Assessing Russia's isolation from the web following their invasion of Ukraine using the DNS root system

George O. Stănculeanu, University of Twente, The Netherlands

ABSTRACT

Censorship of information represents a second nature in authoritarian countries, and this has only extended to the online space, as its significance grew more with the digitalization of the world. A decade full of restrictive laws pre-date current-day Russia, a country that realized the potential of weaponizing information in the most potent medium of data propagation - the Internet. This culminated with 2022's invasion of Ukraine, which was met with strong international backlash but little organized resistance in Russia, due to effective control of the internal narrative and suppression of outside information.

This paper aims to quantify the existence of this isolation effect from a networking perspective, by using requests to DNS root servers and analyzing the path taken by such requests, in order to observe whether significant rerouting occurred after the start of the war. Other factors that might amplify the number of reroutings are path changes due to operators closing service in their country following the war or infrastructure damage. Such changes would signal the existence of network choke points and thus would open the discussion and further study of potential network isolation from the outside world. These are observed for countries in Russia's sphere of influence, as well as Ukraine.

KEYWORDS

Networking, Root server, anycast, BGP, Russo-Ukrainian war, RIPE Atlas

1 INTRODUCTION

The importance of information, together with its free and uncensored flow is monumental and mostly overlooked as a normality, in the modern world. The exception to this rule is represented by authoritarian countries, which are isolating themselves from globally used online services, applications, and websites, to the detriment of their citizens' personal freedoms.

Such is the case of Russia, which has progressively banned news outlets, major social media networks, and even services that seek to anonymize web traffic such as VPNs or the Tor network [2,5,11].

Recent events only point towards a hastening of this isolation effect, such as the implementation of the 'Sovereign internet' law which seeks to create a nationalized DNS [2] or evidence pointing to network congestion, following their invasion of Ukraine [6].All these instances of separation from the online space shared with the rest of the world put in question whether these ramifications can be felt on a network level.

The proposal of one metric that would assess a potential separation is the request to the DNS root servers. Every internet request a person makes for a website must first be resolved, as an address such as "www.google.com" gets translated into an IP address. This is the role of DNS servers, which keep track of all the "translations" of human-readable addresses to IP addresses. With large amounts of data analyzed, less dependence on Russian DNS servers by the outside world could potentially be spotted. This is more likely to be the case in countries such as Ukraine, which have numerous DNS instances themselves where they could reroute traffic, as well as close geographical proximity to more servers in Eastern Europe. The need, in the first place, for a rerouting of requests will be better explained in the Background section but, in short, the routing algorithms do not account for borders of countries but on speed and efficiency.

In the context of the war, these gradual changes are expected to have been amplified, due to fears from Russian authorities that have asked for the removal of the Internet Routing Registry of RIPE, a European entity [19], or from other external factors such as effects of international sanctions.

Moreover, the new development of this conflict that started on 24th February 2022 is likely to bring new details to light regarding network changes. This is due to the infrastructural developments that have connected the region to the rest of the internet in a more efficient way, as compared to 2014 when the conflict started. This is enforced by the Round Trip Time of requests, which is significantly better in current times[1] compared to 8 years ago[2] when the conflict started, despite continuous military interference.

The degree of connectivity to the internet and the reliance on it is evermore increasing, as a bigger percentage of the global population is being coupled to the network. This has also led to major changes in the last 20 years, mainly on the importance of Autonomous Systems (AS). These ASes are in the thousands, as most Internet Service Providers operate at least one [13], in order to provide their services, and thus represent one of the most important parts of global internet infrastructure. There is evidence that most of the Autonomous Systems that were hosted in non-censorious countries 20 years ago have lost significance to ASes in censorious countries, due to traffic changes [8]. This raises the degree of importance of the regional problem of Russian online censorship and centralization, by making it an issue of global interest. The evidence that censorship in Russia has an effect that is 'not limited to its citizens' [8], along with the fact that 'censorious countries control 20.73% of the paths on the Internet'[8] further support this idea.

