The effect of the Russian-Ukrainian conflict from the perspective of Internet eXchanges

Cristian Trusin, c.trusin@student.utwente.nl, University of Twente, The Netherlands

The 2022 Russian-Ukrainian conflict affected the Internet in these two countries. Ukraine is facing outages because of the damage to the infrastructure, Russia is being boycotted by the international community. In this paper we quantified the degree to which the Internet was affected in both countries by analyzing routing tables from several Internet Exchange Points (IXPs). IXPs provide a central point of interconnection where internet traffic can be freely exchanged between Autonomous Systems (ASes). This centrality makes IXPs a good vantage point for analyzing changes in the Internet. With data collected before and after the start of the war we observed considerable damage to the Ukrainian Internet network with numerous outages and no damage to the Russian network. An average of 10% of Ukrainian ASes are now unreachable at each IXP. We identified the biggest outages and the events responsible for them and offer a discussion regarding these results.

1 INTRODUCTION

On 24th of February 2022 Russia invaded Ukraine. The invasion affected the Internet traffic in the two countries. Ukraine has been experiencing blackouts as parts of its infrastructure have been cut off after bombing [9]. Russia has been boycotted by the international community and businesses. Sanctions were registered since 24th of February 2022 and are still ongoing [1]. Major transit providers like Cogent and Lumen, stopped selling Internet access to Internet Service Providers (ISPs) inside Russia [1, 17]. Furthermore, content providers like TikTok and Netflix have ceased their services in the country [18]. These events have had an impact on the Internet in both countries, some services are unreachable or are forced to be routed through a slower path, but it remains unclear how big this impact was.

We will investigate this using data from Internet Exchange Points (IXPs). IXPs are a crucial element of today's internet [4], they provide direct peering opportunities between Autonomous Systems (ASes). Direct peering is a voluntary interconnection of two separate networks with the purpose of directly exchanging the traffic between the users of those networks, it improves latency and decreases interconnection costs. Since IXPs connect many ASes, they are a rich source for networking research [4], and are suitable to analyze changes in the network, thus they can help us quantify the effects of the war on the Internet in Ukraine and Russia.

To do so we will be analyzing Border Gateway Protocol (BGP) data from the routing tables provided by the following IXPs: AMSIX, LINX, SIX, AUIX, SPOIXBR. We will analyze the period between 19th of February 2022 and 29th of April 2022. This provides a reference point of the situation before the war.

Our goal is to quantify the effect that the war had on the Russian and Ukrainian networks from the perspective of the IXPs.

To achieve this goal, we have defined the following research questions (RQs) as a basis for our research:

- **RQ1:** How many Russian and Ukrainian ASes became unreachable?
- **RQ2:** For how long were these ASes unreachable?
- **RQ3:** What were the biggest outages and what events are responsible for them?

This paper will be structured as follows: Section 2 will discuss the necessary background information and the related work. Section 3 will talk about the methodology we will use to answer the Research Questions. Section 4 will discuss the results for Ukraine and Russia, and offer a discussion about these results. In Section 5 we conclude our work and discuss possibilities for future work.

2 BACKGROUND

The Internet is a network of networks, it can be broken into smaller networks called Autonomous Systems (ASes). Each AS is a group of routers that belong to the same organization. For example, to ISPs, universities, tech companies, governments etc. Each AS wishing to connect to the Internet and exchange routing information must have a valid AS Number (ASN) assigned by the Internet Assigned Numbers Authority.

ASes communicate with each other using the Border Gateway Protocol (BGP). BGP provides a standardized way of sharing routing information between ASes, it is the glue that connects all the Autonomous Systems together. At its essence, BGP is trying to connect the whole Internet together by letting ASes share their routing data. Then from this routing data, it selects the best path to a destination based on an attribute called *as_path*. The *as_path* is a sequence of ASNs that a packet will follow to reach the destination. BGP chooses the shortest *as_paths*. The details of this process are not important for this paper, but more information can be found in Sam Halabi's book [19].

For an AS to interconnect with another AS they need to establish a peering session. One way of doing this is to trace a cable between the border routers of both ASes. However, this approach introduces a lot of complexity and scalability problems. Instead, they can choose to connect to an IXP, which is a central point of interconnection for ASes, where they can freely exchange traffic with other members of the IXP. This is achieved by a Route Server. A Route Server is a construct in an IXP which has information about the routes offered by other member ASes. By connecting to a Route Server, you can establish connection to multiple ASes by using a single BGP session, this enables one-to-many peerings instead of traditional one-to-one peerings [14], which improves scalability and makes routing much easier. By connecting to only

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

10 IXPs you can reach 56% of all ASes on the Internet [2], which makes them a good source of insight to answer our research questions. A good high-level introduction to IXPs can be found in Gerson's et al. [7] paper, a more detailed dive into IXPs can be found in [4].

