Russia between May 2021 and May 2022. For each of a list of input URLs, the Web Connectivity test does a DNS lookup, makes a TCP connection, and sends an HTTP or HTTPS GET request from the local network and from a control network. If the results from the two networks differ, the URL is marked "anomalous", signaling potential blocking. The sites tested usually come from the Citizen Lab URL test list [14], though OONI Probe users may test any website of interest. For our longitudinal analysis, we consider 1,803 URLs (58.1% of all URLs tested) that were tested every day between May 2021 and May 2022.

In contrast to OONI's direct measurements, *Censored Planet* uses remote measurement. It tests thousands of "organizational" endpoints (such as ISP servers) in multiple countries remotely from a measurement machine in the United States [84], without requiring physical presence in those countries. We use data from Censored Planet HTTPS measurements where HTTPS requests are sent from the measurement vantage point to web servers in Russia. Responses to multiple requests for a test domain are compared to responses to a control request for a known, uncensored domain. Censored Planet infers blocking if test responses are different from control responses, and the if responses for the test domain show a clear indication of network interference such as network timeout, connection reset or blockpage. Because of the outside-in nature of remote measurements, Censored Planet cannot detect blocking that only affects traffic that originates inside the country, which unfortunately the TSPUs have been reported to use [96, 98].

Findings from OONI data We find a significant increase in anomalies in the days and weeks following the invasion. Figure 2a shows the increase in the percentage of anomalies



(a) **Anomaly per AS in OONI** (b) **Anomaly per domain in OONI** (c) **Anomaly per domain in CP HTTPS**

Figure 2: **Increase in censorship in RU from OONI and Censored Planet data:** Figure 2a shows the increase in blocking in the top 5 ASes with most measurements during the 2022 Russian invasion on days with more than 100 measurements on OONI. Figure 2b shows increasing blocking of social media and news from OONI data. Figure 2c shows increased blocking of the same domains in Censored Planet HTTPS data. The olive bands represent the number of measurements per day.

in the five ASes with the most measurements, including popular ones such as Rostelecom (AS12389) and Vimpelcom (AS8402). The fraction of anomalies in these ASes increased from about 7%–11% in January and early February 2022 to about 12%–21% in mid-March. The number of measurements per day remained fairly stable. We observe similar increases in other ASes as well, although the censorship methods themselves are sometimes different because of the decentralized nature of blocking [71, 100].

Certain website categories were targeted more than others. In particular, popular social media and news media domains were almost completely unavailable after the invasion, as highlighted both in Figure 2b and in OONI's own report [100]. These domains were available before the invasion, but have been blocked since then, as late as the end of May 2022.

Findings from Censored Planet Censored Planet also observed increased blocking. Figure 2c shows several popular social media and news domains. Unlike OONI, Censored Planet does not show these domains as completely blocked, which is possibly a result of methodology limitations: Censored Planet can only detect censorship that affects traffic in both directions, which is the case in only a subset of ASes [98].

Our findings show Russia's increasing attempts to control the information seen by its citizens, by blocking popular news and social media domains in many ASes. However, censorship by Russia is not the only cause of anomalous measurements. OONI's report labels some anomalies as possible geoblocking, done not by a middlebox but by the server [100]. Current censorship monitoring platforms are not well-equipped to measure geoblocking; in OONI's case, they relied on manual investigation and follow-up measurements to identify it. **We fill this gap by developing our own geoblocking measurement techniques.**

4.2 Measuring Geoblocking of Russian Government Domains

In the weeks following the invasion of Ukraine, Russia's Ministry of Digital Development and Communications declared that there had been an unprecedented volume of DDoS attacks against Russia, by Ukrainian IT specialists and their allies [35]. These attacks were believed to be targeted specifically at military and government domains. But in light of the fact that since April 2019, Russia has been creating a legal basis for a "sovereign Runet", with provisions for separating its domestic network from the global Internet in the event of foreign threats such as cyberattacks [59], press reports at the time suggested that Russian government domains had not been brought offline by outside attackers, but been restricted from outside access by Russia itself [88]. **We build novel geoblocking measurement strategies, and conduct reachability measurements from globally distributed vantage points (VPs) to understand if Russian domains are geoblocking users outside the country from accessing them.**

GeoInspector We developed GeoInspector to measure geoblocking on the most common Internet protocols which form the primary stages of an Internet connection–DNS, TCP/IP, and HTTP(S). To the best of our knowledge, we are the first to build methods to systematically identify DNS and TCP/IP-level geoblocking by using geographically distributed measurements, as previous studies have focused exclusively on identifying HTTP(S) geoblocking using server blockpages [60] or on specific case studies [86]. We open-source GeoInspector for continued monitoring of geoblocking in Russia and elsewhere [7].

GeoInspector takes a set of domains as input, and begins by checking for failures during DNS resolution. Case studies conducted previously have shown that US government domains implement geoblocking at the authoritative nameservers; i.e., authoritative nameservers return errors for queries that originate from recursive resolvers in certain countries [86]. Draw-

ing on this insight, GeoInspector conducts iterative DNS lookups from each of our geo-distributed set of vantage points. For each domain, GeoInspector queries the `f-root` server for the nameserver of the TLD, then iteratively queries the resulting nameservers, label by label, until reaching the A record for the complete domain. This process enables us to identify which nameserver(s) in the chain fail to respond to our query. GeoInspector retries failed queries up to three times, as in previous work [84], to reduce the effect of temporary network failures. Note that while DNS queries to a local recursive DNS server could be poisoned due to local censorship [66, 84], our measurement design directly queries remote nameservers, and is not affected by censorship at the local DNS server.

Geoblocking could also be implemented in the TCP/IP, TLS, and HTTP protocols [60, 86]. Web servers, on receiving a request from IP addresses in certain countries, may choose to block or drop the connection at the TCP handshake, TLS handshake or HTTP request stage. We detect these types of geoblocking by attempting TCP handshakes, TLS handshakes, and HTTP(S) GET requests for every domain in our input list. To eliminate the possibility of DNS interference, we use pre-resolved IP addresses from the DNS measurement already described; or, if local DNS resolution failed, we use IP addresses from a control VP located in the US. GeoInspector follows and records all HTTP redirects, and when it observes a temporary network error, it retries the request up to three times to account for transient failures.

Vantage Points and Test Domain List We use four measurement vantage points (VPs) in RU (1 residential and 3 datacenter), as well as 15 globally distributed datacenter VPs in the following countries: Azerbaijan (AZ), Brazil (BR), Canada (CA), Germany (DE), Egypt (EG), France (FR), the United Kingdom (GB), Ireland (IE), India (IN), Japan (JP), South Korea (KR), Kazakhstan (KZ), Singapore (SG), Thailand (TH), and the United States (US). See Figure 3. Measurements from the four RU VPs serve as controls, since we expect the domains to be accessible from RU. We obtain a comprehensive test list of Russian government domains from previous work [80]. Of the 1,003 Russian government domains in the list, 623 were active at the time of our experiment; these we used as our input list. Of the 623 domains, 515 (82.66%) are `*.gov.ru` domains.

Measurement Time Period As shown in Table 1, we used our tool GeoInspector to collect DNS, TCP, and HTTP(S) data daily between March 14 and April 22, 2022. Only 1 Russia VP and 8 global VPs were stable enough to collect measurements throughout the whole period. Therefore, we did an additional round of data collection on May 10, 2022, when all 19 VPs were active. Considering the stability of the data, we primarily report results from May 10, 2022, and wherever appropriate, extend it with results from the earlier longitudinal measurements (for example, see Figure 4). Overall, we did not observe any meaningful changes over time.

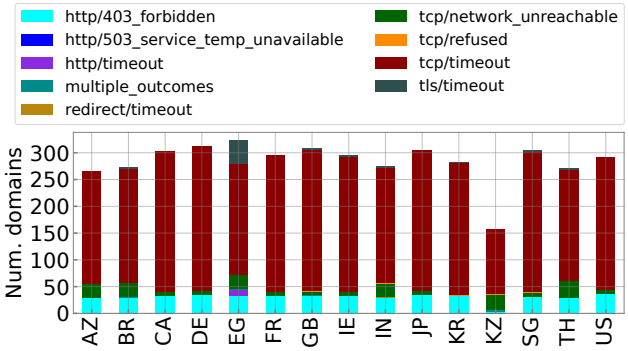


Figure 3: **Geoblocking by RU government domains:** TCP, TLS, and HTTP geoblocking observed on May 10, 2022.