[1] https://atlas.ripe.net/results/maps/rtt-fixed/?measurement=1001&filter=Russia+(ru)&t=1654954080

[2] https://atlas.ripe.net/results/maps/rtt-fixed/?measurement=1001&filter=Russia+(ru)&t=1402493280

TScIT 37, July 8, 2022, Enschede, The Netherlands

2 PROBLEM STATEMENT

Russia's philosophy on censorship of the online space, along with its effects has been extensively studied in the past [7,12], but their self-isolation has not been quantified before. The unexpected and ongoing nature of military conflict in Europe along with its promptness are other reasons why the scientific literature has not studied this area extensively yet. This paper aims to observe this network isolation effect in the context of the newly initiated war on the 24th of February, by comparing pre-conflict and mid-conflict data provided by the regional Internet registry of Europe called RIPE.

This quantitative study will be done by analyzing requests to the DNS root instances and observing their place of resolution.

2.1 Research Question

The problem statement will be addressed by the following research question:

How did the Russo-Ukrainian war influence regional network centralization, regarding changes observed in DNS root Instance requests pre-conflict and mid-conflict?

These effects can be observed in two ways, from an internal perspective of the requests and by analyzing external traffic that passes through the country. Considering the international sanctions, infrastructure damage, and Russian laws which restrict the flow of data, the following hypotheses are constructed:

H1: A significant part of requests from clients outside Russia that would previously resolve in Russia are now resolved locally or in other neighboring states than Russia.

H2: A significant part of requests from Russian clients that would previously resolve abroad, end up resolving on a Russian DNS instance.

With these hypotheses in mind, the research question can be answered by the following sub-questions:

1. Do probes from Ukraine, or other neighboring countries of Russia end up querying Russian DNS server instances in significantly fewer numbers than before the start of the war?
2. What change can be observed in the number of Russian probes which resolve their requests on Russian DNS instances, on different dates relating to the conflict?

3 RELATED WORK

Scientific research has been conducted on this complex socio-political problem of online isolation from multiple viewpoints. The first one would be represented by the study of how the progressively intrusive Russian legislature has shaped public opinion and the online space. This has led to the centralization of information in the online space, as the state-controlled online entities were exempt from fake-news claims and non-approved sources were less likely to appear on news aggregators [14]. This, along with the banning of major social media websites where the average person could freely express their thoughts [5,11] stimulated self-censorship among residents [17].

After the start of their initial round of sanctions following the initial invasion of Ukraine in 2014, Russia has seen to the militarization of the online space, with new laws and authority groups that incentivize 'nationalization and centralization of threat intelligence reporting and sharing capabilities' [9]. This did not stop at the questionable cybersecurity measures taken by Russia, as foreign owned software was banned by the end of 2018 (especially in governmental use) and existing companies were rushed to transfer all of their user-data on Russian servers and infrastructure [9]. This has led to banning of American giants such as LinkedIn [4], while all other foreign companies strictly revised their infrastructure. In this authoritarian land of constant regulation, the assumption that multiple network connections with the outside world have been severed, due to internal or external pressure, is very probable to be a reality.

Moreover, significant network changes have been observed by researchers in the past. By using a different method, namely traceroute, it was shown that parts of Crimea and Donbas have been 'marginalized from the Ukrainian network', while also not being completely incorporated into the Russian network. [10]. However, this study does not take into account the new developments of the conflict that started in 2022 and they are also looking exclusively at regions which are likely to see change, rather than entire countries. Further studies have looked at the impact after the initial invasion in 2014 on the Crimean Peninsula and they have found major infrastructural changes that have led to dependence on Russian-owned equipment [18].

All these facts have ramifications on the existence of a network isolation phenomenon which is studied in this paper. In regard to the creation of a Russian intranet, separated from the global network, current literature states that the 'dependency on the global internet cannot be repelled fast' [2]. Russian traffic to the outside world also faces significant restrictions due to geo-blocking [3], possibly due to western sanctions.