3 METHODOLOGY

In this section we will explain how we performed our research. We quantified the outages and changes in the network by performing Data Analysis on selected BGP attributes from our collected dataset. We will start by explaining what this dataset is and how it was collected, and then dive into our implementation. The code for this implementation as well as a Database required for it is provided here [5].

3.1 Datasets and IXP Selection

Since 13th of February 2021 and until 29th of April 2022, the routing tables from AMSIX, LINX, SIX, AUIX, SPOIXBR have been collected daily through a Looking Glass, as part of the research conducted by Bertholdo et al. [2]. A Looking Glass allows an IXP to share information from the Route Server.

The 5 IXPs listed above were chosen due to their size and representativeness [2, 10]. AMSIX (Amsterdam Internet Exchange) and LINX (London Internet Exchange) are in Europe, close to the conflict. LINX is particularly interesting since they reported sanctions against Russia [3]. AMSIX is the second biggest IXP in Europe after DECIX (Deutsche Commercial Internet Exchange). We found some gaps in the DECIX dataset during war days, so it was not possible to include it in our analysis. We also included other IXPs outside Europe to verify if problems were observed on other continents. SIX (Seattle Internet Exchange) and AUIX (Australia Internet Exchange) were used to represent North America and Australia in this research. And finally for South America we had data from SPOIXBR (San Paolo Internet Exchange Brazil). We had no data from African IXPs but since they are relatively young and small, we would have probably had few Russian and Ukrainian routes. Analyzing this hypothesis is left for future work.

The gathered routing tables are in a .csv format and represent BGP data. We have a routing table for every single day and for each IXP. So, for any given day we have 5 routing tables to analyze since we have 5 IXPs. We will focus on the *as_origin*, *as_neighbor* and *as_path* attributes of the routing tables. *as_origin* denotes the AS that can be reached from this IXP. It is an ASN. If this AS cannot be reached anymore, its *as_origin* will disappear from the routing table. One *as_origin* can route traffic to multiple prefixes. *as_neighbor* from the perspective of an IXP denotes the ASN of the AS that is directly connected to the IXP. *as_path* denotes all the ASes the *as_origin* had to transit through to reach the IXP. *as_path* is a list of ASNs, the last entry in the list is always the *as_origin*. We will use these attributes to analyze if and how routes to Ukrainian and Russian ASes have changed.

We know for a fact that certain ASes experienced outages because of the war [9, 18]. Moreover, the routing paths to some Russian ASes have changed [17]. To quantify these, we needed a baseline. We analyzed several days of data before the war as can be seen in Figure 1, and concluded that except for 2 outages in October and December 2021, the data showed little variation, so we chose 19th of February 2022 to serve as our baseline. The last datapoint we have is on 29th of April (*End* label in Figure 1).

3.2 Implementation

The first phase of the research was identifying which ASNs belong to Russia and Ukraine. We did this by creating a database where we aggregated statistics data from Regional Internet Registries (RIRs). These statistics offer data about the current allocations and assignments of Internet Number Resources (Ips and ASNs). We used the data from all 5 RIRs: AFRINIC, APNIC, ARIN, LANIC and RIPE NCC. These statistics come in a specially formatted .csv file, one for each RIR. The full format can be found here [15]. We filtered this data to contain ASN assignments only, and for each ASN we kept the country to which it belongs. The data from each RIR was later aggregated together, resulting in a big Database that can identify the originating country of a given ASN. The Database was exported as .csv for easy use between working sessions. From now on we will refer to this Database as ASNDB (ASN Database). ASNDB allows us to filter our routing tables and isolate Ukrainian and Russian routes.

3.2.1 *Counting the number of unreachable ASes (RQ1)*

To answer RQ1 we needed to count the number of ASes which became unreachable at any point after the start of the war. We joined ASNDB with our routing tables, resulting in a table where for each route we also have its originating country code as a new column. By filtering on this new column, we were able to find the Ukrainian and Russian *as_origins* for each IXP. By analyzing our baseline and looking at our last datapoint, we identified which and how many *as_origins* became unreachable after the start of the war for each IXP. This was achieved by selecting all distinct prewar *as_origins* and searching for those *as_origins* in the last routing table we have collected. If an *as_origin* was not found it was pronounced unreachable. It could be that a temporary outage was happening during the collection of our last datapoint, making some *as_origins* temporarily unreachable. To avoid drawing false conclusions we also checked if they were unreachable during the 3 days before the collection of our last datapoint. The results did not show any significant differences, and this concludes our approach for answering RQ1.