4.2.1 DNS-based Geoblocking Findings

Only 18 domains (2.89%) failed in iterative queries in at least one non-RU country from our DNS geoblocking measurements of May 10, 2022. For five domains (namely `*.edu.gov.ru` and `nic.gov.ru`), we observe a timeout in eight countries (BR, CA, EG, JP, KR, SG, TH, US). Queries for these domains failed at the same two nameservers, `ns.informika.ru` and `ns2.informika.ru`, indicating that they have a policy of not responding to requests from these eight foreign countries. Moreover, our daily longitudinal measurements from March–April 2022 show that these five domains had failed to resolve over time. All 623 domains were resolved successfully in at least one Russian VP.

4.2.2 TCP-based Geoblocking Findings

We were not able to successfully fetch content from 81 domains (13%) from any control RU VPs, so we exclude these from further analysis, and consider the remaining 542 domains. To identify signs of geoblocking during the TCP handshake, we look for explicit network errors. Figure 3 breaks down the types of responses from our measurement on May 10, 2022.

TCP Timeouts A timeout during the TCP handshake is the most common failure we observe for RU government domains ("tcp/timeout" in Figure 3). This result is consistent across most countries tested. For instance, 99 unique domains (18.26%) observe a timeout across all 15 countries. 87 of these domains are subdomains of `fas.gov.ru` (Federal Antimonopoly Service) and six are subdomains of `tambov.gov.ru` (Tambov region). The remainder are domains belonging to the Ministry of Energy and Resources. Except one domain (`www.yakutskenergo.ru`) that started geoblocking in late March 2022, all the other domains display the same timeout error throughout our daily longitudinal measurements in March–April 2022 (refer to §4.2.5 and Figure 4).

Interestingly, 88 other domains (16.24%) observe a timeout across all tested countries *except Kazakhstan* (KZ). This

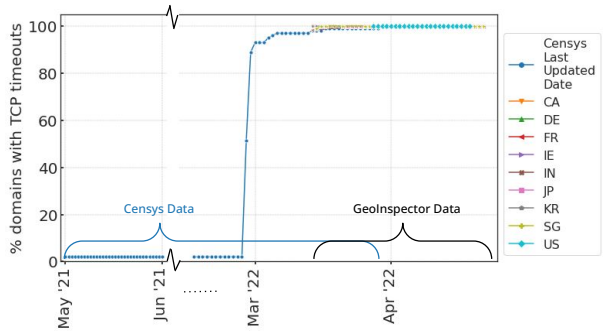


Figure 4: **TCP Geoblocking by RU government domains:** We present data from the Censys Search API (May'21-Apr'22) and our longitudinal GeoInspector measurements (Mar-Apr'22) for domains where we observe a TCP timeout in all countries other than RU. Most domains become unavailable in the four weeks following the 2022 invasion and continued to be blocked through our test period.

shows that some RU government domains treat requests from KZ—a neighboring country—differently than requests from elsewhere. 39 of the 88 domains are subdomains of `rk.gov.ru` (Crimea region) and 9 are subdomains of `fsa.gov.ru` (Federal Accreditation Service).

Network Unreachable We observe 42 domains (7.75%) return a network unreachable error during the TCP handshake, primarily in six countries (AZ, BR, EG, IN, KZ, and TH). 35 of these are subdomains of `ryazangov.ru`, hosted on the IP prefix 185.183.175.66/31. We also find the domains `*.non-tariff.gov.ru`, `www.minpromtorg.gov.ru`, `regulation.gov.ru`, and `kids.minpromtorg.gov.ru`, hosted on the same IP prefix 212.164.137.64/28, return a network unreachable error in a different set of eight countries (CA, DE, FR, GB, IE, JP, SG, US).

4.2.3 HTTP-based Geoblocking Findings

To identify signs of geoblocking during HTTP requests, we looked for HTTP status codes other than "200 OK", since we confirmed manually that "200 OK" had no geoblocking.

403 Forbidden We saw 40 unique domains (7.38%) return the "403 Forbidden" status code during our scan in May 2022. The HTTP 403 Forbidden response status code has been reported by previous work as the most common status code returned by CDNs for geoblocking [60]. Of these 40, 26 are subdomains of `49gov.ru` (Magadan region), which return an empty page with status code 403 in all countries *other than KZ and RU*, similar to the pattern observed with TCP timeouts. The domain `fpi.gov.ru` (Russian Foundation for Advanced Research Projects) returns a page stating "DDos Guard - Service is not available in your region" in all tested countries except RU, suggesting it could be geoblocked due to DDoS concerns. We observed the 403 Forbidden responses consistently for all countries except RU and KZ across our longitudinal measurements in March–April 2022. Three subdomains of `yakutskenergo.ru` provide a 403 Forbidden page for 10 tested countries (CA, DE, EG, FR, GB, IE, JP, KR, SG, US). Combining findings from both TCP and HTTP measurements, we find that 136 RU government domains (25.09%) block access to users outside RU, and a further 112 domains (20.66%) can only be accessed from our RU and KZ VPs.

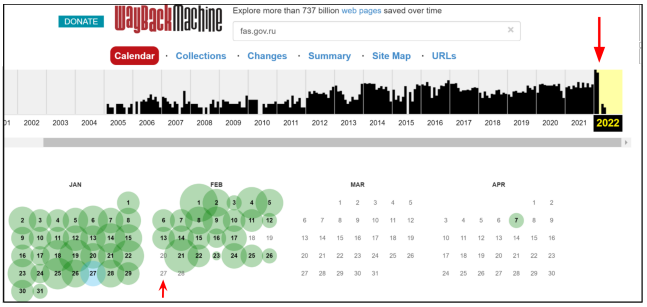


Figure 5: **Confirming TCP timeout–based geoblocking of `fas.gov.ru` using the Wayback Machine [38].**

4.2.4 Other Findings

We also observe some domains returning different errors in different countries. For example, the educational domains (e.g. `edu.gov.ru`) that perform DNS geoblocking also return TCP timeouts in six other countries when control DNS responses are provided. In another example, `chechnya.gov.ru` results in a TCP timeout in certain countries (IN, SG, TH) and 403 Forbidden message in others (DE, GB, KR, US).

4.2.5 Was the geoblocking because of the invasion?

While we did not collect data using GeoInspector before March 2022, we investigated data from multiple public data sources to understand whether geoblocking by RU government domains was active before the 2022 invasion, or if it was instated only after. One source was Censys [20], an Internet-wide scanning project that collects daily snapshots of responsive IPv4 hosts from multiple locations (including the US, but not from RU). Since Censys tries to scan every single IPv4 address, longitudinal data from Censys can show when a specific IP address becomes unresponsive to their scanners over TCP. All of the 99 domains that were geoblocked from every other country other than RU went offline in Censys in the four weeks following the initial start of the 2022 invasion (February 27–March 20), as shown in Figure 4.

For HTTP- and HTTPS-based geoblocking, we extract a timeline of geoblocking from the Internet Archive Wayback Machine [36], which contains archived versions of some tested domains. We manually inspect the 163 domains that had frequent archived snapshots before the invasion. 122 (74.85%) of them stopped being archived after the start of

invasion (an example is `fas.gov.ru` [38], shown in Figure 5). A further 9 domains (5.52%) had the geoblocking page (403 Forbidden) archived after the start of the invasion (an example is `fpi.gov.ru` [37]).

In summary, public, historical data permits us to infer that many of the Russian government domains we tested started to geoblock users outside the country *only after the escalation of hostilities at the end of February, 2022*. Geoblocking techniques vary across government domains: only a few domains apply DNS geoblocking; others implement geoblocking using TCP timeouts or HTTP 403 Forbidden responses, in some cases even with explicit blockpages. **The striking lack of coordination in the implementation of geoblocking suggests that Russia was unprepared for attacks against their government domains and hence, resorted to various ad hoc methods as a defense.**

4.3 Withdrawal of BGP Routes

In response to DDoS attacks and censorship policies, ISPs in Russia implemented major changes to their BGP announcements. We studied data from public sources such as Route Views and IODA [39, 79], and analyzed various BGP events that took place in Russia and the motives behind them.

Protecting against DDoS On February 26, 2022, a Ukraine official called for a volunteer "IT army" of worldwide hackers to target 31 prominent websites of the Russian government and Russian businesses [23]. On the same day, Rostelecom, which serves as the sole transit provider for the e-government website `gosuslugi.ru`, stopped announcing the website's seven prefixes, likely to limit the effects of any DDoS attacks [41]. From Route Views and IODA data, we find that multiple Russian companies began withdrawing their BGP routes during non-working hours in March 2022. Three ASes periodically withdrew routes belonging to prominent organizations in Russia's air and space industry (AS48122, AS210954) [43, 45] and the main electricity provider in the city of Saint Petersburg (AS198074) [42].

