Where .ru? Assessing the Impact of Conflict on Russian Domain Infrastructure

Mattijs Jonker
University of Twente

Gautam Akiwate
UC San Diego

Antonia Affinito
University of Naples

kc Claffy
CAIDA / UC San Diego

Alessio Botta
University of Naples

Geoffrey M. Voelker
UC San Diego

Roland van Rijswijk-Deij
University of Twente

Stefan Savage
UC San Diego

ABSTRACT

The hostilities in Ukraine have driven unprecedented forces, both from third-party countries and in Russia, to create economic barriers. In the Internet, these manifest both as internal pressures on Russian sites to (re-)patriate the infrastructure they depend on (*e.g.*, naming and hosting) and external pressures arising from Western providers disassociating from some or all Russian customers. While quite a bit has been written about this both from a policy perspective and anecdotally, our paper places the question on an empirical footing and directly measures longitudinal changes in the makeup of naming, hosting and certificate issuance for domains in the Russian Federation.

CCS CONCEPTS

• **Networks → Naming and addressing**; • **Social and professional topics → Governmental regulations**; *Network operations*; Import / export controls; *Centralization / decentralization.*

KEYWORDS

DNS, Hosting, Web PKI, Infrastructure, Sanctions, Conflict

ACM Reference Format:

Mattijs Jonker, Gautam Akiwate, Antonia Affinito, kc Claffy, Alessio Botta, Geoffrey M. Voelker, Roland van Rijswijk-Deij, and Stefan Savage. 2022. Where .ru? Assessing the Impact of Conflict on Russian Domain Infrastructure. In *Internet Measurement Conference (IMC '22), October 25–27, 2022, Nice, France.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3517745.3561423

1 INTRODUCTION

On February 24, 2022, Russian forces invaded Ukraine, leading to the largest refugee crisis in Europe since World War II. Unlike Russia's 2014 annexation of Crimea or ongoing support for separatists in Ukraine's south-east, this escalation produced a strong global response — particularly from Western countries. In addition to providing military and financial support for Ukraine, Western countries imposed broad economic sanctions against Russian entities, including the Russian Central Bank, imposed export controls to deny Russia access to strategic material, seized or froze property and assets held abroad, and imposed flight bans and travel restrictions. In addition to these government actions, a broad array of roughly 1,000 private sector companies independently restricted or exited the Russian market [16].

The Internet has not escaped this conflict. For example, the US Office of Foreign Asset Control (OFAC) started listing particular Russian corporate Web sites on its Specially Designated Nationals (SDN) list of sanctioned entities [17]. Independent of these particular sanctions, many western Internet service companies have decided — for some combination of moral principle, reputational risk and/or economic volatility — to broadly disengage from the Russian market. While some have simply halted new sales to Russian customers (*e.g.*, Amazon, Microsoft, Google [13], GoDaddy [6]), others, such as Cogent, have stopped providing service to Russia entirely [20]. Ukraine has advocated for such actions and on March 1st, 2022, their Deputy Prime-Minster formally requested that ICANN revoke the .ru, .рф and .su domains, support the revocation of all TLS certificates for those domains and shut down DNS root servers located in the Russian Federation [5].

These actions have reinforced Russia's long-held concerns about threats to their "Internet sovereignty", leading the government to take proactive steps to repatriate key services.[1] In March 2022, Russian authorities mandated that all state-owned websites and services switch exclusively to domestic ISPs, DNS operators and hosting providers [23]. Similarly, the Russian Ministry of Digital Development announced that it was standing up an independent state-operated Certificate Authority whose root certificate would be trusted by Russian browsers (VK Atom and Yandex.Browser).[2] Russian private sector operators have also started to anticipate third-party disengagement: RU-CENTER, Russia's leading registrar and hosting provider, advised customers "operating in sectors subject to international sanctions" to "purchase certificates by GlobalSign, a Japanese certification authority" [22].

These internal re-patriation pressures from the Russian government, combined with the risk of further shunning by Western service providers, suggest an unprecedented environment for Russian operators and their enterprise customers. It would be entirely reasonable to hypothesize that these forces are driving Russian sites to rapidly decouple from non-Russian infrastructure. This paper is an attempt to put this question on an empirical footing.

[1] Russia has a long of history of trying to exert control over its domestic Internet, including requirements for domestic data storage and surveillance [4] and the ability, recently tested by communications regulator Roskomnadzor, to actively disconnect the country from the global Internet if needed.

[2] The timing of this action appears to have been related to DigiCert's revocation of Russian Bank VTB's TLS certificate — presumably in response to VTB's sanctioning by the US OFAC.

IMC '22, October 25–27, 2022, Nice, France

ACM ISBN 978-1-4503-9259-4/22/10.
https://doi.org/10.1145/3517745.3561423

In particular, we explore the longitudinal changes in the infrastructure used by Russian sites — notably DNS, hosting, and TLS certificate issuance — before and after the invasion of Ukraine. Our analysis combines five years of daily `.ru` and .рф zone transfer data, with contemporary active measurements and historic certificate issuance data. We explore the extent to which such sites have experienced significant patriation of their infrastructure and, to the extent such changes exist, whether they can be best explained by the actions of service providers outside Russia or by the anticipatory decisions made by Russian site operators themselves.

