How Russia's Invasion of Ukraine Impacted the Internet Peering of the Conflicted Countries

Antonios Chatzivasileiou*, Alexandros Kornilakis†, Katerina Lionta*,
Georgios Nomikos†, and Georgios Smaragdakis‡
*FORTH-ICS & University of Crete, †FORTH-ICS, ‡Delft University of Technology
anchatz@ics.forth.gr, kornilak@ics.forth.gr, klionta@csd.uoc.gr, gnomikos@ics.forth.gr, g.smaragdakis@tudelft.nl

***Abstract*—On February 24, 2022, Russia invaded Ukraine after months of military preparations. Although secondary to the human tragedy resulting from the war, the Internet connectivity in the region was disrupted due to the military conflicts and economic sanctions. We study the Internet peering connectivity of the conflicted countries before, during, and after the Russian invasion of Ukraine. Our analysis shows that de-peering activity by Ukrainian, Russian, and international networks started months before the invasion at peering facilities in Ukraine and Russia, respectively. De-peering continued after the Russian invasion of Ukraine, with only minor changes in peering taking place until end of 2023. Our study shows that several Internet exchange points have stopped operating in Ukraine. We also report that the invasion has impacted the registry country code of operational networks in Ukraine and Russia, creating a new status quo in Internet peering in the region.**

I. Introduction

Ukraine and Russia's diplomatic relationship has been challenging since the fall of the Soviet Union and the independence of Ukraine in 1991. In February 2014, Russia invaded Crimea, a southern region of Ukraine where the majority of the population is Russian speakers. In the same year, Russia annexed Crimea despite the United Nations' call for resolution [1]. Crimea's annexation had a significant impact on the Ukrainian Internet structure and flow of traffic. Although much of the traffic between Ukraine and Russia was exchanged in West Europe, traffic from Russian-speaking East Ukraine and Crimea was exchanged in Russia [2, 3]. Because of ongoing tensions, Ukraine's Internet designed and developed its Internet infrastructure to be resilient to Russia's cyber attacks by investing in high-speed links to the West, resilient national backbone network, and Internet exchange points as other countries, like Estonia, have done [4].

In May 2019, Volodymyr Zelenskyy was elected President of Ukraine proposing a pro-west-world orientation. For the following years, the diplomatic relationship between Ukraine and Russia was at the worst level ever. In the second half of 2021, the US President Biden and other countries' leaders repeatedly reported that Russian army forces were mobilized near the border of Russia as well as near the borders of Ukraine with Belarus, a Russia's ally, ready for a possible invasion [5].

On February 24, 2022, Russia invaded the eastern part of Ukraine. Many countries [6, 7] announced economic sanctions against Russia after the Russian invasion of Ukraine. Thus, international enterprises, including telecommunication and technology companies, could no longer operate in Russia. In March 2022, Russian armed forces captured Kherson, a strategic industrial and economic center in East Ukraine. In May 2022, Russian troops captured Mariupol, a port in the Sea of Azov and one of the most important financial centers in East Ukraine. In June 2022, around 20% of Ukraine was occupied by the Russian army [8]. Ukraine, backed with equipment donations by the international community, reclaimed occupied areas after the Summer of 2022. As of April 2024, large parts of Donetsk and Luhansk Ukrainian regions are still occupied [9].

In this paper, we study how the major geopolitical event of the invasion of Russia of Ukraine impacted (i) the peering connectivity between networks of the conflicting countries and (ii) the Internet peering infrastructure in Ukraine and Russia. Our study considers the period from Spring 2021 to Fall 2023, i.e., before, during, and after Russia's invasion of Ukraine. We investigate the period before February 2022 to understand the changes in the already fragmented peering activity of networks operating in Ukraine and the occupied Crimea as well as East Ukraine regions before (an expected) invasion by Russia. We also investigate the period after the invasion, as many Western countries, including the United States, announced economic sanctions against Russia that significantly impacted the operation of companies from these countries in Russia. We also investigate what was the reaction of Russian networks that peer in Ukraine and Ukrainian networks that peer in Russia. Our study uses passive and active measurements from various sources, including control plane data, DNS data, and peering databases, to shed light on the peering changes.

Our contributions can be summarized as follows:

- Our data analysis shows that de-peering activity by Ukrainian, Russian, and international networks started months before the invasion at Internet exchange points in both Ukraine and Russia. Notably, the de-peering rate was 6.3 times higher than the average for Ukraine and 18.3 times for Russia, with the majority of these ASes belonging to Russian and Ukrainian networks, respectively.
- Our analysis also shows that the de-peering of Russian networks in Ukrainian Internet exchange points, as well as Ukrainian and international networks in Russian Inter-

978-3-903176-64-5 ©2024 IFIP

net exchange points continued after the Russian invasion of Ukraine.
- Our study shows only minor changes in peering activity for Ukrainian, Russian, and international networks in Internet exchange points of the conflicting countries in recent months.
- Our study also reports that several Internet exchange points have stopped operating in Ukraine during the peak of the conflict in the Spring and Summer of 2022 and are not available anymore.
- The invasion has impacted the registry country code of operational networks in Ukraine and Russia, creating a new status quo in the Internet peering in the region.