Censorship Following the invasion, the withdrawal of BGP routes has been used to censor media outlets. The Ukrainian network of Radio Free Europe/Radio Liberty has been unavailable since February 25, and their Moscow network has also been withdrawn since March 11 [44, 57].

BGP Twitter Hijack In March 2022, Russia ordered Twitter and Facebook to be blocked in the country [76]. Noteworthy among the attempts by ISPs to block these services is the *Twitter BGP hijack* incident. From BGP data collected by the Route Views project, we observe that on March 28, 2022, from 12:05 to 12:50 UTC, the Russian ISP RTComm (AS8342) hijacked the prefix 104.244.42.0/24 belonging to social media service Twitter, and announced the prefix to the global Internet [40]. However, Twitter had learned from previous hijack attempts in Myanmar in 2021 [65], and had created route origin authorizations for their BGP routes in RPKI. Therefore, ASes practicing RPKI validation rejected the hijacked route. **Studies highlighting network changes during times of heightened censorship are crucial for recording attacks against websites and ensuring that the community learns from them.**

5 Foreign Actors Escalating the Splintering

In response to Russia's invasion, foreign governments and companies began instating a series of financial and policy measures designed to damage Russia's economy and curb those benefiting from the war [3, 89]. On top of this, over 1,000 companies publicly announced their plans to withdraw operations in Russia, according to one report [82]. Among them were companies like Spotify and Netflix, which suspended Russian users from using their services [33, 54]. Subsequently, many, including civil society groups in a letter to the US President, warned that cutting off Russian users from western services would only further isolate Russians seeking information about the war [1]. Despite this outcry, there has been no systematic study to measure and record what popular domains are inaccessible to users in Russia.

Among those sanctioning Russia were western Internet service companies, such as certificate authorities (CAs) that committed to stop issuing certificates to TLDs based in Russia. This action by western certificate authorities sparked Russia to develop and deploy localized solutions. We argue that such restrictions cause further isolation and create information bubbles, powered by localized technology that puts at risk the security and privacy of thousands or millions of users. In this section, we expand on the effects of geoblocking and of western CAs taking action against Russian users.

5.1 Geoblocking by Foreign Websites

We investigate geoblocking by popular services against Russian users using our GeoInspector tool introduced in §4.2, to conduct DNS, TCP, and HTTP(S) reachability measurements.

Our Custom Traceroute Technique Because Russian ISPs and TSPUs *also* prevent Russian users from accessing various foreign resources, distinguishing foreign geoblocking from domestic censorship is a key challenge. To that end, we have developed a TTL-limited measurement technique that localizes the point of failure in the network path [6, 87]. To the best of our knowledge, we are the first to distinguish geoblocking from censorship systematically using network location.

For each domain that returns an error in our RU VPs, we conduct traceroute-like measurements at the transport layer (TCP) or the application layer (TLS/HTTP). An overview is shown in Figure 6. We first send SYN packets to the server's IP address with incrementing TTL values (from 1 to 64) and attempt a TCP handshake. When the IP address is blocked

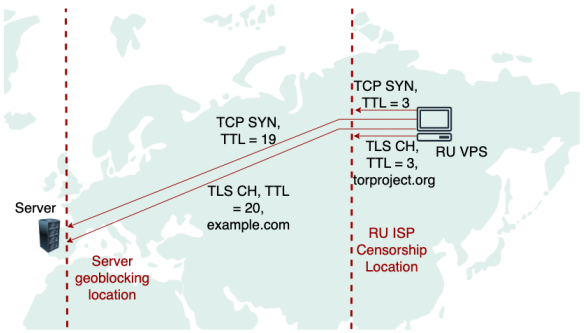


Figure 6: **TTL-limited Traceroute probes to distinguish between censorship and geoblocking.**

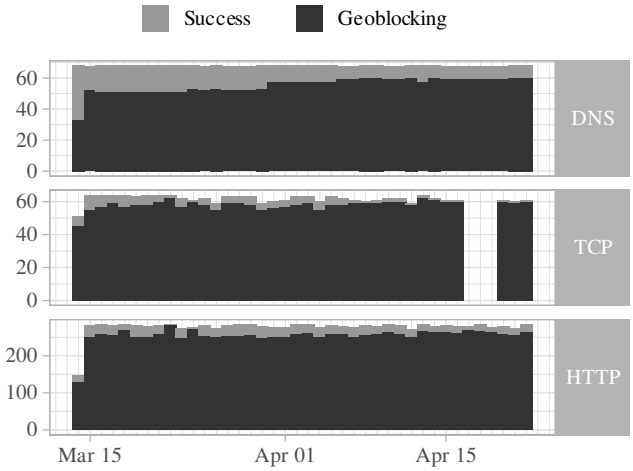


Figure 7: **Longitudinal DNS, TCP, and HTTP geoblocking results in RU for domains performing geoblocking on May 10, 2022.** We observe some domains staring to geoblock RU after the start of our measurement period.

by Russian ISPs, we expect either packet drops or injected RSTs before the packet leaves RU; in the case of server-side geoblocking, the failure will instead occur in the remote server's network. If neither is the case, our probes will successfully establish a TCP connection with the server.

After the TCP handshake, we run two application-layer traceroutes to the server IP address. We send HTTP GET request and TLS Client Hello packets with incrementing TTL values (from 1 to 64), first with the Host header or SNI set to `example.com`, and then again with the Host header or SNI set to the test domain. The control traceroute gives us an estimate of the path to the server, and the test traceroute tells us whether any error occurs within Russia or closer to the server. We evaluate our traceroute with domains known to be blocked in Russia (e.g. `torproject.org`) and measurements to our own vantage points.

Vantage Points and Test Domains List To quantify the number of domains geoblocking users from Russia, we conduct DNS lookups, TCP and TLS handshakes, and HTTP requests, using the same list of VPSes as in §4.2, but this time taking measurements *outside* RU to be the controls. In order to test popular websites, we use the Tranco top 10K domains [68] as input. 1,237 domains (12.37%) did not return a "200 OK" status code in any country; we exclude these from further analysis, and report on the remaining 8,763 domains.

Measurement Time Period As in §4.2, we performed daily longitudinal DNS, TCP, and HTTP(S) measurements using our GeoInspector tool from March 14 to April 22, 2022 in 9 stable VPs. We conducted a larger measurement using all 19 VPs on May 10, 2022. The results primarily come from the May measurement; we add insights from the daily measurements in March and April when appropriate (see Figure 7). We used our traceroute technique to identify the location of all failures in the May experiment.

Data Sanitization: Removing Cases of Censorship All four RU VPs showed signs of TLS-based censorship for 87 domains (0.99%), e.g. `svoboda.org` and `torproject.org`. Tests of these domains resulted in a TCP RST or a timeout in response to a TLS Client Hello. TLS-based traceroutes showed that these errors occur at a hop inside Russia, close to the user, which is a sign of censorship. We therefore remove these domains from our geoblocking results. According to our traceroutes, all of the failures in RU VPs that happened during the TLS handshake were due to censorship. Two RU VPs also saw DNS injection of a blockpage IP address for 38 domains (0.43%); these we remove as well. We did not observe any cases of IP-based censorship.

5.1.1 DNS-based Geoblocking Findings

Of the 8,763 domains we tested for DNS geoblocking, 8,513 (97.15%) returned A records (IPv4 addresses) for all VPs on May 10, 2022. **There are 68 domains (0.78%), mostly belonging to foreign governments (26) and educational organizations (14), that failed to resolve in all four RU VPs.** For instance, certain government domains in the US, India, and Saudi Arabia geoblock Russian users. We confirmed that DNS lookups fail during the query to the authoritative nameserver, or to a nameserver belonging to the organization. There was a small increase (8 domains) in DNS geoblocking by these domains in our daily longitudinal measurements as shown in Figure 7, indicating that at least some of these domains started geoblocking in the months *after the invasion*.