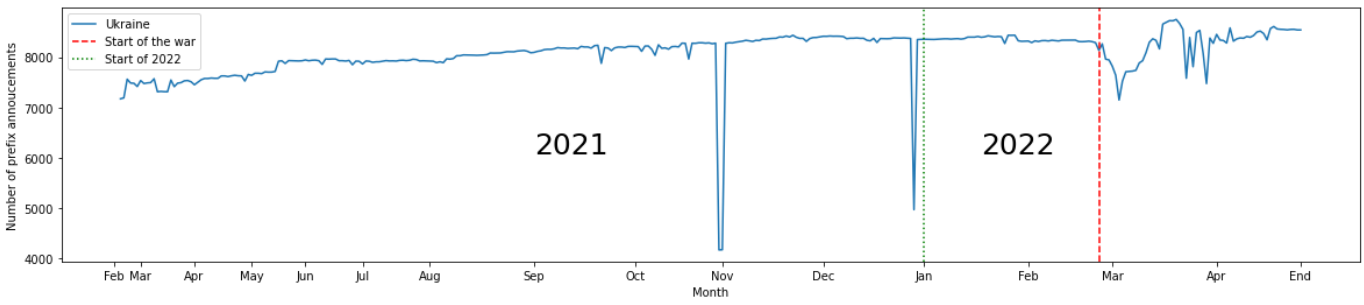

Figure 1 Number of Ukrainian Prefix announcements before the start of the war

3.2.2 *Counting the number of days ASes were unreachable (RQ2)*

To answer RQ2 we had to count the number of days when an ASN was unreachable. We used an approach similar to RQ1. Using the same baseline, we made a list of all distinct Ukrainian and Russian *as_origins* for each IXP. Then we iterated over the data for every day after our baseline and checked if an *as_origin* is no longer reachable. If it was not, we counted that day as an offline day for this *as_origin*. The result of this operation was a data structure where for each ASN we had the number of offline days as a value. This data proved to be hard to visualize due to the sheer amount of *as_origins* and the variation in the number of days they were offline for, so we opted for a different approach later in the research.

We decided to focus on the *as_neighbors*. An *as_neighbor*, in the context of an IXP, is the ASN of the AS which is directly connected to the IXP. We made this decision because if one of these ASes were to disconnect, all the prefixes it provided routing information for will also be disconnected, thus making them unreachable for this IXP and the member ASes of this IXP. This is indicative of an outage at the said AS, since the consequences of disconnecting are very undesirable. If an ISP were to disconnect from an IXP, all its clients would lose access to fast routes connecting them to the global internet. Bearing this in mind, we counted the number of distinct *as_neighbors* for each day at every IXP.

3.2.3 *Identifying the outages and the responsible events (RQ3)*

To answer RQ3 we needed to find when these outages happened. We can use the plot from RQ2 for this purpose, but it only offers a high-level view of the situation. It could be that the *as_neighbor* has not disconnected from the IXP, but it has fever prefixes to route to because of the damage to the infrastructure.

To assess this, we calculated the number of Ukrainian and Russian prefix announcements, alongside the number of distinct Ukrainian and Russian *as_origins* for every day per each IXP. This again was achieved by joining the ASNDB with the routing tables and filtering on routes originating from the two countries, the Ukrainian and Russian routes were saved to separate files for later analysis. We plotted this data to see where we can find dips in the plot that signify an outage. Having found a dip we would look at the news coverage for that day alongside the report from NetBlocks [9] to find events that are responsible for the outage.

4 RESULTS AND DISCUSSION

In this section we show and discuss our findings. Since there is little overlap between the situation of Ukrainian and Russian Networks, we split it into 2 subsections: one discussing our results regarding Ukraine and another regarding Russia. The plots used, show data since 19th of February since we chose this as our baseline of the prewar situation. The datapoints before this day showed little variation as discussed in Section 3.1, so they were cut off from the resulting plot.

4.1 Mapping outages in Ukraine

The Ukrainian network took considerable damage since the start of the war. Table 1 provides information about the number of unreachable Ukrainian ASes at each IXP. On average every single IXP lost 10% of Ukrainian ASes since the war started. The European IXPs were the most affected of all.

Table 1 Number of Unreachable Ukrainian *as_origins*

IXP	Total ASes	Lost ASes	% Lost
AUIX	1016	87	8.5%
LINX	1335	254	19.0%
AMSIX	1571	164	10.4%
SPOIXBR	1021	92	9.0%
SIX	1096	96	8.7%

4.1.1 *Europe*

AMSIX experienced the most variation in available Ukrainian connections. Each *as_neighbor* provides routes to many *as_origins*, the loss of one of them is significant. At AMSIX, a Ukrainian *as_neighbor* provides routes to an average of 400 Prefixes which is around 409.600 IP Addresses. As we can see in the historical graph in Figure 2, most of these ASes experienced an outage for a day, however some (AS 25133 – McLaut-Invest) were gone for 50 days, and some never reconnected (AS 12963 – Volz). A peculiar finding is Omegatelecom (AS 199995) which is a new member of AMSIX coming from Ukraine. It connected on April 9th and is responsible for providing routes to 243 distinct Ukrainian prefixes and 90.264 IP addresses. LINX has not experienced any significant loss of *as_neighbors*. The only disconnection happened on 28th until 29th of March during Event ③ in which LINX lost its only Ukrainian *as_neighbor* which provided routes to many Ukrainian prefixes. This is explained by a cyberattack on Ukrtelecom's core infrastructure as reported by BBC [20] and is also responsible for the decrease in Prefix Announcements during that time.