2 DATA SETS

We use DNS measurement data of all domain names registered under the Russian Federation country code top-level domains (ccTLDs) `.ru` and .рф[3] over a nearly five-year period (1803 days). The exact period of our study is June 18, 2017 through May 25, 2022, meaning the data extends years before Russia's invasion of Ukraine on February 24, 2022, and also extends 90 days forward of this point.

The DNS measurements were provided by the OpenINTEL project, which uses daily zone file snapshots as seeds to actively query all registered domain names under a TLD for a selection of DNS resource records [21].[4] The collected data include each domain's `NS` records (to investigate whether name service is delegated outside `.ru` and .рф), as well as the `A` record resolution for both their name servers and apex domain. We geolocate each of the resulting IP addresses, using contemporaneous results from the IP2location service [9], to provide a proxy for the physical hosting of each domain's DNS infrastructure and Web site, respectively.[5] Our dataset contains *11.7 M* unique Russian Federation domain names, and *13.3 k* and *9.5 k* unique networks (AS numbers) that, respectively, hosted domain apexes or authoritative DNS infrastructure.

We also collected longitudinal certificate data for the `.ru` and .рф domains using both historic certificate transparency logs, as well as active scans by Censys [2] of Internet Web sites during the collection period.[6] Finally, we label 107 unique domains as being specifically *sanctioned* based on their appearance on either US OFAC SDN [17] or UK sanctions lists [7].[7]

3 IMPACT ON DNS ECOSYSTEM

In this section we first provide historical context for the DNS infrastructure supporting `.ru` and .рф domains, and then focus on activity surrounding the 2022 invasion for all Russian domains, sanctioned Russian domains, and the actions taken by major Western providers.

3.1 Historical Context

For historical context, we start by characterizing the long-term locations of Russian domain hosting and name server infrastructure across our full data set from June 18, 2017, to May 25, 2022. We label a domain as *fully* Russian-hosted if all of its `A` records geolocate inside the Russian Federation, *partial* if only a subset are in Russia, or *non* (Russian) if all such records are located outside the Russian Federation. Name service is similarly labeled based on geolocating the authoritative name servers for the domain.

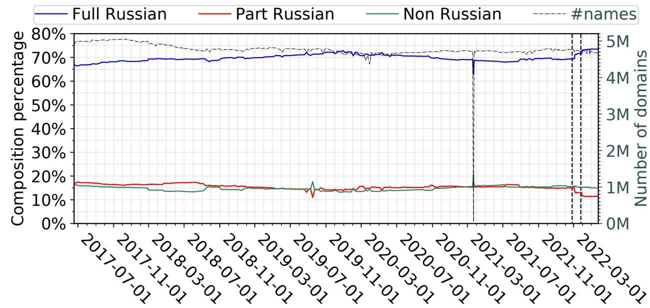

Figure 1: Country composition of DNS infrastructure of `.ru` and .рф domain names. *Full* means the authoritative name servers fully geolocate to Russia. *Non* means the servers altogether do not. *Part* means they partially do.

Historically, the fraction of domains hosted in Russian networks only fluctuates mildly over our period of study. For example, on June 18, 2017, *71.0%* of `.ru` and .рф names are *fully* hosted in Russia, *0.19%* are *partial*, and *28.81%* are *non* Russian. This hosting breakdown does not change significantly until the Ukrainian invasion in February 2022. At that point, there is a *slight* increase in both *fully* and *partial* domains driven by flight from the US and other Western countries to a combination of Russia and the Netherlands.

The name server infrastructure for Russian domains is also relatively stable over the long term, but shows a more pronounced change once the conflict starts. Figure 1 shows this longitudinal name server breakdown in more detail. For all domain names registered under `.ru` and .рф, it displays whether their delegated name servers are *fully*, *partially* or altogether not located inside Russia.[8] The black curve shows the total number of Russian domains (right ticks). As points of reference, we divide recent months into three time periods: pre-conflict (before February 24, 2022), post-sanctions (after March 26, 2022), and pre-sanctions (the period in-between). We delineate these periods in the graphs with vertical dashed lines.

On June 18, 2017, there are just under *5 M* registered domains, *67.0%* of which have name servers *fully* located in Russia. This breakdown, along with the roughly equivalent levels of *partial* and *non* domains, is stable over time, suggesting that internal patriation pressure in the years immediately prior to the 2022 conflict have had little bearing in practice. Changes do become apparent in February 2022, when many domains with name servers *partially* outside Russia clearly transition towards *fully* Russian. However, in historical context, these changes are minor. For our most recent data, *73.9%* names are *fully* Russian, only a *6.9%* change over the five-year period.