5.1.2 TCP-based Geoblocking Findings

We find 90 domains (1.03%) that implemented geoblocking at the TCP handshake phase for all four RU VPs in our May 2022 scan, as shown in Figure 8. While 44 (0.5%) domains geoblocked access from RU exclusively, another 29 (0.33%) geoblocked access from RU and KZ—a pattern we observed earlier in §4.2. TCP traceroutes related to these

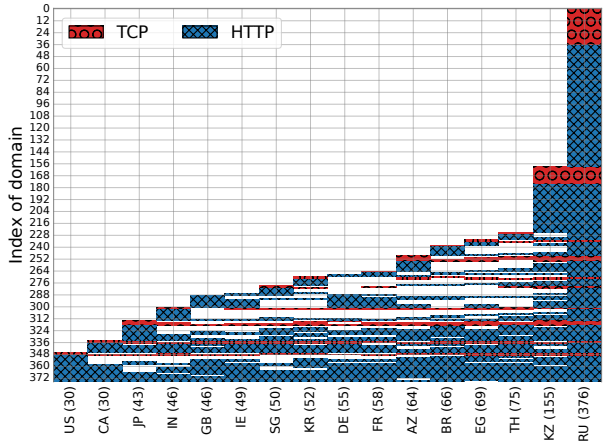


Figure 8: **TCP and HTTP geoblocking across countries on May 10, 2022.** Number of geoblocked domains per country are in parentheses in the *x*-axis. 159 domains are geoblocked only in RU, and 67 are geoblocked only in KZ and RU.

domains confirmed that the failures happened in the same country or AS as the server itself. This would manifest to the user as a TCP timeout. **As with DNS geoblocking, foreign government and education domains are the most common.** The geoblocking by 14 education domains, including 11 North American universities (e.g. `tamu.edu`, `utk.edu`) and a textbook provider (`cengage.com`), is especially concerning, as it affects remote students in Russia. We find 29 domains (0.33%) that are geoblocked through both DNS and TCP, including several US `*.gov` domains. This renders the strategy of circumventing DNS geoblocking by using public resolvers outside the country ineffective. We see 16 domains that started their geoblocking of Russia between March and April, as shown in Figure 7.

5.1.3 HTTP-based Geoblocking Findings

Identifying Geoblocking Signatures An HTTP response from a remote server may contain the expected content page, an error page (e.g. bot detection pages triggered by our use of automated requests), or a geoblocking page. Differentiating between these cases is a key challenge. We adopt an iterative clustering process to determine which responses correspond to geoblocking, taking insights from previous work [60, 85]. We extract text from HTML pages for the 8,556 domains with valid HTTP responses, and use agglomerative clustering to group pages for each domain with at least 90% similar text content or page length [48, 60]. In the first iteration, we manually examine pages for 107 domains where the responses from the RU VPs and the responses from the remaining countries formed distinct clusters, to identify a preliminary set of eight page content *signatures* that we use to label all matching pages. We iteratively repeat this process on any unlabeled

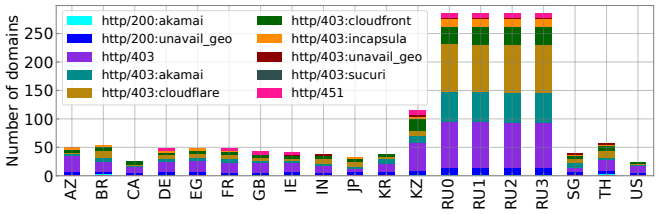


Figure 9: **Geoblocking signatures across countries.** We identify 19 geoblocking signatures and aggregate them based on CDN and status code.

pages until all pages have been manually examined, assigned a signature, or resolved to a single cluster for all countries (which indicates no geoblocking). **In total, we identified 43 signatures (matching pages for 1,185 domains), 19 of which represent geoblocking.**

We find 286 domains (3.26%) with geoblocking signatures for all four RU VPs, with RU being geoblocked by significantly more domains than any other country. See Figure 9. 90 of these domains (1.03%) geoblocked Russia exclusively; i.e., they were available in all countries but Russia. While some of the categories of geoblocking domains, like "Shopping" (46) and "Finance" (20), are consistent with previous work [53, 60], **we also observe 42 "News and Media" domains geoblocked in Russia. The majority are US-based news sites, including national (e.g. `pbs.org`) and local outlets (e.g. `suntimes.com`, `roanoke.com`).**

Interestingly, we find explicit geoblocking signals not only in "403 Forbidden" responses (266), but also in "200 OK" responses (14). For example, `netflix.com` and `spotify.com`, two companies that publicly withdrew their services from Russia, both returned "200 OK" responses, containing a geoblocking message in the page content. Among the "403 Forbidden" responses, we primarily found CDN-enabled blocking, with most domains geoblocked through Cloudflare (87) and Akamai (57) as shown in Figure 9. **As in §4.2, 43 domains (0.49%) exclusively geoblocked KZ and RU.** Similar to DNS and TCP geoblocking, we see a slight increase (13 domains) in HTTP-based geoblocking over time. See Figure 7.

We emphasize the need for tracking the spread of geoblocking and its longitudinal changes. As we have argued, existing censorship measurement platforms are ill-equipped to study this phenomenon. Studying geoblocking is important, as we can identify trends and can engage advocacy groups to pressure server-side entities that contribute to the splintering of the Internet in those regions. In Russia's case, civil society groups wrote a letter to the U.S. President arguing that geoblocking by western companies would only further isolate Russian users and activists already restricted by domestic network policy [1]. But without longitudinal, geographically distributed measurements tracking geoblocking, instances of such restrictions elsewhere in the world could go unnoticed.

5.2 Emergence of a Domestic Certificate Authority in Russia

Following sanctions imposed by western nations, certificate authorities (CAs) such as GoDaddy committed to stop issuing certificates to TLDs based in Russia; .ru, .by, .su and .рф [17, 28, 34]. Some CAs like DigiCert went further, revoking existing certificates of, e.g., Russian banks [11–13]. Shortly after these announcements, the Russian public service Gosuslugi stated that the Ministry of Digital Development would provide a free domestic certificate authority *(CN=Russian Trusted Root CA)* to replace foreign certificates that had expired or been revoked [61]. The appearance of this CA raised discussions among the Web-PKI community concerning the inclusion of the certificate in the trusted root store of western browsers [62, 77].

Russia's new domestic CA is untrusted in most browsers due to concerns that the new CA does not comply with technical requirements [4]. Gosuslugi advised users to use a browser that already trusts the CA, such as Yandex Browser or Atom, or to install the certificate manually [31, 62] Their website lists domains that have reportedly been issued certificates by the new CA. They include important services like online banking [30]; and so, even users outside the country could be forced to trust the new CA or use a Russian browser.

Jonker et al. investigated whether and how sanctions affect the DNS and TLS certificate issuance in Russia and their consequences [49]. But revocation is not the whole story—it is also important to know what certificates are actively used and whether browsers accept them. We ran our own measurements to see what certificates issued by the new CA are in use, and to check whether they replace revoked certificates. We also investigate which websites that use these certificates are accessible from outside Russia, using Yandex Browser and certain western browsers.

Measurement Setup As of May 2022, the new domestic CA had signed 4,658 domains, according to their website [30]. After removing wildcards, we obtained the certificate from the remaining 3,722 domains using Chrome and Yandex Browser from a VP in Germany. We used Certificate Search [10] to get the previously deployed certificates of each domain. Aside, two domains on this list, `22.ctlog.digital.gov.ru` and `test.ct-log.ru`, seem to suggest that Russia plans to operate its own Certificate Transparency logs in the future.

5.2.1 Findings

When accessed in Chrome, 234 out of 3,722 domains (6%) caused a `CERT_AUTHORITY_INVALID` error, which is the expected result when a site's certificate is signed by an untrusted CA. We then accessed the domains using Yandex Browser and found that **114 of them have deployed a certificate signed by the Russian domestic CA.** Investigating these 114 new certificates further, we find that they were **issued between March and April 2022**, shortly after sanctions were imposed, and have a validity period of at least one year. **We also find that 46 domains (40.3%) had a recently expired, un-renewed certificate** originally issued by a trusted CA. Another 36 of these 114 domains (31.5%) had a certificate from a trusted CA that was not yet expired, in addition to one issued by Russian CA. For instance, in Chrome, the domain `getfinance.ru` returned the older, trusted certificate; but in Yandex Browser it returned the newer, Russian-issued one. Finally, 30 of 114 domains (26.3%) had no record of past certificates, and we find only one instance of recent revocation (for the domain `demo-cb.open.ru`).

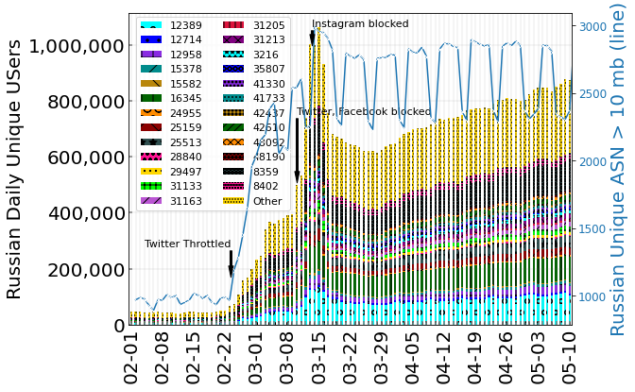


Figure 10: **Psiphon usage before and during the invasion.**

6 Circumvention Tools During the Invasion

Reports suggest that Internet users in Russia users increasingly turn to circumvention tools [22], even as the government cracks down on them [75]. We analyze usage data from the circumvention tools Psiphon [69] and Tor [91], describing the blocking actions against them and their reactions. We also obtain information about the rise in popularity of VPNs [46].