As can be seen in Figure 3 there are significant variations in the number of prefix announcements at AMSIX and LINX since the start of the war. Event ① shows a significant loss of connectivity, around 1000 less prefixes were announced that day. This can be attributed to a major blackout in the region of Sumy, which is

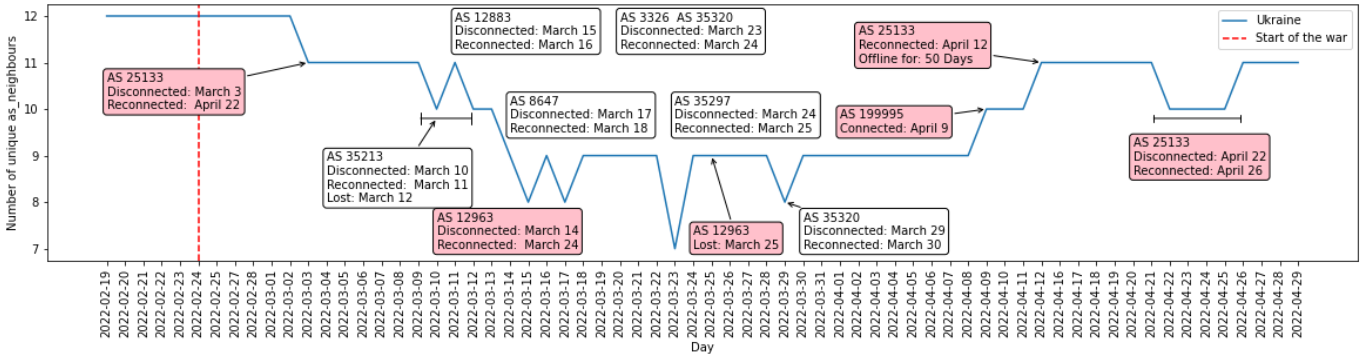

Figure 2 Number of Ukrainian *as_neighbors* at AMSIX

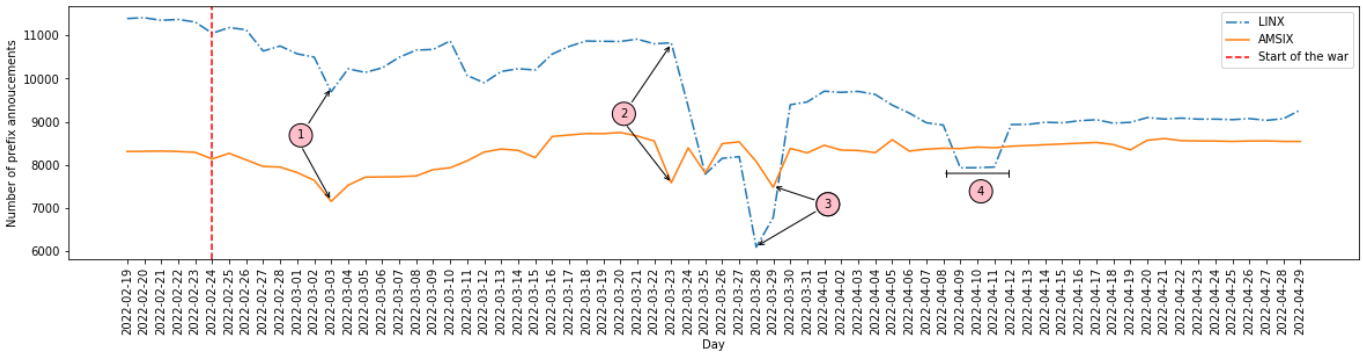

Figure 3 Number of Ukrainian Prefix announcements at AMSIX and LINX

reported as the largest disruption to Telcom services since the start of the war [12]. As a result of bombing at the local thermal power plant, the region of Sumy experienced a large blackout which also affected Internet Connectivity. Connectivity started to improve over the course of the next days, and 10 days later new Prefix Announcements were observed, even more than before the war.

Other major disruptions can be seen at Event ② and Event ③. We could not identify a concrete event responsible for the former, but the latter can be attributed to the cyberattack on Ukrtelecom's core infrastructure mentioned above [13]. Overall Ukrainian prefixes at AMSIX seem to have rebound to prewar levels since April.