4 BACKGROUND

Data is originally collected by probes, which send periodic requests and register the results. Probes are small computers, distributed by RIPE NCC all over the world, in order to 'measure Internet connectivity and reachability, providing an unprecedented understanding of the state of the internet in real time' [1]. RIPE NCC, one of the five Regional Internet Registries' [1] of the world makes all of this data public and easily accessed through the Atlas API, which is the main tool used in drawing the conclusions of this study. This represents the most appropriate way of assessing the questions of this quantitative and descriptive research, because of the reliability of the data and its organization. Out of the numerous data points that can be queried from each probe participating in the network, the most relevant in the context of this paper is the DNS root instance of that request. Since DNS represents 'the backbone of the Internet' [15], the efficiency and speed of resolving the request are of the utmost importance. As there are only 13 root servers, named with letters from A to M, their limited number would not suffice all internet requests efficiently. This has been addressed by the introduction of BGP anycast, a system in which multiple servers can share the same IP address, thus making requests more localized, by rerouting them to local instances, an action that reduces overall latency. However, the requests are not always relayed to the most geographically close instance [20], due to the BGP algorithm which always prioritizes the path with the least overall cost. On top of this, operators can add explicit policies for path selection, a fact that complicates the expectancy of relaying a request to a server in close geographical proximity.

5 METHODOLOGY

By analyzing select probes which have been operating both pre-invasion and post-invasion of Ukraine, it can be stated whether a change has taken place. Such a difference can be of importance, in the context of this paper, if it is part of one of the categories:

(1) Observing a centralization of local Russian traffic, meaning that Russian requests to root servers that would previously resolve in an instance located in a different country, will now resolve locally in Russia. This implies that the previous path has increased in cost, and it is not feasible anymore, pointing to a possible network isolation effect on the Russian side.

(2) Observing the opposite of the previous effect, on probes originating from Russia's neighbors such as Ukraine or the Baltic countries. If the cost of paths through Russia has increased because of the invasion's regional effects, traffic that was previously routed to Russian instances of DNS servers should now be resolved elsewhere.

By analyzing many probes, an observed change would be very significant because instance selection through BGP is highly stable [20].

Furthermore, the root servers to which the requests will be initialized need to be of relevance. Changes are more likely to be observed on root servers that have instances present in all the countries of comparison such as roots K and L or F, with presence in Russia and Ukraine. The results shown in this paper are from queries of those three root letters, although similar results have been observed on root letters E and J which also meet the criteria.

For the purposes of reproducing the results of this study, the following data collection and manipulation steps are described:

(1) The probes were initially filtered by country.
(2) The measurements corresponding to the probes have been filtered by the date and type.
(3) Since every request to a DNS root server returns different data depending on the chosen server, parsing has been applied in order to normalize the data.
(4) The country code was appended to each airport code for later separation of data per country.

To further clarify the last two steps, most root letters return the IATA airport code or the IATA code which accounts for all the airports in a city. Using the 'airportsdata' python library, the location code was mapped to its corresponding country. The location of almost all DNS instances can be identified with this method, other than Yandex DNS servers, as their structure does not behave to the aforementioned standard, and they do not disclose their location. As they represent a minority among places of resolution and most of them are located in Russia, they will be discarded from the analysis in order to not add potential confusion.

Having organized the data better, the next step is interpreting and assessing whether Russian probes resolve more on Russian instances and whether Ukrainian probes lessen their dependence on Russia after the start of the war.

In the context of the war, we need to observe changes in a significant number of probes, at dates of interest. With this in mind, three dates were chosen for data analysis:

(1) 01.Feb.2022, an arbitrarily chosen date before the start of the invasion
(2) 01.Apr.2022, a mid-conflict date that can be compared to the first date
(3) 01.Dec.2021, a date that helps towards creating a basis of normality, by comparing it with the first pre-invasion date. The purpose of this date is to better contrast with significant changes seen in the other comparison.

These dates will be used to better visualize country-specific changes in data, with the passing of time. The tool used for these visualizations is a Sankey diagram, which is a diagram used to show the flow of data while maintaining proportionality [16]. If big networking changes are observed for some of the root node requests, they will be further analyzed on a day-by-day basis on a separate graph, in order to observe whether specific dates acted as catalysts.