One aspect of Russian domain infrastructure that becomes less Russian-focused over time are the TLD dependencies of Russian

[3] .рф is the Cyrillic code for Russian Federation. The internationalized domain name form of this ccTLD is `.xn--p1ai`.

[4] https://openintel.nl/coverage/

[5] We note that there is a small percentage of disagreement in country-level geolocation and inferences made regarding relocation may "lag behind," in particular when IP address (space) of hosting or DNS infrastructure is moved rather than changed.

[6] We consider a certificate to "match" if either its *Common Name (CN)* or *Subject Alternative Name (SAN)* fields include a domain name under a `.ru` or .рф TLD.

[7] While the US OFAC subsequently issued license exceptions for a range of Internet services on April 22, 2022 [24], we have not observed clear changes in certificate issuance behavior in response to this modified policy.

[8] The dip on March 22, 2021 is a measurement outage.

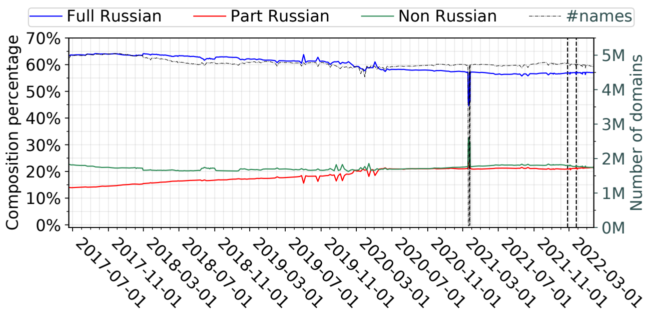

Figure 2: TLD dependency composition of `.ru` and .рф domain name authoritatives. *Full* means the name servers are all registered under Russian TLDs. *Non* means none are. *Part* means some but not all are.

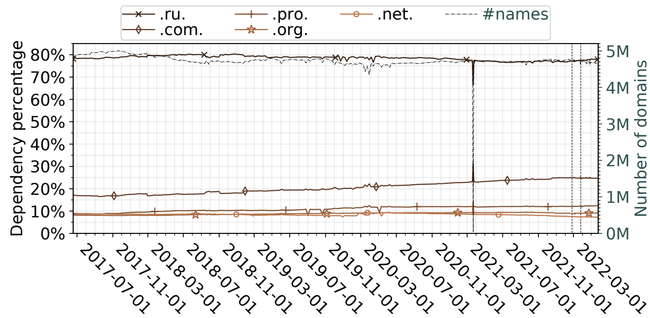

Figure 3: Top *5* TLDs used by authoritative name servers of `.ru` and .рф domain names. The other *265* TLDs (not shown) see *<1%* each.

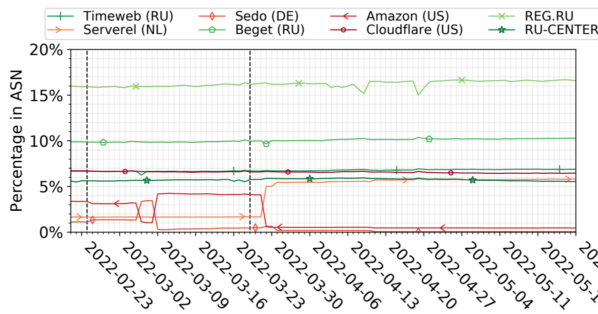

Figure 4: Hosting networks of `.ru` and .рф domain names (Top ASNs). The share of Russian domain names that each network hosts is shown. The vertical dashed lines delineate the *pre-conflict, pre-sanctions* and *post-sanctions* periods.

domains. We extract the TLD of each name server to which `.ru` and .рф domain names delegate authority. If all of a domain's name servers are exclusively registered under the Russian Federation TLDs, we consider the TLD dependency *fully* Russian. Similar to prior categorizations, if only a subset are Russian TLDs, we consider it *partial*, otherwise we consider it *non* Russian.

Figure 2 shows the name server TLD composition breakdown over time. Perhaps counter-intuitively, there is a slight downward trend in *fully* Russian (a net reduction of *6.3%* comparing extrema), and an increase in *partial* (a net increase of *7.9%*). Over time, Russian domains increasingly delegate to name servers whose names are in non-Russian TLDs, implicitly increasing their dependence on external infrastructure, which could become subject to Western sanctions. Figure 3 shows a longitudinal breakdown of specific TLDs under which authoritatives of Russian domains are registered. We show the Top *5* TLDs (out of a total *270*). Unsurprisingly, most Russian domains delegate to name servers with a name in `.ru`: *78.3%* on May 25, 2022. Second is `.com` with *24.7%* of Russian domains (a net increase of *7.5%* over the five-year period). Next in rank are: `.pro` (*12.4%* up from *8.8%*), `.org` (*9.2%* up from *8.2%*), and `.net` (*7.3%* down from *9.1%*). The remaining TLDs see *<1.0%* each (on May 25).