However, LINX does not show such a rebound. It sustained the biggest Ukrainian losses, registering a total of 254 out of 1335 ASes. A share of 19% of all Ukrainian networks were disconnected from this IXP. Figure 3 shows that LINX has been experiencing a gradual decline in Ukrainian connections since the beginning of the war. Besides experiencing the same outages as AMSIX, LINX also had a loss of connectivity during Event ④, an emergency was reported by the operator WNET which impacted Ukraine's international connectivity during that period [11].

4.1.2 *Other continents*

Figure 4 shows the data analyzed for SIX (USA), AUIX (Australia) and SPOIXBR (Brazil). These IXPs follow a similar pattern to Europe, with a significant loss of connectivity at Event ①, due to the Sumy Blackout [12] and cyberattacks at Event ② and Event ③ [13]. Another dip in connections can be seen during Event ⑤. This can possibly be explained by a global Internet Disruption in mid-March, where the number of Internet outages increased by 22% [8]. None of these IXPs have Ukrainian *as_neighbors*, thus none of them were lost during the war.

4.1.3 *Observations and Discussion*

Ukraine has sustained damage to its networks since the start of the war, and average of 10% of Ukrainian ASes are now unreachable. We have found 5 outages: Event ① - The Sumy Oblast Blackout, Event ② - Unidentified Outage, Event ③ - Ukrtelecom Cyberattack, Event ④ - WNET International Connectivity emergency, Event ⑤ - March Global Internet Disruption. The first three of these can be observed both in and outside Europe. Event ④ is exclusive to LINX, and Event ⑤ is exclusive to IXPs outside Europe. Except for LINX, the number of Ukrainian connections at IXPs has started recovering and the number of outages has decreased significantly since April.

LINX had the biggest losses, we observed a decrease of 19% in the number of reachable Ukrainian *as_origins*. Judging by the fact that Event ③ marks the biggest outage for LINX with a loss of 2000 Prefix Announcements, and that LINX temporarily lost its only Ukrainian as_neighbor during that event, we can assume that these losses are attributed to the disconnection of that neighbor. This as_neighbor provided routes to most Ukrainian Prefixes at LINX and because of the war, it likely lost connection to a lot of ASes, so it could no longer provide routes to those ASes for LINX.

AMSIX has 12 Ukrainian *as_neighbors* which provided more redundancy. If one neighbor lost connection to some ASes, another one might still have a way to reach them, which explains why AMSIX restored most connections. The reason why LINX did not lose all Ukrainian routes due to the disconnection of the said *as_neighbor*, is because neighboring countries kept providing alternative routes to some Ukrainian ASes.