Given the impartiality of network routing algorithms, an existing isolation effect or a mass of reroutes would have to be observed in neighboring countries not directly affected by the war. With this basis in mind, probes from Finland, the Baltic countries, as well as Asian neighbors of Russia such as Kazakhstan or Mongolia have been analyzed. It was observed that reroutes were more commonplace after the start of the war, implying that pre-war routes are no longer as low cost as before or that certain links have been broken. With this in mind, large scale routing changes are hard to be directly connected to the conflict or to Russia itself, since there are many external factors that could account for these changes. Furthermore, the number of probes from the aforementioned countries that would resolve in Russia is too minimal to be taken into account for further analysis, as most of them have less than 10% reliance on Russian DNS instances, at any given root node. Therefore, we decided to focus only on probes originating from Russia and Ukraine and disregard any other neighboring countries from further analysis.

6 RESULTS

The paper's results are organized from general to more detailed, as some visualizations were not representative enough of the networking effects and needed more study. The results of each subsection are further categorized by the originating country of the probes queried.

6.1 Bi-monthly changes in resolutions

The bi-monthly changes presented in this section are visualized through Sankey diagrams. Each Figure shows the three dates of interest selected in this study, at the top of the imagine and flow that they represent (see Figure 1 for an example). On the flows themselves, the captions are created according to the format XXX-Y-Z, where:

(1) XXX represents the 3 letter IATA code corresponding to the city of resolution
(2) Y represents a counter that separates each city instance from each other by date. For example, since we have 3 dates, they will be represented as XXX-1 for day 1, XXX-2 for day 2 and XXX-3 for day 3.
(3) Z represents the number of probes that had their request resolved in that specific city, at that specific date

6.1.1 Russia

We start by comparing what happens to DNS queries from probes in Russia before and during the conflict.

Figure 1 shows Russian probes querying the K root. Here, an initial stability can be observed in the two pre-war dates, especially regarding the Russian DNS instances LED (representing the Pulkovo Airport in Saint Petersburg), which sees a change from 298 resolutions to 299, MOW (Moscow Metropolitan Airport in Moscow) from 47 to 48, both insignificant. This is not the case when we compare the mid-conflict date with the pre-conflict one, as the Russian instances absorb a good percentage of the traffic that would have resolved in Western Europe. This is significant, especially when it is considered that the Russian DNS instances already represented the majority, with 73.8% of probes resolving on Russian instances, out of the total 470 Russian online probes at all the times of querying. The airport in Saint Petersburg absorbed most of the traffic, including all 37 instances in Italy (PMO), some from Estonia (TLL) and more than half of the ones from the Netherlands (AMS). Now, Russian DNS servers account for 87.6% of total resolution, and they are the only DNS servers that saw an increase in traffic, with all other DNS instances either keeping their traffic or losing it.