II. Related Work

Russia-Ukraine conflict was the subject of research on their impact on the Internet. Fontugne et al. [2] documented the radical changes to the Crimean Internet in terms of connectivity and regulation after the annexation of the Crimean peninsula to the Russian Federation (in 2014). This work reported that traffic previously going through Ukraine started to be routed through Russia-based ISPs and transit providers. BGP was also used to measure the Ukrainian Internet fragmentation during the same crisis [10]. The study also reported that the same geopolitical dynamics of annexation and fragmentation can be observed in cyberspace as a direct consequence.

Following the Russia-Ukraine 2022 war, Luconi et al. [11] studied the impact of the first three months of the war on routing and latency in Ukraine. The verdict was that there was a substantial increase in BGP announcements and withdrawals, while latency also increased significantly. An analysis by Mizrahi et al. [12] displayed an asymmetric picture: during the war, Internet performance in Ukraine has been significantly degraded, while the performance in Russia has been improved. Khavrona [13] utilized BGP historical data to analyze route changes related to the war. The author noticed a significant number of BGP messages and route changes in the Ukrainian and Russian networks, but not in the Italian networks that were used as a baseline.

The geopolitical importance of Internet pathways, particularly in the Donbas region, is explored in [14]. A comprehensive examination of the connectivity of Autonomous Systems (ASes) within Ukraine indicates a gradual shift of those closely associated with Donbas from Ukrainian cyberspace to Russian cyberspace. Over time, the AS graph depicts the Donbas cluster on the outskirts of the Ukrainian Internet, yet not entirely integrated into the Russian Internet [14]. Indications, though anecdotal, suggest that the physical routes at the IP level may exhibit notable differences depending on whether the source is located within the territory governed by the Ukrainian government or one of the separatist republics [14]. While both routes lead to Moscow, the former follows an indirect path through international carriers to circumvent the Ukraine-Russia border, whereas the latter is more direct. Nevertheless, the study lacks statistical significance due to the limited number of analyzed paths.

The Mutually Agreed Norms on Routing Security (MANRS) initiative reported incidents of DDoS attacks and potential BGP hijacking events in the region [15]. RIPE Labs published an article assessing the resilience of the Internet in Ukraine during the initial three weeks of a critical period [16]. Their findings highlighted that the absence of market concentration and the presence of numerous Internet Exchange Points (IXPs) providing connectivity to Ukraine contributed to a remarkably resilient network, even amidst catastrophic events and cyber attacks. In a follow-up article a year after the invasion, a new report by RIPE Labs showed that the state on the Internet in Ukraine has not changed significantly [17].

Between February 21 and March 4, Cloudflare monitored the infrastructure of major cities in Ukraine [18]. The observed traffic patterns indicated an increase in activity in western cities, attributed to the movement of people towards the western border. Concurrently, there was a decrease in traffic at eastern cities. Notably, Cloudflare also detected a high number of Distributed Denial of Service (DDoS) attacks during this period, underscoring the interconnected nature of real-world conflicts and the emergence of hostile activities in the cyber domain. Cloudflare took proactive security measures by relocating customer encryption key material from their data centers in Ukraine, Russia, and Belarus. Operations were seamlessly preserved through more secure data centers. Additionally, the deployed machines were configured to self-brick in the event of power or connection losses, enhancing the overall security posture [19].

Trusin et al. [20] studied the impact related to the connectivity of Russian and Ukrainian ASes. They examined the routing tables from 5 large IXPs (AMSIX, LINX, SIX, AUIX, and SPOIXBR) during the period of 19 February 2022 to 29 of April 2022. Their findings revealed a disruption in connectivity, with each IXP experiencing an approximate 11% loss in connections to Ukrainian ASes. However, signs of recovery were observed across most IXPs beginning in April 2022. Despite the encountered challenges and network disruptions, the Ukrainian network demonstrated resilience, largely attributed to its redundant infrastructure and routing strategies. As for Russia, they did not find any substantial damage or loss of connectivity. This assertion finds support in a study by Aben [21], which highlights the crucial role played by the high-level structure of interconnections within Russian networks and their connectivity to the global network. This structural resilience significantly contributed to mitigating the impact of the sanctions imposed.

A study by Cloudflare on the anniversary of a year of Russia's invasion of Ukraine showed that traffic in occupied areas was re-routed to Russia but [22]. The same study also showed that Ukraine's widespread connectivity to networks outside the country and the operation of IXPs in the country helped Ukraine to remain resilient from both an infrastructure and routing perspective. Singla et al. [23] scanned the Ukrainian IPv4 space daily for protocols used in critical infrastructure for over six months to assess the impact of Russia's invasion on Ukrainian critical infrastructure.

A year after Russia's invasion of Ukraine, Google published a report describing how the Ukraine conflict transformed the cyber threat landscape [24]. The report outlined how Russian government-backed attackers were involved in a parallel cyberwar in the region and worldwide. This is not the first time Russia has engaged in such practices during a conflict. Previous studies also investigated the impact of cyberattacks on critical Internet services during the conflict between Russia and Estonia as well as between Russia and Georgia in 2007 [4].