TLD dependency trends also change at the start of the conflict. Both *fully* and *partial* Russian compositions (Figure 2) increase very slightly (by *0.2%* and *0.5%*, respectively). As a result, the small fraction of Russian domains that changed from a *non* composition are less exposed to potential Western interference. Those that remain could become unresolvable in case the authoritatives stop providing service or Russia disconnects itself from the global Internet.

3.2 Recent Activity

In the post-conflict period, Russian domains have experienced more movement in their hosting networks, but the movement has almost entirely been among networks outside of Russia. Figure 4 shows a selection of providers networks that host `.ru` and .рф domain names. The Russian ASNs have stable and consistent customer bases over time, together accounting for *38%* of Russian domains at the start and *39%* at the end. The other stable curve is Cloudflare, which accounts for nearly *7%* of Russian domains throughout this period. The networks that *do* experience movement correspond to `.ru` and .рф domains that switch back and forth between Amazon (US) and Sedo (Germany), and then ultimately move to Serverel (Netherlands). This dynamic is, in part, driven by business reactions to the conflict, which we discuss further in Section 3.4.

Russian domains have also experienced changes regarding where their DNS infrastructure is hosted, with noticeable movement starting during the pre-sanctions period and continuing post-sanctions. A significant change involved Netnod, a Swedish DNS provider, and RU-CENTER, a large Russian domain name registrar and (former) Netnod customer. Due to IP address reconfigurations on March 3rd, Netnod stopped providing service for *76 k* Russian domains, which quickly changed from *partial* to *fully* Russian DNS infrastructure (Figure 1). We observe other large transitions at the end of March involving migration out of the networks of Hetzner (Germany) and Linode (US). One non-Russian network that hosts DNS infrastructure for a substantial number of Russian domains is Cloudflare, and this network sees little change since the conflict started.

3.3 Sanctioned Domain Names

We now focus on domain names specifically tied to Russian entities that were sanctioned by the US and UK.

Note that the potential for impact on the hosting of these domains is inherently slight as *101* of the *107* sanctioned domains (*94.4%*)

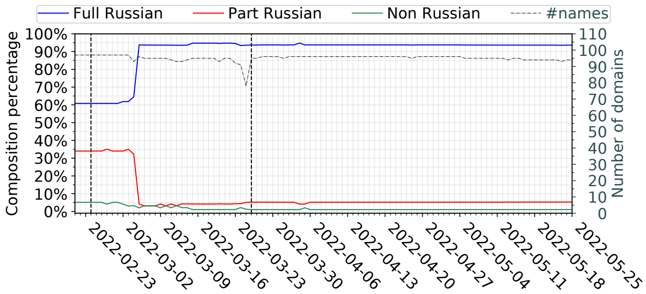

Figure 5: Country composition of DNS infrastructure authoritative for *sanctioned* Russian domains, broken down in fully, partially, and not geolocated to Russia. Significant movement is seen in the *pre-sanctions* period.

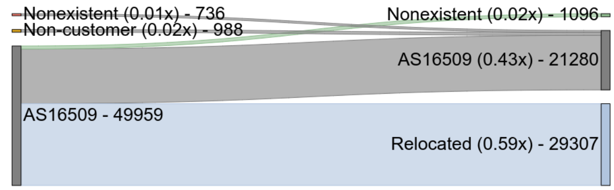

Figure 6: Russian domain name movement in *Amazon*'s `AS16509` (comparing 2022-03-08 and 2022-05-25).

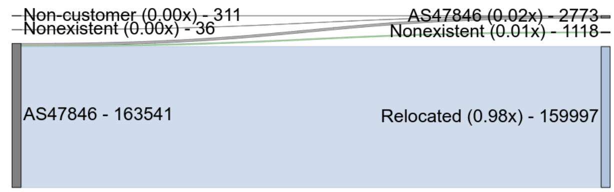

Figure 7: Russian domain name movement in *Sedo*'s `AS47846` (comparing 2022-03-08 and 2022-05-25).

were already hosted exclusively in Russian ASNs before the conflict on February 24, 2022. Three more became *fully* Russian hosted by May 25, 2022,[9] and the final three have remained *fully* hosted in Germany, Czech Republic, and Estonia.

However, the name server infrastructure for these sanctioned domains *has* experienced significant movement. Figure 5 shows the country composition of the authoritative name servers for these domains over time. The three colored curves again distinguish among *fully*, *partial* and *non* Russian composition, and the black curve shows the daily total number.

On February 24, 2022, *34.0%* of sanctioned domains are *partial* and *5.2% non* Russian. This situation drastically changes by March 4, 2022 when the vast majority (*93.8%*) of the DNS infrastructure for the sanctioned domains are strictly hosted in Russia. Note that for the *partial* sanctioned domains that changed to *full*, nearly all of them had an authoritative name server hosted by Netnod (in Sweden) until the change to *full* Russian on March 4.

3.4 Actions taken by Providers

A number of Western providers publicly stated the business actions their company would take in response to the conflict, either in voluntary protest or for alignment with sanctions. Using our DNS data, we examine the extent and effect of the business actions taken by four major Western providers.