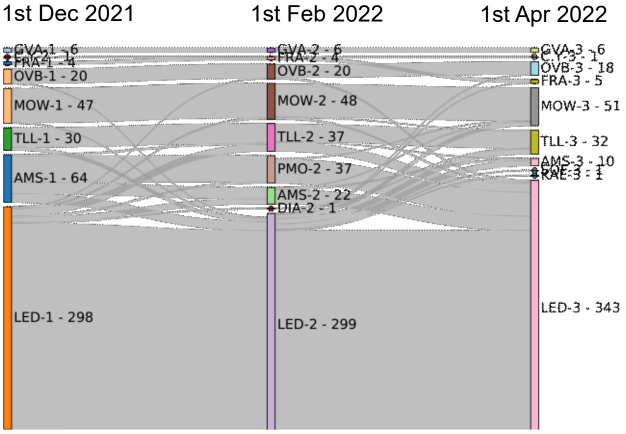

Figure 1. Results after querying K root node on Russian probes

Compared with the K root, L root tells a different story. As it can be seen from Figure 2, root L is characterized by chaotic network changes and less centralization of DNS servers, as more countries are involved in the resolution of requests. Out of all the queried root letters, it is the most similar with one from Western Europe, where close proximity of countries helps towards the decentralization of resolutions and thus improving overall network delay. Most of the unreadable DNS servers present in Figure 2 belong to Yandex, a Russian-based search engine and it is to be noted that they have a significant presence when all are added together, although they will not be further analyzed due to the uncertainty of their geographical location which they do not disclose (even though known that the majority of them are Russian). Now, Russian instances still represent a majority with 49.4% of total probes pre-war and their increase mid-conflict is only marginal, reaching an absolute majority at 51.3%. Outside of this slight increase, what is interesting about the L root in particular is the introduction of Belarus, with its GME instance in the Gomel District. The Belarusian instance takes the entire traffic of the Odessa airport after the start of the war, leaving Odessa with only 1 resolution out of the total of 80, which is a drastic change. It is to be noted that the stability of this node is undeniable before the start of the Russian invasion on the 24th of February, as it can be seen from the comparison of the 1st of December 2021 and 1st of February 2022 dates. Although uncertain without ground truth, this change is likely due to infrastructural damage, considering Odessa was one of the first location under heavy bombing. Proximity wise, this makes sense, as the Gomel District in Belarus is the closest to the eastern front of Russia and makes for a great replacement to the Odessa DNS instance, although if we consider that Belarus is the most obedient country in the sphere of influence of Moscow, the idea of a centralization of regional traffic still stands.

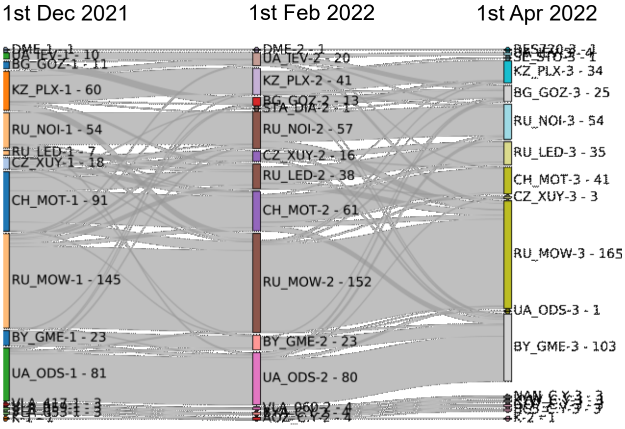

Figure 2. Results after querying L root node on Russian probes

6.1.2 Ukraine

It can be observed from Figure 3 that Ukrainian probes are fewer and thus slight changes are more proportionally significant. At first glance, the Russian presence diminishes post-war with both airports DME and SVO losing resolutions, but this does not seem relevant, especially when compared with the baseline date of December 1st, 2021. With this date considered as well, it can be seen that it is rather a fluctuation rather than an overall decrease. This root node is characterized by unpredictable changes, which will need further studying.

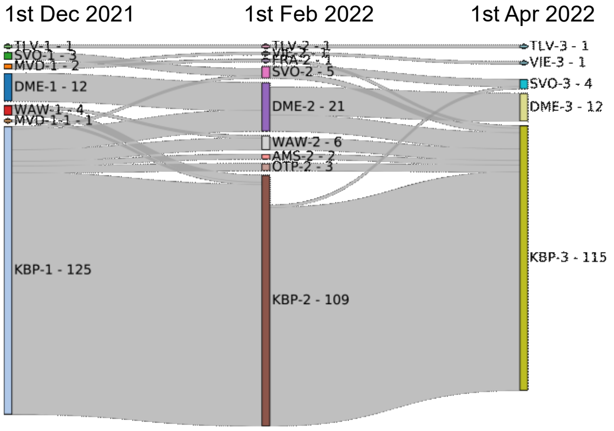

Figure 3. Results after querying F root node on Ukrainian Probes

Overall results are worth further analysis and initially point towards more resolution on local DNS instances in Russia after the start of the war, as well as a questionable diminishment of Ukrainian reliance on Russia. As the 3 selected dates only present the broad, generalized situation, more dates are needed for further understanding.

6.2 Day-by-day changes in resolutions

In order to visualize daily changes in the number of resolutions, new graphs were devised that take into account daily changes in the number of instances that resolve in Russia or Belarus. This is represented on the y axis, by the percentage of total probes of that day. Also, the interval of study was broadened, by adding dates up until mid-May, as opposed to the previous analysis that stopped in April. A shading of portions of the graph was added, in order to better differentiate between pre and mid conflict dates.