RIPE NCC has published a statement addressing its stance on the Russo-Ukrainian war, outlining its approach to membership, billing, and the sanctions in effect [25]. Notably, all members of RIPE NCC are treated equally, with Ukrainian members assured that delayed payments will not result in account closure. Additionally, RIPE NCC is fully compliant with EU sanctions. Given that IP resources are deemed economic assets, all IP resources in sanctioned areas are considered frozen. Consequently, sanctioned entities are prohibited from acquiring additional resources or transferring existing ones. However, RIPE NCC does not de-register already existing resources for these entities.

Proceeding with the AS classification task, Carisimo et al. [26] achieved an organization-to-AS mapping to uncover the ones owned by the state. A few years ago, Yacobi-Keller et al [27] published a paper that proposed a methodology for AS geolocation. ASdb [28] is a system that attempts to identify the type of organization that owns an AS. Our work differs from the previous ones since we geolocate the AS based on the organization's physical address, and neither are we interested in geolocating at the city level or considering the organization's characteristics per se.

III. Datasets

This section offers an overview of the datasets used in our study, spanning from April 2021 to October 2023. Given that most of our data sources provided information at three-month intervals, we established timestamps from April 2021 to October 2023, also at three-month intervals. Figure 1 illustrates the pipeline of data collection and merging datasets from the different data sources.

A. Data Plane

1) AS to Organization Data: We used data from CAIDA [29] and RIPEstat [30] sources for the AS-to-organization dataset. In the case of CAIDA, we downloaded all available AS-to-org datasets available in the time range we were studying, performing parsing and data merging to achieve the desired format. This approach allowed us to retrieve a total of 100,309 ASes for the initial timestamp. Over the course of our measurements, this number steadily increased, reaching 114,070 ASes by our final timestamp. It's important to note that this growth reflects the natural increase in registered ASNs, although not all of these ASes are necessarily active.

As for the RIPEstat dataset, we developed a script leveraging HTTP requests to interact with the RIPEstat API. This script facilitated the retrieval of all ASes affiliated with organizations in Russia or Ukraine, mirroring our approach with the CAIDA dataset. By utilizing the RIPEstat API, we were able to efficiently gather the necessary data. For Ukraine, we initially gathered data on 1,840 ASes for the first timestamp, which reduced to 1,729 ASes by April 2022. Subsequently, the number remained relatively stable at around 1,730 ASes up to our latest timestamp. In the case of Russia, we initially obtained information on 5,180 ASes, which decreased to 5,070 ASes by the latest timestamp.

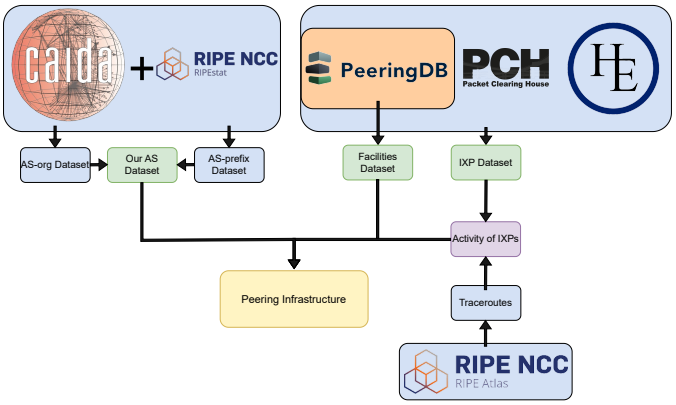

Fig. 1. Pipeline of data collection and analysis per timestamp.

2) Prefixes: For the Prefixes dataset, we also relied on data from both CAIDA and RIPEstat sources. To populate the prefix to AS map, we utilized the information obtained from CAIDA, which, in turn, derives its data from Routeviews. For each timestamp, we downloaded a file that serves as a prefix-to-AS mapping. Additionally, for the RIPEstat dataset, we employed a script designed to send specific requests, enabling the retrieval of prefixes associated with Ukrainian or Russian ASes.

3) AS classification: To categorize each Autonomous System, we utilized the dataset of May 2022 from ASdb [28]. The AS classification from ASdb consists of two layers, each offering distinct levels of detail regarding the type of the AS. Layer One, termed the "General type," provides a broad classification such as "Computer and Information Technology" or "Education and Research." Layer Two further refines this classification, offering more detailed insights into the category of the AS, including designations like "ISP" or "Cloud provider." This hierarchical structure allows for a comprehensive understanding of AS types, from overarching classifications to specific categories within each type. Finally, ASdb provides multiple pairs of Layer one - Layer two classifications for each AS according to the spectrum of classes that each AS covers, with Category 1 indicating the most probable classification and subsequent categories detailing the least suited classes.