6.1 Psiphon and its Protocols

Psiphon is a free and open-source circumvention tool. The Psiphon client automatically tries a number of protocols to find one that works, prioritizing ones that have higher performance or lower cost. Analyzing Psiphon usage data is informative in two ways: the total number of users reflects the demand for circumvention, while the distribution of circumvention protocols settled on by clients hints at the severity of blocking; i.e., what protocols are blocked and not blocked.

As shown in Figure 10, overall Psiphon usage began to increase at the start of the invasion, on February 24. Usage escalated rapidly starting on February 26, when the Russian government began throttling access to Twitter [73], and surged further on March 4 when Twitter, Facebook, and other media sites including the BBC were fully blocked [100]. Psiphon's

Protocol	Blocking characteristics
Directory authorities	All 10 blocked by IP address, starting December 1.
Public relays	Largely blocked, by IP address, with the blocklist being updated to include new relays.
Default obfs4 bridges	All 16 blocked by IP address.
Non-default obfs4 bridges	Progressively discovered and the bridges blocked by IP address.
meek bridge	Blocked, but only on an even smaller subset of ISPs (in Moscow and Saint Petersburg), until December 13.
Snowflake bridge	Blocked by protocol signature until a new software release on December 14.
torproject.org	Blocked by ISPs (not TSPU) beginning December 7. Unblocked on July 14, then blocked again on July 28.

Table 2: **Summary of blocking events related to Tor.**

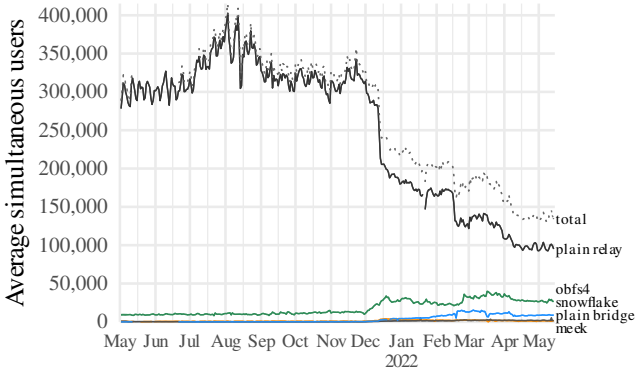


Figure 11: **Tor users in Russia, by protocol.**

usage numbers peaked at over 1.1 million daily unique users on March 10, which is when the Russian government announced it would block access to Instagram [27].

Close inspection of the protocols select by clients reveals fine-grained information about changes in protocol blocking. The protocols Psiphon supports can be broadly categorized as *direct* or *indirect*. Direct protocols have high performance and low cost, but are more vulnerable to aggressive filtering. Indirect protocols, while relatively less efficient and more costly, are more resistant to blocking. We have seen in the past that Psiphon's protocol selection is tightly to censorship activity—sudden shifts in protocol distribution accompany (and in some cases anticipate) filtering, throttling and shutdowns. We examined minute-by-minute changes in Psiphon's protocol distribution on March 16. There was a large shift from direct to indirect protocols across all major Russian ISPs, changing within an hour from a mix of 99% direct and 1% indirect, to 10–20% direct and 80–90% indirect. The temporal component reveals more insights: at 15:16 UTC, we see blocking in Rostelecom and larger fixed-line ISPs; then about 10 minutes the same blocking in mobile carriers such as MTS, Beeline, and MegaFon. **This phenomenon points to a centralized roll out of new network censorship tactics, potentially using the TSPU system [96, 98].**

6.2 Tor and its Pluggable Transports

On December 1, 2021, the Tor network was blocked, without warning, in many ISPs in Russia [99]. This was around the time the US released intelligence on anticipated conflict [32]. Blocking Tor comprehensively is an involved task. The Tor network consists of thousands of servers at well-known addresses (relays and directory authorities) that communicate using a TLS-based protocol [18], as well as thousands of secret "bridges" and circumvention protocols (pluggable transports) that disguise the use of Tor. The blocking action in December 2021 was extraordinary in its comprehensiveness, affecting, for at least a short time and a subset of ISPs, all the common ways of accessing Tor. Table 2 is a summary.

The directory authorities are servers at static IP addresses that maintain a consensus of the state of the network. All directory authorities were blocked on December 1. The majority of public relays were blocked at the same time, and the blocks were updated over time to include new relays.

Not only public relays, but also secret bridges and pluggable transports were targeted. The obfs4 pluggable transport re-encrypts Tor traffic so that it no longer resembles Tor TLS. All the "default" obfs4 bridges, whose addresses are not secret, were blocked on December 1. Non-default obfs4 bridges were also targeted; though because of their secret addresses they were better able to resist blocking, and usage of obfs4 actually increased following the onset of general Tor blocking.

The meek pluggable transport tunnels traffic through a CDN edge server over HTTPS. The censors in Russia briefly blocked the IP address of the CDN edge server used by meek—a drastic step because it also affected non-Tor traffic. The block of meek affected fewer networks than the other Tor-related blocks, a few ISPs in Moscow and Saint Petersburg only. The IP address block was removed on December 13.

The Snowflake pluggable transport [81], which uses temporary peer-to-peer WebRTC proxies, was blocked on December 1. The censors used a distinctive feature in Snowflake's implementation of WebRTC to detect and block connections. Tor developers released a new version of Snowflake on December 14 to fix the WebRTC fingerprinting flaw [90], and Snowflake began working again. The number of users of Snowflake in Russia thereafter increased; in May 2022 users from Russia constituted about 70% of Snowflake users.

The Tor Project's website was blocked on December 7. Unlike the network blocks, the website block was acknowledged by Roskomnadzor. It was implemented by the familiar method [71] of ISPs enforcing a shared blocklist, and affected a greater number of ISPs than the Tor network blocks.

Figure 11 shows estimated user counts before and after the invasion. The number of relay users dropped by about two

thirds. (The fact that it did not go to zero reflects that not every ISP was affected.) The number of bridge and pluggable transport users increased, but not by an equal amount.

6.3 VPN Providers

At the time of the invasion, non-profits like the Open Technology Fund raised funds to subsidize access to censorship circumvention services for activists, users, journalists, and anyone in need of circumvention in Russia and Ukraine [67]. These included services such as nthLink, Psiphon, and Lantern. Apart from these tools, other VPN providers also joined in the efforts to help users in Russia and Ukraine to stay connected to the rest of the Internet. We obtained data from one such provider, IVPN [46]. Their data shows a drastic increase of visitors from Russia and Ukraine after the invasion. Between February and March 2022, there was a 380% increase in visitors from Russia and a 157% increase from Ukraine; whereas worldwide visitors to IVPN increased only 28%. The increase correlates with the general increase in awareness of and need for VPNs, with periodic jumps in visitors and users when IVPN's free access campaign was shared widely. In the seven months since February 2022, IVPN has distributed over 6,000 one-month gift codes.

7 Related Work

Geopolitical events in the physical world affect the digital world as well. In the case of the Russian invasion of Ukraine, digital media has become part of the war itself [15]. After the invasion, censorship levels increased, as did targeted blocking of news and social media. We use data from OONI, which itself has reported on network changes in Russia [78, 100], and augment it with data from Censored Planet, a remote censorship measurement observatory [84]. Combining the data from these complementary sources provides a unique view of the heightened Internet censorship during the Russian invasion.

Russia has been implementing new and bold censorship techniques over the past decade. Ramesh et al. studied Russia's decentralized information control policy [71]. Xue et al. investigated the throttling of Twitter by Russia in 2021 [98], and the massive deployment of a technical extension (TSPU) used in Runet's infrastructure to censor users' traffic [96]. Kaye investigates how technology companies deal with Russian censorship [51]. Fontugne et al. noted that Russia, during the annexation of Crimea in 2014, demonstrated their long-term plans for the network [25]. Valentovitch and Ermoshina compared blocking in Crimea and Russia during the 2018 presidential election [93]. Other studies explore Russia's flourishing market for censorship and surveillance technology and its spread [21, 94], and Russia's use of censorship to create and foster a social media bubble [29]. Studies have also shown users turn to circumvention tools to bypass restrictions [74]. These circumvention tools could use tunneling technologies, and obfuscation techniques to avoid detection. However, some prior research has highlighted the burgeoning commercial VPN ecosystem with too many providers to choose from [72], many providers containing leakages and implementation failures in VPNs [52,70], and has shown even with obfuscation techniques, OpenVPN is still at risk of being fingerprintable by censors and network providers [97].