Amazon – On March 8, 2022, Amazon reported that it would no longer be accepting new Russian or Belarusian AWS account registrations [1]. Since that time, we see significant changes in the makeup of `.ru` and .рф domains resolving to Amazon's ASN (`AS16509`), including the surprising appearance of newly hosted domains from these TLDs.

Figure 6 displays the movement of Russian domains that originally resolved to Amazon's ASN on March 8, 2022. By May 25, 2022, more than half of these domains relocated to other ASNs, but we do not know whether this reflects Amazon's initiative or independent customer decisions. A little under half (*43%*) remained, but this set also includes *574* newly registered `.ru` and .рф domain names (confirmed using Cisco's *Whois Domain* API) and *988* existing domains that relocated to Amazon. While this influx of *1.5 k* `.ru` and .рф names appears inconsistent with Amazon's statement, it is possible that these domains are owned by existing customers.[10]

Sedo – On March 9, 2022, it was reported that *Sedo* was "pulling the plug" on Russian domains [15]. Sedo followed through on its stated intention, although the plug was not pulled completely. Figure 7 shows the significant movement of `.ru` and .рф name hosting from Sedo's `AS47846`. Starting on March 8, 2022, *164 k* `.ru` and .рф domains resolved to Sedo's ASN (`AS47846`). By May 25, 2022, *160 k* (98%) had relocated to a different ASN, *2.7 k* (1.6%) remained, and *311* external domains relocated to Sedo.

Cloudflare – Cloudflare wrote in a March 7, 2022, article that it was complying with sanctions [18]. It also expressed that, in consultation with government and civil society experts, the company would not terminate Cloudflare's services inside Russia. The domain resolutions confirm that the company is doing business as usual. Starting March 7, 2022, nearly *315 k* `.ru` and .рф names resolved to `AS13335`. On May 25, 2022, a little over *296 k* (*94%* of the original set) remain in Cloudflare's AS, and *34 k* Russian domains newly appeared. This activity is consistent with the sentiment expressed by Cloudflare's CEO Matthew Prince, that "Russia needs more Internet access, not less" [18].

Google – On Thursday, March 10, 2022, a Google spokesperson was reported as saying that the company would stop accepting new customers in Russia [11], but declined to comment if existing cloud customers in Russia would see action taken. Starting on March 10, 2022, *17.7 k* `.ru` and .рф domains resolved to Google's ASN (`AS15169`). By May 25, 2022, *57.1%* (*10.1 k*) of these domains had relocated to a different ASN, but most of these (*75.2%*) had simply

[9] These three domains were previously hosted exclusively in Germany or Poland.

[10] Using Cisco's *Whois Domain* API, we found registrant information for a subset of these domains (≈*1/6th*). Manual inspection revealed that some registrations were business-as-usual or defensive, by non-Russian, existing Amazon customers (*e.g.*, Disney registered various brand names such as `thorloveandthunder.ru` and `blackpantherwakandaforever.ru`).

Pre-Conflict			Pre-Sanctions			Post-Sanctions		
Issuer Org.	# Certs	(%)	Issuer Org.	# Certs	(%)	Issuer Org.	# Certs	(%)
Let's Encrypt	6,586k	91.58%	Let's Encrypt	3,285k	98.06%	Let's Encrypt	5,458k	99.23%
DigiCert	244k	3.40%	GlobalSign	25k	0.76%	GlobalSign	28k	0.52%
cPanel	153k	2.13%	cPanel	11k	0.34%	Google	13k	0.24%
Other CAs	207k	2.89%	Other CAs	28k	0.84%	Other CAs	422	0.01%

Table 1: Issuing activity of Certificate Authorities in the three time periods in 2022.

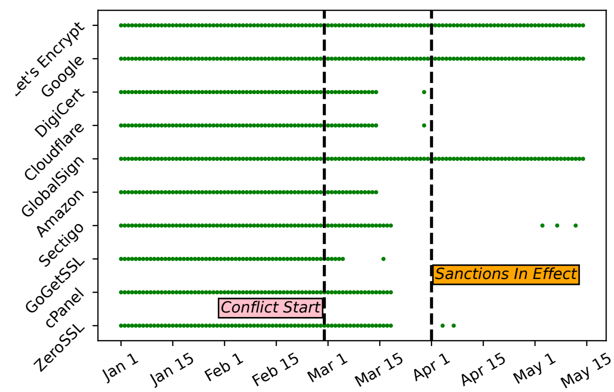

Figure 8: Timelines for CAs issuing new certificates for .ru and .рф domains. A green dot indicates the CA issued at least one certificate on the day.

relocated to a different Google ASN (AS396982).[11] In this period, a small number of external Russian domains (*187*) and newly registered domains (*184*) relocated to Google. As with Amazon, while seemingly inconsistent with Google's stated policy, it is possible that this influx of domains was created by existing customers.