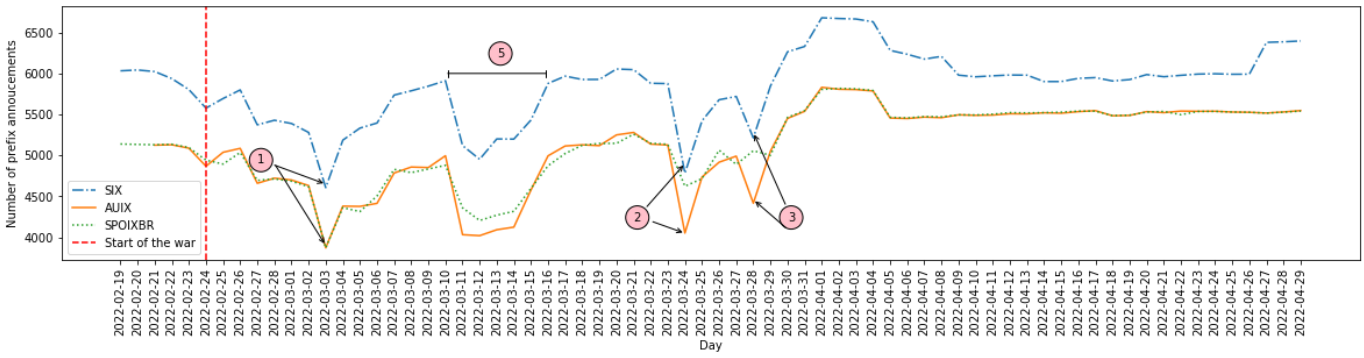

Figure 4 Number of Ukrainian Prefix announcements at SIX, AUIX and SPOIXBR

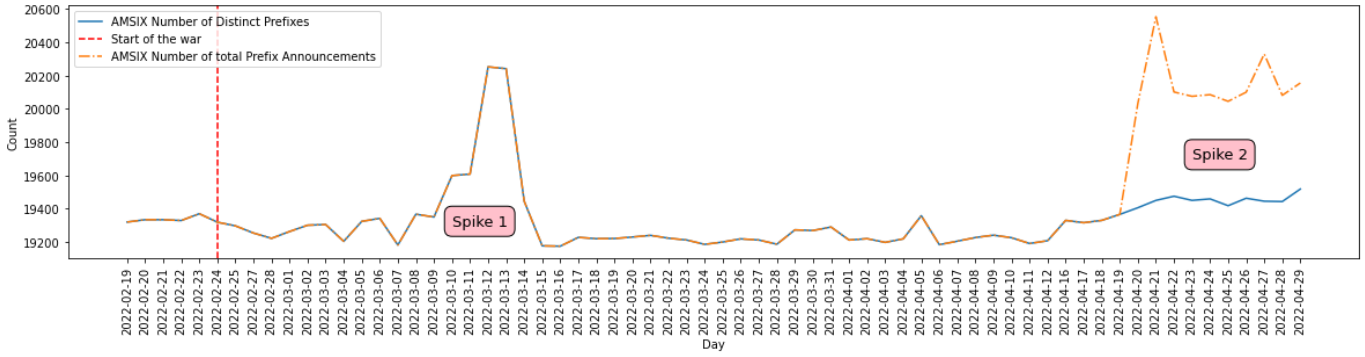

Figure 5 Number of Russian Connections at AMSIX

4.2 The effects of the boycott on Russia's connectivity to IXPs

Russia was heavily boycotted for their invasion by most countries in the world [1]. There have been threats that Russia will be cut off from the Global Internet. Moreover, major Internet Transit Providers like Cogent and Lumen have stopped offering Russia their services [1,17]. In this section we analyze how the Russian network was affected at the IXPs.

Table 2 provides information about the number of Russian ASes that lost access to the IXP since the start the of the war. An average of 10.94% ASes were lost. However, new ASes have connected during that same period, thus increasing the total number of Russian *as_origins* and Prefixes since the start of the war.

Table 2 Number of Unreachable Russian *as_origins*

IXP	Total ASes	Lost ASes	% Lost
AMSIX	3749	117	3.1%
LINX	2886	109	3.7%
SIX	421	62	14.7%
AUIX	415	78	18.7%
SPOIXBR	419	61	14.5%

4.2.1 Europe

As can be seen in Figure 5, AMSIX shows no decrease in Russian Prefixes Announcements and the number of distinct Prefixes. A sudden increase in Prefix Announcements was observed for 6 days (Fig. 5 Spike 1). We analyzed the number of distinct Russian Prefixes at AMSIX for this time and found an increase of about 800 Prefixes during this period. Another such spike can be seen (Fig. 5 Spike 2), however this time it was only followed by an increase of 200 distinct Prefixes, and it is still ongoing. There was no variation in the number of Russian *as_neighbors* at AMSIX.

LINX tells a similar story to AMSIX, there was no decrease in the number of Russian routes and *as_neighbors*. As can be seen in Figure 6, an increase of distinct Prefixes was observed from 15th of April. These findings are peculiar since LINX was one of the few IXPs that announced sanctions against Russia, and one would expect the number of Russian connections to decrease. After further investigation we found that LINX only disconnected two Russian ASes: Rostelecom (AS 12389) and Megafon (AS 31133) [3]. These ASes are Russia's biggest ISPs, but apparently, they had little to no traffic at LINX and were planning on abandoning LINX services themselves [16].

4.2.2 Other continents

Figure 7 shows the data for SIX, AUIX and SPOIXBR. They all show that Russia experienced an outage on 12th until 14th of March (Fig. 7 Outage 1), which is consistent with the outage observed at these IXPs for Ukraine (Fig 4 Event ⑤) in the same period. It is also explained by the mid-March global Internet Disruptions [8]. Another serious outage was observed on 31st of March (Fig. 7 Outage 2). SIX and AUIX had no Russian *as_neighbors* prewar, and the situation remained unchanged. SPOIXBR had one Russian *as_neighbor* and besides a small 1-day outage on 2nd of March it remained stable. These IXPs also show an increase in Russian prefixes in April, as well as an increase in distinct *as_origins* since the start of the war.