Russia's invasion of Ukraine led to various countries imposing economic sanctions [26,92]. Jonker et al. [49] investigated the effects of such sanctions on Internet infrastructure, and their consequences for Russian domain owners, by exploring longitudinal changes in the infrastructure used by Russian sites. They found that the impact on sanctioned domains was small: most subjected domains had been hosted in Russian ASes before the conflict. In contrast, our geoblocking measurements show recent changes in access restrictions for many Russian government websites. In contrast to previous work on geoblocking [53, 60], we find that many news media as well as education domains geoblock Russian users.

8 Limitations

Study Time Period This paper focuses on changes to the global Internet, in terms of Internet freedom and security, immediately following Russia's invasion of Ukraine in 2022. This event is what spurred our investigations, and so we could collect targeted measurements only in the months afterward, specifically February 2022 to May 2022. We supplement our own after-the-fact measurements with data before this period from public datasets, when possible. However, *the conflict is still ongoing at the time of writing*, and future work can investigate and report on long-term changes to the network. We open-source the measurement toolkits we built, to enable continued monitoring [7].

Measurements We combine data from multiple sources with our own novel measurements to obtain a multi-perspective view of network changes after Russia's invasion in 2022. Our study is naturally limited to the set of endpoints tested, and is subject to the constraints of third-party public datasets. OONI and Censored Planet's test lists (about 2,000 websites) tend toward popular and politically sensitive websites, and the platforms do not have coverage of all networks in Russia, however, they do cover the major ASes. Our geoblocking measurements are done from 19 geo-distributed VPs, which provides an in-depth view of geoblocking by Russian and foreign domains. However, we may miss fine-grained regional patterns because of a lack of VPs. Finally, our measurements of Russia's domestic CA used two major browsers, Chrome and Yandex, but the behavior of other browsers may be relevant. Our estimation of the extent of geoblocking, which treats geoblocking as a function of source IP address, is

a conservative one, as other factors that could also affect this decision, such as language preferences and user agent strings.

9 Discussion and Conclusion

We have recorded the infringements on Internet freedom that resulted from the escalation of the war in Ukraine. Our multi-perspective analysis shows how splintering of the Internet is exacerbated by actors on all sides, including the Russian government, ISPs, and foreign services. The events in Russia demonstrate that a threatened effect of any future geopolitical conflicts is splintering of the Internet. It is a cautionary tale for Internet freedom activists that highlights how easily censors and large Internet services may isolate specific regions from the support of the rest of the world.

Many companies, whether for legal or humanitarian reasons, have taken to implementing strict measures to restrict Russian users. These policies ultimately hurt Russian users, including those who want to educate themselves about the invasion, or condemn it. The widespread prevalence of CDN-enabled geoblocking shows the outsize influence companies have to estrange users from any part of the world.

There is a pernicious asymmetry in blocks due to sanctions: once in place, they are hard to remove, and may last longer than necessary since there are generally no penalties for overcompliance [5, 50]. For instance, previous work showed services continuing to refuse access from Sudan and Iran, even after US sanctions on Sudan had been relaxed in 2017 and 2022 respectively [56, 60]. Moreover, overcompliance with sanctions could lead to collateral blocking, where users from non-sanctioned countries are affected, because of proximity in geography or network topology. More studies like ours will help highlight the dangers of overcompliance with sanctions and prevent further splintering of the Internet.

We observe both Russian authorities and foreign actors taking advantage of the decentralized nature of the Internet to implement more access restrictions and localized control. For instance, Russia's move towards a localized certificate authority, and having local browsers trust it, is an alarming expansion of its capabilities. When critical services are involved, like banks, Russian users inside and outside Russia are forced to either install a root CA certificate or use a state-approved browser, which increases the risk of future man-in-the-middle attacks, reminiscent of events in Kazakhstan [83]. We worry that success by Russia will cause a domino effect that encourages other countries to create local bubbles of information control that are hard to monitor and advocate against.

Preventing the splintering of the global Internet will require multi-faceted support and cooperation from the private sector, academia, and the Internet freedom community. This type of study is possible only because of collaboration between researchers, Internet freedom groups, and industry partners, who came together at a time of dire need and worked towards the common goal of getting users connected to Internet resources. Rapid-response studies like this one are unfortunately not sustainable at scale, since current monitoring platforms are not equipped to study multiple types of restrictions and share data. We hope our work inspires advances in censorship measurement capabilities, and encourages more collaboration and data sharing, in order to inform better policies and protect the Internet as a global medium.

10 Acknowledgment

The authors are grateful to our shepherd and the reviewers for their feedback. This work was made possible by the Open Technology Fund, the Defense Advanced Research Projects Agency under Agreement No. HR00112190127 and a Bureau of Democracy, Human Rights and Labor (DRL) Grant (No. SLMAQM20GR2132), and National Science Foundation grant CNS-2141512 and CNS-2237552.

References

[1] Access Now. Letter to U.S. government: Do not disrupt internet access in Russia or Belarus, Mar. 2022. https://www.accessnow.org/letter-us-government-internet-access-russia-belarus-ukraine/.

[2] D. Anderson. Splinternet behind the Great Firewall of China: Once China opened its door to the world, it could not close it again. *Queue*, 10(11):40–49, 2012. https://dl.acm.org/doi/10.1145/2390756.2405036.

[3] BBC News. What sanctions are being imposed on Russia over Ukraine invasion?, Jan. 2022. https://www.bbc.com/news/world-europe-60125659.

[4] CA/Browser Forum. Information for Developers. https://cabforum.org/information-for-manufacturers-and-developers.

[5] N. Campbell and N. El Saadany. Sanctions can deny Internet access when people need it most. Internet Society, 2022. https://www.internetsociety.org/blog/2022/09/sanctions-can-deny-internet-access-when-people-need-it-most/.

[6] Censored Planet. CenTrace Tool. https://github.com/censoredplanet/centrace.

[7] Censored Planet. GeoInspector Tool. https://github.com/censoredplanet/geoinspector.

[8] Censored Planet Observatory. https://censoredplanet.org/data/raw.

[9] Censys Search API, May 2022. https://search.censys.io/api.

[10] Certificate Search. https://crt.sh.

[11] Certificate Search – Promsvyazbank, Mar. 2022. https://crt.sh/?id=2713661323.

[12] Certificate Search – The Central Bank of the Russian Federation, Feb. 2022. https://crt.sh/?id=2355590937.

[13] Certificate Search – VTB Bank, Mar. 2022. https://crt.sh/?id=5828347935.

[14] Citizen Lab et al. URL testing lists intended for discovering website censorship, 2014. https://github.com/citizenlab/test-lists.

[15] D. Ciuriak. Social media warfare is being invented in Ukraine. Centre for International Governance Innovation, 2022. https://www.cigionline.org/articles/social-media-warfare-is-being-invented-in-ukraine/.

[16] Dan York. What is the Splinternet? and why you should be paying attention. Internet Society, 2023. https://www.internetsociety.org/blog/2022/03/what-is-the-splinternet-and-why-you-should-be-paying-attention/.

[17] DigiCert. Embargoed countries & regions, Mar. 2022. https://knowledge.digicert.com/solution/Embargoed-Countries-and-Regions.html.

[18] R. Dingledine and N. Mathewson. Tor protocol specification, Nov. 2021. https://spec.torproject.org/tor-spec.

[19] D. Dittrich, E. Kenneally, et al. The Menlo Report: Ethical principles guiding information and communication technology research. Technical report, U.S. Department of Homeland Security Science and Technology Directorate, 2012. https://www.dhs.gov/publication/st-menlo-report.

[20] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman. Censys: A search engine backed by Internet-wide scanning. In *ACM Conference on Computer and Communications Security (CCS)*, 2015. https://dl.acm.org/doi/10.1145/2810103.2813703.

[21] K. Ermoshina, B. Loveluck, and F. Musiani. A market of black boxes: The political economy of Internet surveillance and censorship in Russia. *Journal of Information Technology & Politics*, 19(1), 2022.

[22] A. Faiola. How millions of Russians are tearing holes in the Digital Iron Curtain. *The Washington Post*, May 2022. https://www.washingtonpost.com/world/2022/05/06/russia-vpn-putin-censorship-disinformation/.

[23] M. Fedorov. We are creating an IT army. We need digital talents. All operational tasks will be given here: t.me/itarmyofurraine. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists. Tweet, Feb. 2022. https://twitter.com/FedorovMykhailo/status/1497642156076511233.