6.2.1 Russia

As previously discussed, the Belarussian DNS server had more influence on the results of the L root and, implicitly, the incapacitation of the Ukrainian node at Odessa made the biggest jump in local dependence on a date that corresponds with the start of the war. This can be seen in Figure 4 at the start of the shaded area of the graph. The increase from 53% to 70% overnight is definitely significant, as it does not compare with other fluctuations of the graph. This trend continues upwards to 75% on the 1st of April, but seems to level down after it, although still higher than pre-invasion.

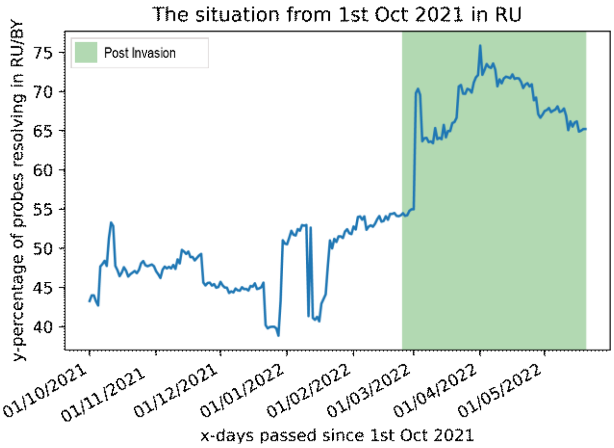

Figure 4. Percentage of Russian probes that resolve on Russian instances by day - L node

6.2.2 Ukraine

By further analyzing the situation in Ukraine for the F root, Figure 5 shows that the date that corresponds to the start of the invasion represented a catalyst, that diminished the reliance on Russian Instances by almost half (from 13% to 8%), which also corresponds with the lowest point overall. Although it bounced back in the following month, until 1st April 2022, it seems permanently affected now and, on the downtrend, without significant fluctuations that can be seen all the way from the beginning of the graph to the start of the invasion. Compared to the Russian instances that showed clear trends already from the Sankey Diagrams, similar trends have been observed for the Ukrainian probes only after introducing more data.

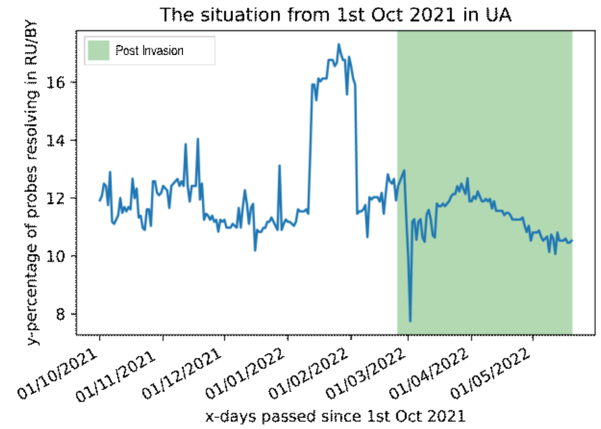

Figure 5. Percentage of Ukrainian probes that resolve on Russian instances by day – F root

Together with the Russian instances seen in Figure 4, by adding the Ukrainian instances of the same root letter (L), a relation of inverse-proportionality can be observed by comparing the results of Figure 4 and Figure 6. This is not necessarily implied directly by the changes to the Odessa DNS server, as both Ukraine and Russia have more DNS servers that could contribute to a result change, such as RU_NOI, UA_IEV, RU_LED and RU_MOW. We can observe that Ukraine had a lot of reliance on the DNS servers in the Russian sphere of influence (lowest 16%, highest 35%), but it stabilized for most pre-war months for a reliance between 30% and 35%. This makes the drop from the date of the invasion all the more significant, as it dropped from 35% to sub 10%, and never seemed to recover to a pre-war level.