B. Peering Infrastructure

1) IXPs: Retrieving historical information for past periods presents a significant challenge. In order to comprehend the

current and previous states of IXPs in Russia and Ukraine, it was necessary to obtain historical data. CAIDA maintains historical IXP data from three distinct sources: Peering DB (PDB) [31], Hurricane Electric (HE) [32], and Packet Clearing House (PCH) [33] in three-month intervals. Consequently, our process involved parsing these specified files and filtering the IXPs located in Russia and Ukraine to construct a comprehensive historical dataset. IXP dataset contains information about the name of the IXP, its country and city location, website URL, contact information, as well as IPv4 and IPv6 prefixes. Finally, it provides a list with all the ASes that are members in that particular IXP.

In contrast to the decreasing trend observed for ASes over the examined period, this does not appear to be the case for IXPs. Specifically, Ukrainian IXPs seem to increase in number, from 16 IXPs at the initial timestamp to 24, while Russian IXPs show a similar pattern, rising from 47 to 50. However, as we will delve into later in this work, the reality may not be as straightforward as it seems.

2) Peering facilities: The peering facilities dataset contains information similar to that of the IXPs dataset. We specifically sourced historical data from CAIDA, which, in turn, obtains this information only from PeeringDB. More precisely, the number of Ukrainian peering facilities was 32 at the start of our measurements and increased to 41 by the end of the period. The count initially stood at 61 for Russian peering facilities and increased to 65. This targeted approach ensures the incorporation of pertinent historical data, enhancing our analysis of the evolving landscape of Internet Exchange Points and peering facilities in both studied regions.

3) ASes in IXPs and peering facilities: After specifying the Internet exchange points and peering facilities in Ukraine and Russia for the given timestamps, a critical task is to identify the AS members for each IXP and peering facility at any given timestamp. This poses a non-trivial challenge due to the dynamic nature of the problem. Indeed, IXPs may have several hundred AS members, and these can be added or removed at any time.

Initially, our strategy involved obtaining the AS members listed on each IXP's website. However, this approach proved challenging as only a limited number of IXP websites offered such information. Additionally, accessing historical data from these websites via web archive [34] was also partially available, further limiting our ability to gather comprehensive datasets. Similarly, the Euro-IX IXP database [35] did not offer historical data either through its platform or via web archives. Our next choice was again CAIDA which keeps historical data about the AS membership of IXPs and peering facilities as described in Sections III-B1 and III-B2. Consequently, confirming the accuracy of data provided by PDB, HE, or PCH becomes inherently difficult. Nevertheless, we populated our IXP and peering facility dataset with AS members based on the information available from these sources. Giotsas et al. [36] introduced a method for validating the membership of ASes within IXPs and peering facilities by leveraging DNS records, as outlined in their study. We followed this approach in our research (see Section IV-F) to validate the sources used in our study.

The data reveals that the membership for Ukrainian IXPs and peering facilities decreased from 579 to 577, and for the Russian counterparts, it reduced from 1,355 to 1,064. However, as we will delve into in Section V, these numbers conceal a wealth of insights.

4) AS Relationships: To gather the relationship status of Ukrainian and Russian ASes, we utilized the AS-relationship dataset serial-1 from CAIDA [37]. For each timestamp, we downloaded the corresponding file for IPv4 and IPv6, containing nearly 600,000 entries in total. This dataset provides AS relationships inferred from BGP data.

5) Traceroutes: In order to determine which IXPs in Ukraine are active during our period, we retrieved all traceroutes from RIPE Atlas [38] for the first 10 days of each timestamp. In Section IV-E we describe how we use these data in order to determine which IXPs are active. For each timestamp, the size of the traceroute file was approximately 20 GB.

6) PTRs: A DNS pointer record, or PTR, refers to the host name linked to an IP address. To validate the IXP members provided by PDB, HE, and PCH, we chose to retrieve PTRs for all IPs associated with each Ukrainian IXP's prefix during our latest at that time timestamp in July 2023. It is important to note that this procedure could not be executed for previous timestamps due to the unavailability of historical PTRs covering the IPs of the tested IXPs. We successfully obtained 1,852 PTRs out of the 5,952 IPs retrieved from Ukrainian IXP interfaces. This is a noteworthy achievement considering that IXPs typically do not utilize the entire IP space of their prefix.

IV. Methodology

In this section, we present our methodology for inferring changes before, during, and after Russia's invasion of Ukraine.

A. AS-org Data and Prefixes

As mentioned in Section III-A, for each timestamp, we obtained AS information, including organization details, from CAIDA, along with the AS-to-prefix mapping. We then integrated the AS-to-prefix mapping data from CAIDA with the AS-organization dataset from the same source. This integration allowed us to create a comprehensive dataset that encompasses ASes, their associated information, and prefixes for every AS. CAIDA's dataset contains numerous ASes without any associated prefix. To focus exclusively on routed ASes, we opted to disregard those ASes lacking prefixes.

In our approach with the RIPEstat dataset, our focus was on gathering Ukrainian and Russian ASes, along with their organizational details and corresponding prefixes. We then merged the CAIDA and RIPEstat datasets to create a comprehensive AS dataset, prioritizing the Ripestat database as the baseline and integrating any additional routed ASes from CAIDA. Our analysis revealed a high level of consistency, approximately 99.8%, particularly concerning routed ASes.