[24] Free and Open Communications on the Internet, 2023. https://foci.community/.

[25] R. Fontugne, K. Ermoshina, and E. Aben. The Internet in Crimea: a case study on routing interregnum. In *IFIP Networking Conference*, 2020. https://ieeexplore.ieee.org/document/9142776.

[26] Foreign, Commonwealth and Development Office. The UK sanctions list. https://www.gov.uk/government/publications/the-uk-sanctions-list.

[27] S. Ghaffary. Russia continues its online censorship spree by blocking Instagram. *Vox*, Mar. 2022. https://www.vox.com/recode/22962274/russia-block-instagram-facebook-restrict-twitter-putin-censorship-ukraine.

[28] GoDaddy. How GoDaddy is supporting Ukrainian customers, Mar. 2022. https://aboutus.godaddy.net/newsroom/company-news/news-details/2022/How-GoDaddy-is-Supporting-Ukrainian-Customers/default.aspx.

[29] Y. Golovchenko. Fighting propaganda with censorship: A study of the Ukrainian ban on Russian social media. *The Journal of Politics*, 84(2), Apr. 2022.

[30] Gosuslugi. List of domains signed by Russia's CA. https://www.gosuslugi.ru/api/nsi/v1/custom/dic/tls/csv.

[31] Gosuslugi. Получите электронный сертификат безопасности. (Translation) Get an electronic security certificate. https://www.gosuslugi.ru/tls.

[32] S. Harris and P. Sonne. Russia planning massive military offensive against Ukraine involving 175,000 troops, U.S. intelligence warns. *The Washington Post*, Dec. 2021. https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.

[33] T. Hatmaker. Spotify will suspend its services in Russia in light of free speech crackdown. *TechCrunch*, Mar. 2022. https://techcrunch.com/2022/03/25/spotify-will-suspend-its-services-in-russia-in-light-of-free-speech-crackdown/.

[34] IdenTrust. TrustID and IGC foreign certificates list, Mar. 2022. https://www.identrust.com/sites/default/files/resources/trustid_and_igc_foreign_countries_lists_en.pdf.

[35] M. Ilyushina. Russian government websites face 'unprecedented' wave of hacking attacks, ministry says. *The Washington Post*, Mar. 2022. https://www.washingtonpost.com/world/2022/03/17/russia-government-hacking-wave-unprecedented/.

[36] Internet Archive. Wayback Machine. https://web.archive.org/.

[37] Internet Archive. Wayback Machine – Example of geoblocking page (`fpi.gov.ru`). https://web.archive.org/web/2022*/fpi.gov.ru.

[38] Internet Archive. Wayback Machine – Example of TCP timeouts (`fas.gov.ru`). https://web.archive.org/web/2022*/fas.gov.ru.

[39] IODA. https://ioda.inetintel.cc.gatech.edu/asn/.

[40] IODA. Twitter BGP hijack incident by RTComm (AS8342). https://grip.inetintel.cc.gatech.edu/events/moas/moas-1648469100-13414_8342.

[41] IODA Signals for AS196747 (Electronic-government). https://ioda.inetintel.cc.gatech.edu/asn/196747?from=1645592400&until=1648094399.

[42] IODA Signals for AS198074 (PESSPB-AS). https://ioda.inetintel.cc.gatech.edu/asn/198074?from=1645938000&until=1648439999.

[43] IODA Signals for AS210954 (LASPACE). https://ioda.inetintel.cc.gatech.edu/asn/210954?from=1645938000&until=1648439999.

[44] IODA Signals for AS41180 (RFERL-Moscow). https://ioda.inetintel.cc.gatech.edu/asn/41180?from=1646802000&until=1649563199.

[45] IODA Signals for AS48122 (MIHELICOPTER-AS). https://ioda.inetintel.cc.gatech.edu/asn/48122?from=1645938000&until=1648439999.

[46] IVPN. https://www.ivpn.net/.

[47] B. Jones, R. Ensafi, N. Feamster, V. Paxson, and N. Weaver. Ethical concerns for censorship measurement. In *NS Ethics '15: Proceedings of the 2015 ACM SIGCOMM Workshop on Ethics in Networked Systems Research*, 2015. https://www.icir.org/vern/papers/censorship-meas.nsethics15.pdf.

[48] B. Jones, T.-W. Lee, N. Feamster, and P. Gill. Automated detection and fingerprinting of censorship block pages. In *Internet Measurement Conference (IMC)*. ACM, 2014. https://people.cs.umass.edu/~phillipa/papers/JLFG14.pdf.

[49] M. Jonker, G. Akiwate, A. Affinito, A. Botta, G. M. Voelker, and S. Savage. Where .ru? Assessing the impact of conflict on Russian domain infrastructure. In *Internet Measurement Conference (IMC)*. ACM, 2022. https://cseweb.ucsd.edu/~savage/papers/IMC2022-RU.pdf.

[50] Julia Grauvogel. Easier in than out: The protracted process of ending sanctions. German Institute for Global and Area Studies, 2019. https://www.giga-hamburg.de/en/publications/giga-focus/easier-in-than-out-the-protracted-process-of-ending-sanctions.

[51] D. Kaye. Online propaganda, censorship and human rights in Russia's war against reality. *American Journal of International Law*, 2022. https://www.cambridge.org/core/journals/american-journal-of-international-law/article/online-propaganda-censorship-and-human-rights-in-russias-war-against-reality/359EF362F588AC8F601FE6C28260AD83.

[52] M. T. Khan, J. DeBlasio, G. M. Voelker, A. C. Snoeren, C. Kanich, and N. Vallina-Rodriguez. An empirical analysis of the commercial VPN ecosystem. In *Proceedings of the Internet Measurement Conference (IMC)*, 2018. https://dl.acm.org/doi/10.1145/3278532.3278570.

[53] R. Kumar, A. Virkud, R. Sundara Raman, A. Prakash, and R. Ensafi. A large-scale investigation into geodifferences in mobile apps. In *USENIX Security Symposium*, 2022. https://www.usenix.org/conference/usenixsecurity22/presentation/kumar.

[54] B. Lang. Netflix suspends service in Russia amid invasion of Ukraine. *Variety*, Mar. 2022. https://variety.com/2022/digital/news/netflix-suspends-service-russia-ukraine-invasion-1235197390/.

[55] M. A. Lemley. The Splinternet. *Duke LJ*, 70, 2020. https://scholarship.law.duke.edu/dlj/vol70/iss6/3/.

[56] S. Lyngaas. Cloudflare says White House asked tech firm to bypass Iran censorship, but US sanctions got in the way. CNN, 2023. https://edition.cnn.com/2023/01/19/tech/cloudflare-white-house-iran-censorship-bypass/.

[57] D. Madory. The Ukraine network of @RFERL (62.4.111.0/24) went down at 17:13 UTC (7:13pm local) on 23-Feb and hasn't returned. #UkraineRussiaConflict. Tweet, Feb. 2022. https://twitter.com/DougMadory/status/1497020385195442182.

[58] Matthew Mpoke Bigg. A history of the tensions between Ukraine and Russia. the New York Times, 2022. https://www.nytimes.com/2022/03/26/world/europe/ukraine-russia-tensions-timeline.html.

[59] V. Matviyenko. О Федеральном законе «О внесении изменений в Федеральный закон „О связи“ и Федеральный закон „Об информации, информационных технологиях и о защите информации“. (Translation) On the Federal Law "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'", Apr. 2022. http://council.gov.ru/activity/documents/104263/.

[60] A. McDonald, M. Bernhard, L. Valenta, B. VanderSloot, W. Scott, N. Sullivan, J. A. Halderman, and R. Ensafi. 403 Forbidden: A global view of CDN geoblocking. In *Internet Measurement Conference (IMC)*. ACM, 2018. https://censoredplanet.org/assets/403forbidden.pdf.

[61] Mozilla dev-security-policy. Russia preparing for MitM, Mar. 2022. https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/QaKxfr5hOXg.

[62] Multiple authors. MITM in Russia, Mar. 2022. https://bugzilla.mozilla.org/show_bug.cgi?id=1758773.

[63] A. A. Niaki, S. Cho, Z. Weinberg, N. P. Hoang, A. Razaghpanah, N. Christin, and P. Gill. ICLab: A global, longitudinal internet censorship measurement platform. In *2020 IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2020. https://people.cs.umass.edu/~phillipa/papers/oakland2020.pdf.

[64] OONI: Open Observatory of Network Interference. https://ooni.org/.