4 IMPACT ON WEB PKI ECOSYSTEM

In the modern Web ecosystem, TLS certificates are crucial infrastructure for securing domains. In this section, we examine how Certificate Authorities (CAs) have reacted to the conflict and sanctions in terms of the certificates they authorize for Russian domains.

On the one hand, the conflict and sanctions *have not* significantly undermined the number of certificates issued for .ru and .рф domains from global CAs. For our three time periods in 2022, CAs issued *130 k* certificates per day on average pre-conflict, *115 k* certificates per day *pre-sanctions*, and *115 k* per day *post-sanctions*. However, individual CAs *have* reacted very differently to the conflict, and in this section we characterize the behavior of global CAs who issue and revoke certificates, as well as the effect of the new Russian Trusted Root CA.

4.1 Shift in Certificate Issuance

We use the Certificate Transparency (CT) logs indexed by Censys [2] to obtain the TLS certificates securing an .ru or .рф domain from January 1, 2022 to May 15, 2022. For each certificate, we extract the Issuer Organization term from the Issuer DN field to identify the CA responsible.

[11] Using OpenINTEL DNS measurement data of non Russian Federation domain names, we observe significant relocation from AS15169 to AS396982 for names under other TLDs too (around March 16). As such, we conclude that this intra-Google relocation did not occur because the *8.5 k* (*75.2%* of *10.1 k*) domains are Russian.

	.ru and .рф Domains		Sanctioned Domains	
Issuer	Issued	Revoked	Issued	Revoked
Let's Encrypt	15M	10k (0.06%)	16k	196 (1.19%)
DigiCert	247k	2.1k (0.80%)	308	308 (100%)
GlobalSign	95k	1.6k (1.68%)	905	23 (2.54%)
Sectigo	96k	5.1k (5.15%)	164	164 (100%)
ZeroSSL	56k	165 (0.30%)	82	2 (2.43%)

Table 2: Revocation activity by the five CAs with the most revocations.

Figure 8 shows timelines for when the top 10 CAs issue new certificates for Russian domains. A green dot indicates that the CA issued at least one certificate for a .ru or .рф domain on that day. Six of the ten top CAs for Russian domains stopped issuing certificates altogether after the conflict started or sanctions were imposed. The three CAs that continue issuing certificates are now the only major issuers for .ru and .рф domains. Since CAs typically issue certificates under different Common Names (CNs) (*e.g.*, DigiCert issues certificates under CNs RapidSSL and GeoTrust), we suspect the isolated dots are likely a result of CAs not preventing issuance from their lesser known CNs.

Table 1 shows the number of issued certificates in each of the three time periods for the top three issuing CAs in each period. Overall, the effect of the conflict has been to further concentrate certificate activity to just three CAs. While Let's Encrypt already dominated the market before the conflict, it increases its share to more than *99%* afterwards. Pre-conflict there was a long tail of CAs issuing certificates, but post-conflict only three CAs effectively participate.

4.2 Revocation Activity

Issued certificates only paint half the story: not only have many CAs stopped issuing new certificates, but some have responded by also fully revoking sanctioned domains. Using the the Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) state as indexed by Censys, we tallied the revocations for certificates securing .ru and .рф domains across all CAs whose validity ended after February 25, 2022.

Table 2 shows the breakdown of domains issued and revoked by the top five CAs with the most revocations. Significantly, both DigiCert and Sectigo have revoked the certificates for all of the sanctioned domains that they issued, apparently choosing to remove any risk of engagement. Although we have no insight into individual CA policy decisions, we note that all CAs have significantly higher revocation rates for sanctioned domains than other `.ru` and .рф domains. We also suspect some revocation activity may be initiated by the sanctioned domains themselves as they navigate the sanctions by testing different CAs.

4.3 Russian Trusted Root CA

The creation of the Russian Trusted Root CA by Russia's Ministry of Digital Development received significant attention when announced. In addition to being a state-run CA, it does not record its issued certificates in the CT logs and is not trusted by major browsers.[12] To evaluate the initial impact of this new Russian CA, we used the Censys Universal Internet Data Set (CUIDS), which performs daily Internet-wide IP scans that index all TLS certificates returned from responding IP addresses.[13] Using these results we identified all TLS certificates containing the Russian CA in their certificate chain, between its inception and May 15, 2022.

The certificate scans show two trends. First, very few sites are offering certificates from the Russian CA: only 170 unique certificates from the Russian CA are seen in the CUIDS data. For context, all other CAs issued more than *800 k* certificates for Russian domains in the same time period. While the metrics are not the same — far more certificates are issued than are in active use — the small number of active certificates from the Russian CA indicates it has yet to have a significant impact on the overall Russian domain ecosystem. Second, as expected, the certificates all secure Russian-related entities, many of which are sanctioned domains. The 170 certificates secure 130 `.ru` and 2 .рф domains while the remainder, in a long tail of other TLDs, are affiliated with Russian sites. Based on the issuance times, the certificates seem to be issued over a period of a few weeks. Of the 170 certificates, 36 secure sanctioned domains (thus accounting for *34%* of the sanctioned domain list).