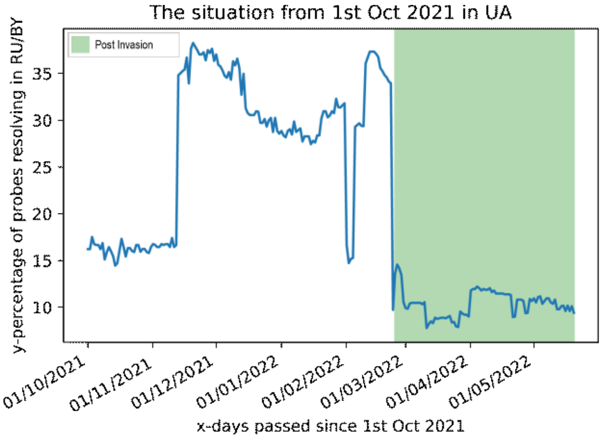

Figure 6. Percentage of Ukrainian probes that resolve on Russian instances by day - L node

The results shown in this paper for nodes K, L and F seem consistent with the overall network changes observed in the other analyzed roots, thus accounting for all DNS root instances that are present in both countries. Exceptions to the rule can be seen in the J root, which does not present any significant differences, as a leveling off effect can be seen on the Ukrainian instances and a slight decrease on the Russian ones. This was to be expected, as requests to J node are already very centralized (over 90% of Russian probes resolving in Russia), as well as the least amount of reliance by the Ukrainian probes (around 10% or less across the entire 6-month period of analysis).

7 LIMITATIONS

The first set of limitations would relate to the number of data points. The Atlas API helps researchers see correlations and anomalies about overall connectivity of countries and regions like no other, but definitive conclusions are harder to be drawn. Moreover, it is hard to assess that the 605 active Russian probes and 198 Ukrainian ones are representative of the whole situation of their respective countries or whether more data is needed. Considering that 16% of probes went inactive in Ukraine in only 4 days after the start of the war, bringing the number from 222 to 186, the war effects represent another variable that can skew the results of this study. This is important, in the context of this study, as only probes that were online during all the querying dates will count towards the result, thus making regions truly affected by the war less likely to appear in the results.

8 FUTURE WORK

As DNS analysis of measurements have been the main focus of this paper, future work could add traceroute analysis, which could provide more precision to the changed paths, before reaching a root node. This has the potential to identify more network wide reroutes, around potential war-damaged infrastructure. This is not addressed in this paper, as only the final DNS server of resolution is provided by the DNS measurements. With this considered, traceroute measurements present difficulties in the analysis stage, especially in the context of the Atlas API, as the traceroute responses require thorough breakdown of the data, which proves hard to do systematically for thousands of measurements.

As this analysis has been done at a time of ongoing military conflict, another future study could look at whether these observed effects will diminish over time and arrive to pre-war states after the end of the conflict or whether they are permanent

9 CONCLUSION

We have observed significant shifts in the number of DNS resolutions after the start of the 2022 Russian invasion of Ukraine which point to the isolation of Russia from a network perspective. This was analyzed from both the Russian perspective, as we saw the increases of resolutions on Russian DNS servers, and also from the Ukrainian perspective, as we observed a sharp decrease in the number of probes that resolve in Russia after the start of the invasion. Due to small dependence on the Russian DNS nodes by neighboring countries, a decrease in the entire region could not be spotted or was too marginal. However, after considering that the network effects observed in this paper could be the result of a multitude of external factors, it becomes hard for them to be linked with the effects of the war without knowing the ground truth. One of such factors could be the application of local legislature (as was the case of Russia with their supposed application of the 'Sovereign Internet' law in 2022), or operator mandated re-routes. With all of these cautions in mind, the results of this study do point to the war as the main catalyst for the changes, but further study would be needed to conclude this with certainty.

REFERENCES

[1] 2016. RIPE Atlas Probes and Anchors. Retrieved from https://www.internetsociety.org/resources/doc/2016/ripe-atlas-probes-and-anchors/

[2] Alexander Isavnin. 2022. The Russian Sovereign Internet and Number Resources. *RIPE Labs*. Retrieved from https://labs.ripe.net/author/alexander-isavnin/the-russian-sovereign-internet-and-number-resources/

[3] Allison McDonald, Matthew Bernhard, Luke Valenta, Benjamin VanderSloot, Will Scott, Nick Sullivan, J. Alex Halderman, and Roya Ensafi. 2018. 403 Forbidden. *Proceedings of the Internet Measurement Conference 2018* (2018). https://doi.org/10.1145/3278532.3278552