[65] R. Padmanabhan, A. Filastò, M. Xynou, R. Sundara Raman, K. Middleton, M. Zhang, D. Madory, M. Roberts, and A. Dainotti. A multi-perspective view of Internet censorship in Myanmar. In *Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet*, 2021. https://dl.acm.org/doi/10.1145/3473604.3474562.

[66] P. Pearce, B. Jones, F. Li, R. Ensafi, N. Feamster, N. Weaver, and V. Paxson. Global measurement of DNS manipulation. In *USENIX Security Symposium*, 2017. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/pearce.

[67] J. Pearson and C. Bing. U.S. targets Russia with tech to evade censorship of Ukraine news. *Reuters*, June 2022. https://www.reuters.com/world/exclusive-us-targets-russia-with-tech-evade-censorship-ukraine-news-2022-06-15/.

[68] V. L. Pochat, T. V. Goethem, S. Tajalizadehkhoob, M. Korczynski, and W. Joosen. Tranco: A research-oriented top sites ranking hardened against manipulation. In *Network and Distributed Systems Security Symposium (NDSS)*. Internet Society, 2019. https://doi.org/10.14722/ndss.2019.23386.

[69] Psiphon. https://psiphon.ca/.

[70] R. Ramesh, L. Evdokimov, D. Xue, and R. Ensafi. VPNalyzer: Systematic investigation of the VPN ecosystem. In *Network and Distributed System Security*, 2022. https://dx.doi.org/10.14722/ndss.2022.24285.

[71] R. Ramesh, R. Sundara Raman, M. Bernhard, V. Ongkowijaya, L. Evdokimov, A. Edmundson, S. Sprecher, M. Ikram, and R. Ensafi. Decentralized Control: A Case Study of Russia. In *Network and Distributed Systems Security Symposium (NDSS)*. Internet Society, 2020. https://www.ndss-symposium.org/wp-content/uploads/2020/02/23098.pdf.

[72] R. Ramesh, A. Vyas, and R. Ensafi. "All of them claim to be the best": Multi-perspective study of VPN users and VPN providers. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, 2023. https://www.usenix.org/conference/usenixsecurity23/presentation/ramesh.

[73] Reuters. Russia reinstates Twitter slowdown, says Meta, Google are 'instigators of war'. *Reuters*, Mar. 2022. https://www.reuters.com/world/russia-reinstates-twitter-traffic-slowdown-computers-over-fake-ukraine-posts-2022-03-01/.

[74] H. Roberts, E. Zuckerman, and J. G. Palfrey. 2011 circumvention tool evaluation. *Berkman Center Research Publication*, (2011-08), 2011. https://ssrn.com/abstract=1940455.

[75] Roskomnadzor. О принятии мер в отношении сервисов обхода ограничения доступа к противоправному контенту. (Translation) On adopting measures in relation to services that circumvent restrictions on access to unlawful content, June 2021. https://rkn.gov.ru/news/rsoc/news73700.htm.

[76] Roskomnadzor. Приняты ответные меры на ограничение доступа к российским СМИ. (Translation) Response measures taken to restrict access to Russian media, Mar. 2022. https://rkn.gov.ru/news/rsoc/news74156.htm.

[77] Roskomsvoboda. Russia introduces a domestic root TLS certificate, 2022. https://roskomsvoboda.org/post/gossertifikat-dlya-saytov.

[78] Roskomsvoboda and OONI. How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine, Feb. 2023. https://ooni.org/post/2023-russia-a-year-after-the-conflict/.

[79] University of Oregon Route Views Project. http://www.routeviews.org/.

[80] S. Singanamalla, E. H. B. Jang, R. Anderson, T. Kohno, and K. Heimerl. Accept the risk and continue: Measuring the long tail of government https adoption. In *Internet Measurement Conference (IMC)*. ACM, 2020. https://ictd.cs.washington.edu/docs/papers/2020/IMC2020-Government-HTTPS-Measurement.pdf.

[81] Snowflake, Apr. 2022. https://snowflake.torproject.org/.

[82] J. Sonnenfeld et al. Almost 1,000 companies have curtailed operations in Russia—but some remain. Yale School of Management, May 2022. https://som.yale.edu/story/2022/almost-1000-companies-have-curtailed-operations-russia-some-remain.

[83] R. Sundara Raman, L. Evdokimov, E. Wustrow, J. A. Halderman, and R. Ensafi. Investigating large scale HTTPS interception in Kazakhstan. In *Internet Measurement Conference (IMC)*. ACM, 2020. https://censoredplanet.org/assets/Kazakhstan.pdf.

[84] R. Sundara Raman, P. Shenoy, K. Kohls, and R. Ensafi. Censored Planet: An Internet-wide, Longitudinal Censorship Observatory. In *Conference on Computer and Communications Security (CCS)*. ACM, 2020. https://censoredplanet.org/assets/censoredplanet.pdf.

[85] R. Sundara Raman, A. Stoll, J. Dalek, R. Ramesh, W. Scott, and R. Ensafi. Measuring the deployment of network censorship filters at global scale. In *Network and Distributed Systems Symposium (NDSS)*. Internet Society, 2020. https://censoredplanet.org/assets/filtermap.pdf.

[86] R. Sundara Raman, A. Virkud, S. Laplante, V. Fortuna, and R. Ensafi. Advancing the art of censorship data analysis. In *Free and Open Communications on the Internet (FOCI)*, 2023. https://www.petsymposium.org/foci/2023/foci-2023-0003.php.

[87] R. Sundara Raman, M. Wang, J. Dalek, J. Mayer, and R. Ensafi. Network measurement methods for locating and examining censorship devices. In *In ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, 2022. https://censoredplanet.org/assets/censorship-devices.pdf.

[88] A. Teraoka and R. Namiki. Russia walls off government websites from nonfriendly countries. *Nikkei Asia*, Mar. 2022. https://asia.nikkei.com/Politics/Ukraine-war/Russia-walls-off-government-websites-from-nonfriendly-countries.

[89] The White House. Fact sheet: United States, G7 and EU impose severe and immediate costs on Russia, Apr. 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/.

[90] Tor Project. New alpha release: Tor Browser 11.5a1 (Windows, macOS, Linux), Dec. 2021. https://blog.torproject.org/new-release-tor-browser-115a1/.

[91] Tor Project, May 2022. https://torproject.org/.

[92] U.S. Department of the Treasury. Specially designated nationals and blocked persons list (SDN) human readable lists. https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

[93] I. Valentovitch and K. Ermoshina. Measuring Internet censorship in disputed areas: An examination of online media filtering in Russia and Crimea during the 2018 Russian presidential elections. Technical report, Open Technology Fund, May 2018. https://www.opentech.fund/news/exploring-online-media-filtering-during-2018-russian-presidential-elections/.

[94] V. Weber. The worldwide web of Chinese and Russian information controls. *Centre for Technology and Global Affairs Working Paper Series*, Sept. 2019. https://www.ctga.ox.ac.uk/article/worldwide-web-chinese-and-russian-information-controls.

[95] Splinternet. https://en.wikipedia.org/wiki/Splinternet.

[96] D. Xue, B. Mixon-Baca, ValdikSS, A. Ablove, B. Kujath, J. R. Crandall, and R. Ensafi. TSPU: Russia's decentralized censorship system. In *Internet Measurement Conference (IMC)*. ACM, 2022. https://censoredplanet.org/assets/tspu-imc22.pdf.

[97] D. Xue, R. Ramesh, A. Jain, M. Kallitsis, J. A. Halderman, J. R. Crandall, and R. Ensafi. OpenVPN is open to VPN fingerprinting. In *USENIX Security Symposium*. USENIX Association, 2022. https://www.usenix.org/conference/usenixsecurity22/presentation/xue-diwen.

[98] D. Xue, R. Ramesh, ValdikSS, L. Evdokimov, A. Viktorov, A. Jain, E. Wustrow, S. Basso, and R. Ensafi. Throttling Twitter: An emerging censorship technique in Russia. In *Internet Measurement Conference (IMC)*. ACM, 2021. https://censoredplanet.org/assets/throttling-imc-paper.pdf.

[99] M. Xynou and A. Filastò. Russia started blocking Tor, Dec. 2021. https://ooni.org/post/2021-russia-blocks-tor/.

[100] M. Xynou and A. Filastò. New blocks emerge in Russia amid war in Ukraine: An OONI network measurement analysis, Mar. 2022. https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/.

[101] B. Zevenbergen et al. *NS Ethics '15: Proceedings of the 2015 ACM SIGCOMM Workshop on Ethics in Networked Systems Research*. ACM, 2015. https://conferences.sigcomm.org/sigcomm/2015/pdf/papers/sigcomm_2015/forms/nsethics.htm.