However, discrepancies emerged regarding four specific ASes (AS 41082, AS 50005, AS 197880, and AS 50553). The classification discrepancies primarily involved the first three ASes: CAIDA identifies them as Russian (AS 50005 until 10/2022), whereas RIPEstat categorizes them as Ukrainian. Conversely, CAIDA designates AS 50553 as Ukrainian, while RIPEstat identifies it as Russian.

Considering the aforementioned four ASes, we opted to assess changes in country codes specifically using the RIPEstat dataset. For each Ukrainian AS, we documented potential alterations in the country code to Russian and conversely, for Russian ASes, we recorded any changes suggesting a shift to Ukrainian. More details about this in Table I and Sections V-A1 and V-B1.

B. IXPs and peering facilities

For each timestamp, we combined the IXPs and peering facilities dataset, as obtained in section III-B, resulting in an extensive collection that encompasses information about the location and AS members of every Internet exchange point (IXP) and facility within each country which is updated at three-month intervals. We focus on IXPs and peering facilities in Ukraine and Russia.

C. ASdb classification

The ASdb dataset offers a wide range of categories for each AS. Our primary focus lies in examining the types of ASes removed from IXPs and peering facilities in networking terms. To achieve this, for each AS in ASdb, we prioritize identifying the first category where the Layer One type is "Computer and Information Technology." Subsequently, we explore the second layer of this category. However, if there is no category directly related to "Computer and Information Technology," we resort to utilizing the Category One Layer Two type of the AS.

D. Russia-Ukraine AS relationships

To categorize the relationship status between Ukraine and Russia, we classified them into three categories: Peer to Peer (P2P), Client to Provider (C2P), and Provider to Client (P2C). For each pair provided in the AS relationship file, see Section III-B4, if the first AS in the pair is Ukrainian and the second is not, with a relationship value of -1, we add the non-Ukrainian AS to the P2C list. Conversely, if the second AS is Ukrainian and the first is not, we include the non-Ukrainian AS in the C2P list. Finally, for P2P relationships, we are interested in both sides of the pair when the relationship value is 0. We then count the number of Russian ASes in each list, and based on these numbers, we plot Figures 7-10, see Section V-C.

E. Status of Ukrainian IXPs

One of the central challenges in our research is the reliance on self-reported data for the status of IXPs. This presents a significant issue, particularly during times of turmoil, such as the invasion. Many IXPs that were known to have shut down during the invasion continued to appear as 'online' in the dataset. In an effort to clarify their status, we reached out via email to all Ukrainian IXPs. However, only one IXP, Meshroom-IXP, responded, confirming that it was destroyed in March 2022 and remained offline until our latest measurements in October 2023. This information contradicts the data from PDB, HE, and PCH, all of which continued to report Meshroom-IXP as active.

To validate self-reported data, we used traceroute information from RIPE Atlas. For each timestamp, we collected all available traceroutes for the first 10 days using RIPE Atlas API. If we detected an IP address associated with a specific IXP in a traceroute path, we considered the IXP as active during that timestamp, and kept the source-destination pair of that measurement. Figure 6 depicts in detail our findings.

However, the absence of a particular IXP in a traceroute does not necessarily imply it is offline. This could be due to the lack of that specific traceroute (source-destination). To address this, we grouped traceroutes by source-destination IP pairs. For instance, if, in two timestamps (2021/4 and 2021/7), IXP DTEL is not visible in any traceroutes for the first timestamp but is visible for the second timestamp, we attempt to find if the traceroute group (source-destination IP) matching DTEL-IX in 2021/7 also exists in 2021/4. If it does, it is more likely that DTEL-IX was offline in 2021/04, although there is a chance that the same traceroute followed a different path for the first timestamp. But, if there is no traceroute with the same source-destination pair, we cannot assume anything. Despite the uncertainty arising from potential path changes, this method represents the best effort analysis we could derive from traceroute data.

F. Validating IXP Membership

Similar to verifying the status of IXPs, we also encountered the need to validate the AS members of each IXP. To address this, we implemented a method involving retrieving reverse DNS records for every IP within each IXP, see Section III-B6. Typically, Internet Exchange Points (IXPs) allocate a dedicated IP address from their network to each member for communication purposes. Moreover, many IXPs encode AS (Autonomous System) information directly into the hostnames of their router interfaces. For instance, a hostname like tenet-ix.giganet.ua signifies that a router is located in Giganet in Ukraine and is connected to a network named tenet. By examining these PTR records, we could extract organizational information and subsequently determine the corresponding Autonomous System Numbers (ASNs) of the IXP members.

Some network operators encode the facility information directly into the hostnames of their router interfaces. For instance, a hostname like x.y.rtr.thn.lon.z indicates that a router is situated in Telehouse-North in London. In our study, we compiled a comprehensive list of naming conventions used by seven operators in the UK and Germany to denote interconnection facilities. We then verified the accuracy of these DNS records with the respective operators to ensure their currency. Our validation process yielded promising results, with 91 out of 100 (91%) public peering interfaces and 191

TABLE I
OF ASES THAT CHANGED COUNTRY DURING OUR PERIOD BASED ON RIPESTAT DATA

# of ASes	2021/04 - 2022/01	2022/01 - 2022/10	2022/10 - 2023/04	2023/04 - 2023/10
RU to UA	2	4	21	0
UA to RU	6	4	35	6

out of 213 (89%) cross-connect interfaces correctly pinpointed based on the validated DNS records.