4.2.3 Observations and Discussion

Russia has not sustained much damage to their network, contrary to the rumors circling in press that it will be disconnected from the global Internet. We found a decrease of 10.94% in the number of distinct *as_origins* since the start of the war. However, as we

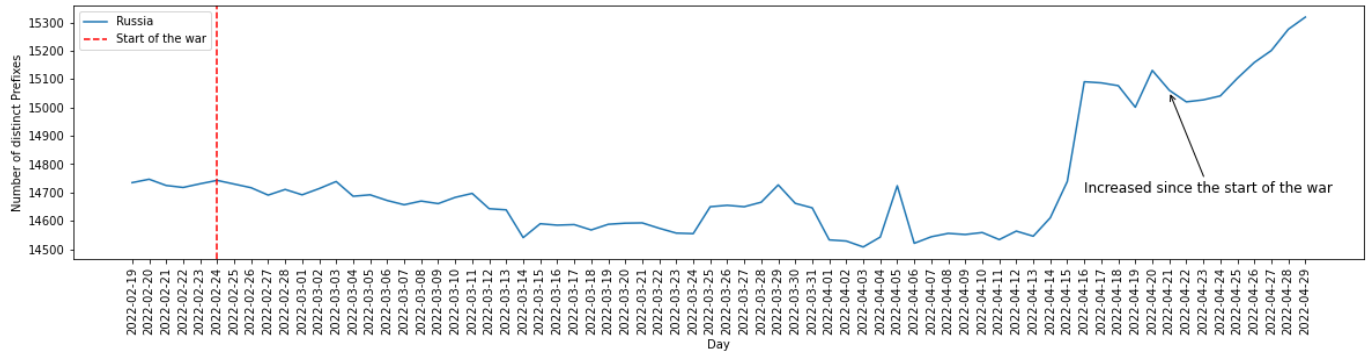

Figure 6 Number of Distinct Russian Prefixes at LINX

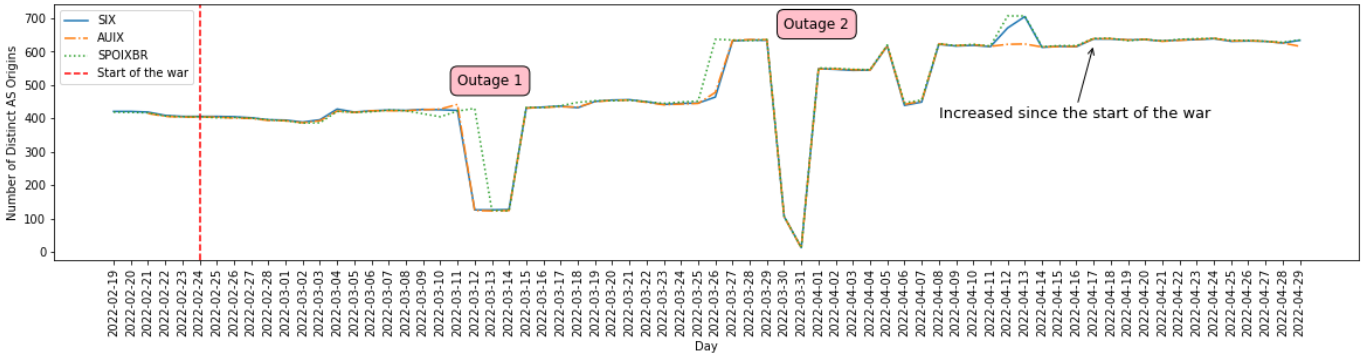

Figure 7 Number of Distinct Russian *as_origins* at SIX, AUIX and SPOIXBR

observed in the plots the number of distinct *as_origins* has increased after the war, making this loss less significant since the total number of Russian ASes has grown since the start of the war. The loss of the old ASes could just signify a change in Russia's internal Internet network infrastructure. Moreover, the number of Russian prefixes has increased, suggesting that the sanctions applied to Russia did not have a major impact on their network. Our findings align with the ones seen in the report by ThousandEyes [17].

Major transit providers Cogent and Lumen have stopped their services to Russia, this did not amount to much since we did not register a drop in overseas Russian Prefixes at SIX, AUIX and SPOIXBR. This can be explained by the numerous alternative transit providers that Russia can still use [21]. The reason behind this ban was limiting Russia's capacity to perform cyberattacks, according to CNN [22].

IXPs have not ceased providing services to Russia in any meaningful way. LINX has stopped providing services to the two biggest Russian ISPs: Rostelecom and Megafon. However, these ISPs were barely using LINX's services already, and LINX continues to advertise prefixes which contain those ISPs in their *as_path*. According to the statement provided by LINX to their customers, these measures were not designed to block Russia from the internet but rather to target individuals which are affiliated with the current Russian government and responsible for the war [3]. Some of them are in direct ownership or benefit from Rostelecom and Megafon. Europe imposed sanctions against these persons [6] and LINX was merely complying with them.

5 CONCLUSIONS AND FUTURE WORK

In this paper we analyzed the effects of the Ukrainian conflict on the Internet using routing tables gathered from five IXPs. We found how many Ukrainian and Russian ASes were lost, for how long were they lost, and we identified the biggest outages and the events responsible for them.

Our results show that each IXP has lost connection to an average of 10% of Ukrainian ASes. We identified 5 big outages which are responsible for this loss. LINX lost most Ukrainian connections and has not yet restored all of them. Other IXPs started recovering since April and the number of outages has decreased.