[4] Andrey Rumyantsev. 2017. Russia: Information Security Doctrine, Stricter Regulations Against "Fake News" and Blocking LinkedIn. *Computer Law Review International* 18, 1 (2017). DOI:https://doi.org/10.9785/cri-2017-0108

[5] Anna Shirokanova and Olga Silyutina. 2018. Internet Regulation Media Coverage in Russia: Topics and Countries. In *Proceedings of the 10th ACM Conference on Web Science* (*WebSci '18*). Association for Computing Machinery, New York, NY, USA, 359–363. https://doi.org/10.1145/3201064.3201102

[6] Emile Aben. 2022. How Is Russia Connected To The Wider Internet? RIPE Labs. Retrieved from https://labs.ripe.net/author/emileaben/how-is-russia-connected-to-the-wider-internet/

[7] Eva Claessen. 2020. Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU. *Journal of Cyber Policy* 5, 1 (2020), 140-157. DOI: https://doi.org/10.1080/23738871.2020.1728356

[8] H. B. Acharya, Sambuddho Chakravarty, and Devashish Gosain. 2017. Few Throats to Choke: On the Current Structure of the Internet. *2017 IEEE 42nd Conference on Local Computer Networks (LCN)* (2017). DOI:https://doi.org/10.1109/lcn.2017.78

[9] Ilona Stadnik. 2019. Internet Governance in Russia – Sovereign Basics for Independent Runet. *TPRC47: The 47th Research Conference on Communication, Information and Internet Policy 2019* . DOI:https://doi.org/10.2139/ssrn.3421984

[10] Kevin Limonier, Frédérick Douzet, Louis Pétiniaud, Loqman Salamatian, and Kave Salamatian. 2021. Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine. *First Monday* (2021). DOI:https://doi.org/10.5210/fm.v26i5.11700

[11] Ksenia Ermoshina and Francesca Musiani. 2021. The Telegram ban: How censorship "made in Russia" faces a global Internet. *HAL*. Retrieved from https://hal.archives-ouvertes.fr/hal-03215281/document

[12] Ksenia Ermoshina, Benjamin Loveluck, and Francesca Musiani. 2021. A market of black boxes: The political economy of Internet surveillance and censorship in Russia. *Journal of Information Technology & Politics 19*, 18-33. DOI: https://doi.org/10.1080/19331681.2021.1905972

[13] M. Caesar and J. Rexford. 2005. BPG routing policies in ISP networks. *IEEE Network* 19, 6 (2005), 5-11. DOI:https://doi.org/10.1109/mnet.2005.1541715

[14] Mariëlle Wijermars. 2021. Russia's law 'On news aggregators': Control the news feed, control the news?

Journalism 22, 2938-2954. DOI:https://doi.org/10.1177/1464884921990917

[15] Mouhammd Al-kasassbeh and Tariq Khairallah. 2019. Winning tactics with DNS tunnelling. *Network Security* 2019, 12 (2019), 12-19. DOI: https://doi.org/10.1016/s1353-4858(19)30144-8

[16] Radar Chart - A Complete Guide | FusionCharts. Retrieved June 22, 2022 from https://www.fusioncharts.com/resources/chart-primers/radar-chart

[17] Rashid Gabdulhakov. 2020. (Con)trolling the Web: Social Media User Arrests, State-Supported Vigilantism and Citizen Counter-Forces in Russia. *Global Crime 21*, 283-305. DOI:https://doi.org/10.1080/17440572.2020.1719836

[18] Romain Fontugne, Ksenia Ermoshina, and Emile Aben. The Internet in Crimea: a Case Study on Routing Interregnum. *2020 IFIP Networking Conference (Networking)* 2020 , 809-814.

[19] Stephane Bortzmeyer. 2022. Internet Network Shutdowns in Russia *RIPE Labs*. Retrieved from https://labs.ripe.net/author/stephane_bortzmeyer/internet-network-shutdowns-in-russia/

[20] Ziqian Liu, Bradley Huffaker, Marina Fomenkov, Nevil Brownlee, and Kc Claffy. Two Days in the Life of the DNS Anycast Root Servers. *Lecture Notes in Computer Science* 4432, 125-134. DOI: https://doi.org/10.1007/978-3-540-71617-4_13