V. IMPACT ON PEERING

It is essential to emphasize that we do not take any political stance regarding the status of Crimea. Instead, our approach is strictly data-driven, presenting the information as acquired from the aforementioned data sources. By maintaining neutrality on political matters, we aim to ensure the integrity and objectivity of our analysis, allowing our findings to stand on empirical evidence rather than political bias. Our focus remains solely on analyzing and interpreting the technical data related to internet infrastructure and connectivity in the region. However, there are challenges. For example, Crimea is a disputed area. Recognizing the complex geopolitical context surrounding the region, we rely on RIPEstat country registry, as RIPE is responsible for the allocation of address space in both Ukraine and Russia.

Figures 2 and 3 depict the locations of each IXP in Ukraine and Russia, respectively. The radius of each circle is proportional to the number of IXPs in a given city. To generate these maps, we utilized the city field of each IXP. Notably, both countries include IXPs in Crimea, which we incorporated into both figures.

A. Impact in Ukraine

1) Visibility of Ukranian ASes: Throughout our observed period, the number of Ukrainian ASes experienced a modest decline, reaching its peak at 1,842 ASes in April 2021 and gradually decreasing to 1,717 by October 2023. However, upon closer examination of ASes over time, we identified a noteworthy trend: 55 ASes underwent a transition in their country code, shifting from Ukrainian to Russian between April 2021 and October 2023. Recognizing the possibility of recurrent changes in country codes for certain ASes, we conducted a comprehensive analysis by comparing all available timestamps from April 2021 to October 2023, aggregating the instances where ASes underwent country code modifications. This trend was also observed by Heichenko [39], who studied changes in ASes from Russian organizations to Ukrainian. The preeminent period for these AS-country changes unfolded from October 2022 to April 2023, encompassing 35 of the observed alterations as detailed in Table I.

2) AS Churn in Ukraine: In Figure 4, we illustrate the ingress and egress of non-Ukrainian ASes, specifically those from Russia, the United States (US), and other countries, from the Ukrainian IXPs and peering facilities. The inclusion of US ASes in this analysis is strategic, as they encompass numerous networks engaged in peering activities. We will focus on two timestamps marked by following notable changes.

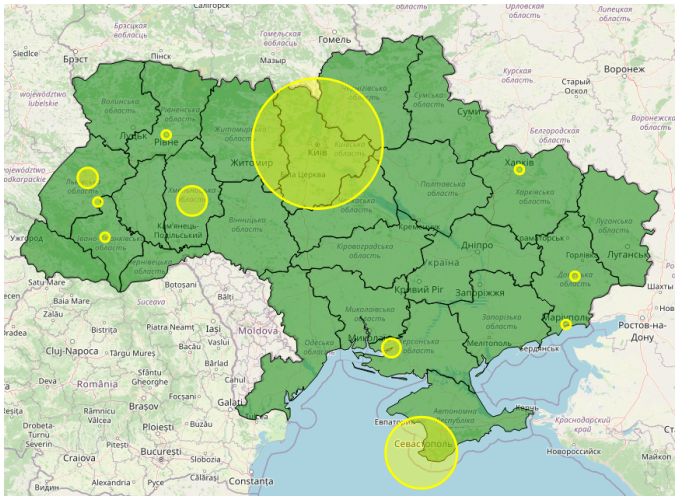

Fig. 2. Map of Ukrainian IXPs, the size of the radius is proportional to the number of IXPs in the specific area.

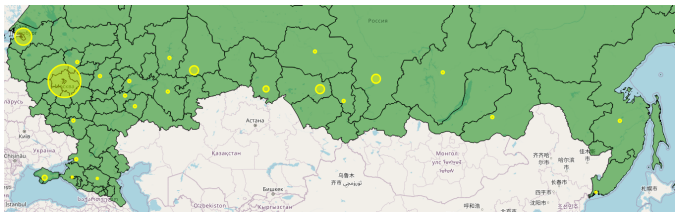

Fig. 3. Map of Russian IXPs, the size of the radius is proportional to the number of IXPs in the specific area.

October 2021 until January 2022: During this period, the total number of ASes disconnected from the Ukrainian infrastructure is 45, a figure 6.3 times higher than the average number of ASes disconnected from the Ukrainian infrastructure during historic periods we studied (excluding 1/2022 - 4/2022). Out of these 45 ASes, 37 (82.22%) are Russian, and the remaining 8 (17.78%) are other entities. Furthermore, among these 45 ASes, 71.11% are categorized as ISPs, 4.44% as cloud providers, and 4.44% as computer and network security.