5 RELATED WORK

The relation between state political interests and Internet communication has become an important field of study, ranging from analyses of global state censorship [8, 25] to the use of blocking, denial-of-service attacks and wholesale closing of Internet access to control opposition forces [3, 10]. Specific to Russia, Moyakine *et al.* [14] explore the 2015 *Yarovaya* counter-terrorism law, which mandated extensive surveillance requirements on Russian telecommunication providers and its impact on the communication of vulnerable groups. Epifanova and Dietrich [4] explore Russia's contemporary goals for "digital sovereignty", both for controlling domestic communication and to reduce dependence on foreign IT services. This goal is evident in empirical studies by Zembruzki *et al.* [26] and Liu *et al.* [12], who analyze the centralization of hosting and e-mail service with a small number of Western providers, but show that Russia bucks this trend with a heavily centralized infrastructure. Ramesh *et al.* [19] analyze the centralized blocking policy dictated by Roskomnadzor to characterize Russian content blocking and the differential experience between residential and business customers.

[12] Russian citizens were instructed to either use a state-approved browser or to configure their browser to accept the new CA.

[13] Since active scans of certificates are likely a subset of issued certificates, the scans represent a lower bound.

6 DISCUSSION

The Russian government has long understood their potential exposure to foreign-operated Internet services. Government efforts to establish a "sovereign Internet" have included a range of regulatory requirements on service providers, including requirements for domestic storage of data on Russian citizens, the use of Russian-controlled DNS root instances, as well as increasing pressure to prefer the use of domestic information and communications technology (ICT) services [4]. Perhaps most inflated is Russia's purportedly-tested capability to disconnect from the global Internet. Thus, even though Russia may have underestimated the magnitude of Western response to its invasion of Ukraine, it is clear that they understood the Internet could be a potential pressure point.

Indeed, we have clear empirical evidence of this pressure, with many thousands of Russian sites losing access to a range of Western service providers, *e.g.*, Netnod for DNS hosting, Sedo for site hosting, and DigiCert and Sectigo for certificate issuance. However, these issues have been far from existential. First, Russia enjoys the benefits from high levels of pre-existing domestic provisioning. The vast majority of Russian sites (≈*70%*) were fully hosted in Russia with entirely domestic name servers long before the start of the conflict.[14] Thus, while we see changes in single digit percentages, when measured against the entirety of the Russian Internet, these are modest effects. Second, for those Russian sites who have made use of non-Russian infrastructure, there are many providers who continue to service Russian customers, both within Russia and without. Thus, while prominent Western providers chose to leave the Russian market, virtually all of the impacted sites quickly found new providers. Moreover, we see little evidence of spontaneous or anticipatory repatriation by Russian domain operators who have not been forced to act.

Finally, we note that certificate issuance represents the one area of significant exposure for Russia. The near-complete control Let's Encrypt holds in securing `.ru` and .рф sites is startling. While Let's Encrypt has a public interest mission that provides free CA service to all comers, it is also a US entity and subject to US law and export control restrictions. Moreover, Russia does not appear to have anticipated this issue by establishing domestic CAs with similar capabilities and, most importantly, established trust relationships with the major browsers.

7 ETHICS

In this paper, we attempt to contextualize changes in underlying infrastructure of `.ru` and .рф domains as a result of push and pull from competing forces (internal and external to Russia) and the vision of "cyber sovereignty". While this type of analysis — identifying trends in infrastructure — does not raise ethical objections, we accept the sensitivities around the conflict and the implications of sanctions on the global Internet may raise concerns. While we recognize these concerns, we believe full transparency is the way ahead.

[14] Our data extends back to 2017, so we cannot establish if this domestic Internet service centralization represents Russia's longer-term state of affairs.

ACKNOWLEDGEMENTS

We thank the anonymous IMC reviewers for their insightful feedback and suggestions. This work was supported in part by the EU H2020 CONCORDIA project (830927), US National Science Foundation grant CNS-1705050, the Irwin Mark and Joan Klein Jacobs Chair in Information and Computer Science at UCSD, and operational support from the UCSD Center for Networked Systems. This research was made possible by OpenINTEL, a joint project of the University of Twente, SURF, SIDN, and NLnet Labs.

REFERENCES

[1] Amazon. 2022. Updates to Amazon's retail, entertainment, and AWS businesses in Russia and Belarus. https://www.aboutamazon.com/news/aws/updates-to-amazons-retail-entertainment-and-aws- businesses-in-russia-and-belarus. *aboutamazon* (March 2022). Accessed: 2022-05.

[2] Censys. 2022. Censys Bulk Data Access. https://censys.io/data.

[3] Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo, and Antonio Pescapé. 2014. Analysis of Country-Wide Internet Outages Caused by Censorship. *IEEE/ACM Transactions on Networking* 22, 6 (dec 2014), 1964–1977.

[4] Alena Epifanova and Philipp Dietrich. 2022. Russia's Quest for Digital Sovereignty: Ambitions, Realities and Its Place in the World. *German Council on Foreign Relations* 1 (2022).