We did not find any substantial damage, or loss of connectivity to the Russian network. Contrary to the sanctions imposed by numerous companies, the Russian network remains reachable and shows signs of growth. From our results the sanctions showed no considerable effect on the Russian network.

As this research focused on a limited set of IXPs, future work could analyze data from other IXPs. In particular DECIX, since it is the largest one in Europe and from the limited data we had, we noticed that it had a lot of Russian and Ukrainian connections, so it might provide some new insights. Besides, since we saw some patterns in the overseas IXPs it would be interesting to investigate an African IXP and see if those patterns repeat there as well. It would also be worthwhile to look at the data we analyzed from a different angle, by counting the number of unique reachable IP addresses. This will show more detailed and fine-grained results than our approach, but it was unfortunately too complex for the given timeframe.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Leandro Bertholdo for assisting me with the research and providing the dataset I analyzed. This research would not have been possible without his numerous suggestions and invaluable feedback.

REFERENCES

[1] 2022 boycott of Russia and Belarus - Wikipedia: *https://en.wikipedia.org/wiki/2022_boycott_of_Russia_and_Belarus* Accessed: 2022-07-01.

[2] Bertholdo, L.M. et al. 2021. Forecasting the Impact of IXP Outages Using Anycast. (2021).

[3] Bill Woodcock on Twitter, March 11 2022: *https://t.co/Wytcj098LJ* Accessed: 2022-06-22.

[4] Chatzis, N. et al. On the importance of Internet eXchange Points for today's Internet ecosystem.

[5] Code Repository for this research: *https://github.com/Bo0ne/UkraineResearch*

[6] EUR-Lex - 32014R0269 - EN - EUR-Lex: *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0269* Accessed: 2022-06-25.

[7] Gerson, J. et al. A PRIMER ON INTERNET EXCHANGE POINTS FOR POLICYMAKERS AND NON-ENGINEERS.

[8] Global internet outages jump 22%, business-hours disruptions fall in mid-March | S&P Global Market Intelligence: *https://www.spglobal.com/marketintelligence/en/news-*

insights/latest-news-headlines/global-internet-outages-jump-22-business-hours-disruptions-fall-in-mid-march-69455283 Accessed: 2022-06-23.

[9] Internet disruptions registered as Russia moves in on Ukraine - NetBlocks: *https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K* Accessed: 2022-05-07.

[10] List of Internet exchange points by size - Wikipedia: *https://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size* Accessed: 2022-06-22.

[11] NetBlocks on Twitter, April 8 2022: *https://t.co/x6gPCYKyt0* Accessed: 2022-06-23.

[12] NetBlocks on Twitter, March 3 2022: *https://t.co/zNG42jfbIS* Accessed: 2022-06-23.

[13] NetBlocks on Twitter, March 28 2022: *https://twitter.com/netblocks/status/1508465391244304389?s=20&t=lNIGIXV-kAkEttykeSDVCw* Accessed: 2022-06-23.

[14] Richter, P. et al. 2014. Peering at Peerings: On the Role of IXP Route Servers. (2014). DOI: *https://doi.org/10.1145/2663716.2663757*

[15] RIR statistics exchange format – APNIC: *https://www.apnic.net/about-apnic/corporate-documents/documents/resource-guidelines/rir-statistics-exchange-format/* Accessed: 2022-06-20.

[16] Rostelecom and MegaFon were disconnected from the LINX Internet traffic exchange point, which is located in London | AKM EN: *https://www.akm.ru/eng/press/rostelecom-and-megafon-were-disconnected-from-the-linx-internet-traffic-exchange-point-which-is-loca/* Accessed: 2022-06-25.

[17] Russia and the Global Internet | ThousandEyes: *https://www.thousandeyes.com/blog/russia-global-internet* Accessed: 2022-05-07.

[18] Russia, Blocked From the Global Internet, Plunges Into Digital Isolation - The New York Times: *https://www.nytimes.com/2022/03/07/technology/russia-ukraine-internet-isolation.html* Accessed: 2022-05-07.

[19] Sam Halabi 200AD. *Internet Routing Architectures*. Cisco Press.

[20] Ukraine war: Major internet provider suffers cyber-attack - BBC News: *https://www.bbc.com/news/60854881* Accessed: 2022-07-02.

[21] Updated: Cogent and Lumen curtail operations in Russia | Kentik Blog: *https://www.kentik.com/blog/cogent-disconnects-from-russia/* Accessed: 2022-06-25.

[22] Why internet backbone services Cogent and Lumen are cutting off Russia - CNN: *https://edition.cnn.com/2022/03/11/tech/russia-internet-backbone-cogent-lumen/index.html* Accessed: 2022-07-02