January 2022 until April 2022: During this period, we observe a notable surge in the removal of Russian ASes from the Ukrainian infrastructure. A total of 60 ASes disconnected, marking an increase of 8.4 times above the average in other peiods we studied. Out of these 60 ASes, 55 (91.67%) are of Russian origin, 1 AS is from US (ISP), while the remaining 4 (6.67%) that are also ISPs, belong to other entities. The classification of these ASes mirrors a similar pattern as the previous timestamp, with 73.33% categorized as ISPs, 5% as cloud providers, and 3.33% as software development.

3) Infrastructure Changes in Ukraine: Figure 6 illustrates the status of Ukrainian IXPs throughout our timeline. The green color denotes active IXPs, determined based on the methodology outlined in Section IV-E. Red indicates IXPs where a traceroute exists with the IXP's IP in its path for a timestamp before or after, but for the specific timestamp in question, we find the previously matched IXP (source -

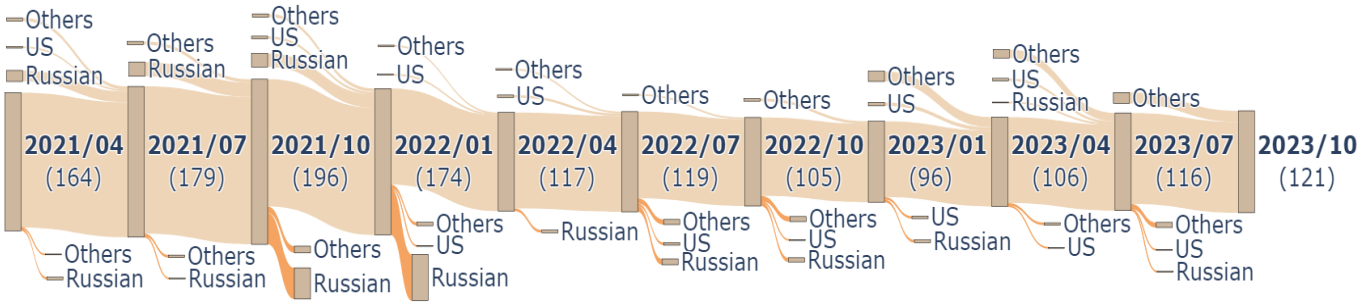

Fig. 4. Joins and disconnections of non-Ukrainian ASes in Ukrainian infrastructure.

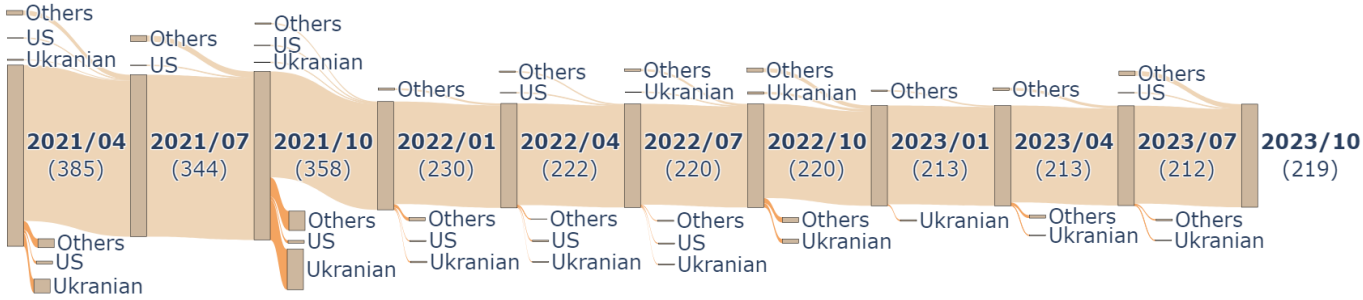

Fig. 5. Joins and disconnections of non-Russian ASes in Russian infrastructure.

Fig. 6. Ukrainian IXPs activity. Green: IXPs IP detected, Red: IXPs IP not detected for the same route that in previous or next timestamp did, Grey: The IXP does not exist in the specific timestamp, Dark red: IXP existed in our dataset but with no matched traceroute.

destination) but without the IXPs IP in the path. Dark red represents IXPs not found in any traceroutes, with no matches for timestamps before or after. Finally, grey color indicates that the specific IXP at the specific timestamp does not exist in our dataset, created from (PDB, HE, and PCH).

The first three IXPs, namely MESH-IX, DN-IX, and CLOUD-IX KHA, offer intriguing insights into their activity patterns. Situated on the southeast side of Ukraine, these IXPs experienced notable changes following the invasion on February 24. Both MESH-IX and CLOUD-IX went offline after the invasion and remained inactive until the conclusion of our research period. DN-IX, on the other hand, remained active from July 2022 to October 2022. However, starting from January 2023, we were unable to detect any of its IPs in traceroutes. This shift in activity underscores the dynamic nature of the region's internet infrastructure during the turbulent period under examination.

The majority of Ukrainian IXPs are visible in at least three of our timestamps, except for the last five IXPs for which we were unable to match any of their IPs. We explain in Section IV-E, regarding why two out of the five IXPs are undetectable. It is important to highlight that when an IXP is not marked as grey, it indicates that our sources consider the IXP to be active. However, in the case of MESH-IX, we received confirmation that it was destroyed. This discrepancy underscores the potential lack of updates in our sources. Nevertheless, our methodology aligns with the assertions made by the network administrator regarding the status of MESH-IX.