[5] Mykhailo Fedorov. 2022. Letter to Goran Marby, President and CEO of ICANN. https://eump.org/media/2022/Goran-Marby.pdf. Accessed: 2022-06.

[6] GoDaddy. 2022. How GoDaddy is Supporting Ukrainian Customers. https://aboutus.godaddy.net/newsroom/company-news/news-details/2022/How-GoDaddy-is-Supporting-Ukrainian -Customers/default.aspx. Accessed: 2022-05.

[7] UK Government. 2020. The UK Sanctions List. https://www.gov.uk/government/publications/the-uk-sanctions-list. Accessed 2022-04-14.

[8] James Griffiths. 2021. *The great firewall of China: How to build and control an alternative version of the internet.* Bloomsbury Publishing.

[9] IP2Location. n.d. IP2Location IP Address Geolocation Database. https://www.ip2location.com/database/ip2location/. Accessed: 2022-05.

[10] Lukas Kawerau, Nils B. Weidmann, and Alberto Dainotti. 2022. Attack or Block? Repertoires of Digital Censorship in Autocracies. *Journal of Information Technology & Politics* 0, 0 (2022), 1–14. https://doi.org/10.1080/19331681.2022.2037118

[11] Rebecca Klar. 2022. Google Cloud to stop accepting new customers in Russia. https://www.msn.com/en-us/news/politics/google-cloud-to-stop-accepting-new-customers-in-russia/ar-AAUTGK4. *msn* (2022). Accessed: 2022-05.

[12] Enze Liu, Gautam Akiwate, Mattijs Jonker, Ariana Mirian, Stefan Savage, and Geoffrey M. Voelker. 2021. Who's Got Your Mail? Characterizing Mail Service Provider Usage. In *Proceedings of the 21st ACM Internet Measurement Conference (Virtual Event) (IMC '21)*. Association for Computing Machinery, New York, NY, USA, 122–136.

[13] Ron Miller. 2022. Amazon, Microsoft and Google Have Suspended Cloud Sales in Russia. https://techcrunch.com/2022/03/10/amazon-microsoft-and-google-have-suspended-cloud-sales-in-russia. *TechCrunch* (2022). Accessed: 2022-05.

[14] E. Moyakine and A. Tabachnik. 2021. Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived legislation in the age of modern technology. *Computer Law & Security Review* 40 (2021), 105512.

[15] Kevin Murphy. 2022. Now Sedo Pulls the Plug on Russians. https://domainincite.com/27630-now-sedo-pulls-the-plug-on-russians. *Domain Incite* (2022). Accessed: 2022-05.

[16] Yale School of Management. 2022. Almost 1,000 Companies Have Curtailed Operations in Russia — But Some Remain. https://som.yale.edu/story/2022/almost-1000-companies-have -curtailed-operations-russia-some-remain. Accessed: 2022-05.

[17] US Department of Treasury. 2022. 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. Accessed April 14th.

[18] Matthew Prince. 2022. Steps We've Taken Around Cloudflare's Services in Ukraine, Belarus and Russia. https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/. Accessed: 2022-05.

[19] Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. 2020. Decentralized Control: A Case Study of Russia. In *Network and Distributed System Security*. The Internet Society. https://www.ndss-symposium.org/wp-content/uploads/2020/02/23098.pdf

[20] Reuters. 2022. U.S. firm Cogent cutting internet service to Russia. https://www.reuters.com/technology/us-firm-cogent- cutting-internet-service-russia-2022-03-04/. Accessed: 2022-05.

[21] Roland van Rijswijk-Deij, Mattijs Jonker, Anna Sperotto, and Aiko Pras. 2016. A High-Performance, Scalable Infrastructure for Large-Scale Active DNS Measurements. *IEEE journal on selected areas in communications (JSAC)* 34, 6 (June 2016), 1877–1888. https://doi.org/10.1109/JSAC.2016.2558918

[22] RU-Center. 2022. Recommended SSL certificates. https://www.nic.ru/en/catalog/ssl/recommended-ssl. Accessed May 14th.

[23] Julija Tišina, Anastasija Gavriljuk, Venera Petrova, and Nikita Korolev. 2022. Authorities Isolate Networks. https://www.kommersant.ru/doc/5249500. *Kommersant* (2022). Accessed: 2022-05.

[24] Department Of The Treasury. 2022. GENERAL LICENSE NO. 25 Authorizing Transactions Related to Telecommunications and Certain Internet-Based Communications. https://home.treasury.gov/system/files/126/russia_gl25.pdf.

[25] Barney Warf. 2011. Geographies of global Internet censorship. *GeoJournal* 76, 1 (2011), 1–23.

[26] Luciano Zembruzki, Raffaele Sommese, Lisandro Zambenedetti Granville, Arthur Selle Jacobs, Mattijs Jonker, and Giovane C. M. Moura. 2022. Hosting Industry Centralization and Consolidation. In *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 1–9.