Another significant observation from Figure 6 is the presence of IXP GigaNET in our datasets until April 2022. Subsequently, GigaNET IXP vanished from our datasets, resulting in it being grayed out after April 2022. Additionally, three new IXPs were introduced: GigaNET Lviv, GigaNET IXN, and GigaNET Zaporizhzhya. For the latter two, we weren't able to find any matched IP from traceroutes. However, it is noteworthy that our dataset provides a much smaller number of IPs for each IXP compared to when it was GigaNET alone. Previously, GigaNET had one /23 and three /24 IPv4 prefixes,

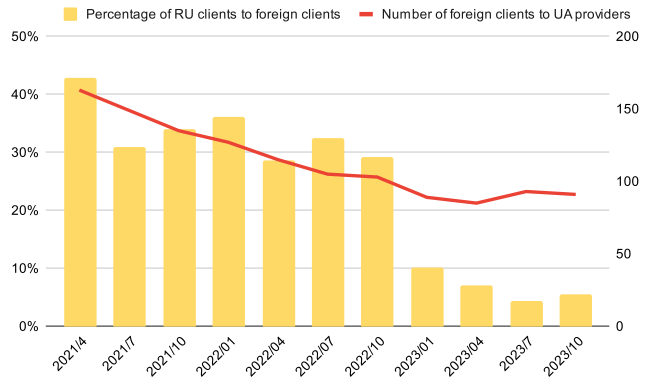

Fig. 7. AS Relationship for Ukrainian providers. Right vertical axis represents the number of foreign ASes being clients to Ukrainian providers. Left vertical axis represents the percentage of Russian ASes among those clients.

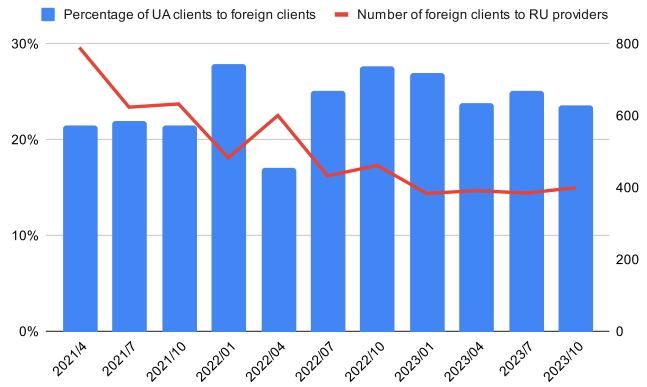

Fig. 8. AS Relationship for Russian providers. Right vertical axis represents the number of foreign ASes being clients to Russian providers. Left vertical axis represents the percentage of Ukrainian ASes among those clients.

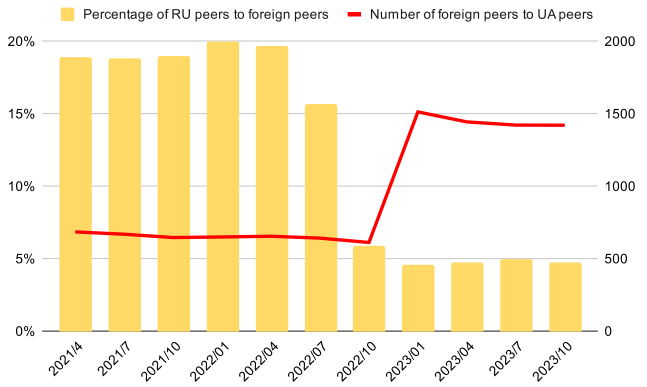

Fig. 9. AS Relationship for Ukrainian peers. Right vertical axis represents the number of foreign ASes peering with Ukrainian ASes. Left vertical axis represents the percentage of Russian ASes among those peers.

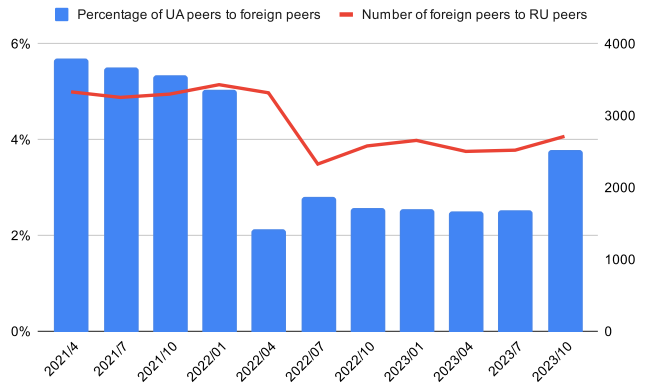

Fig. 10. AS Relationship for Russian peers. Right vertical axis represents the number of foreign ASes peering with Russian ASes. Left vertical axis represents the percentage of Ukrainian ASes among those peers.

and five /64 IPv6 prefixes. Now, GigaNet Lviv has one /26, GigaNet IXN has one /23, and GigaNet Zaporizhzhya has one /26 IPv4 prefix.

B. Impact in Russia

1) Visibility of Russian ASes: Similar to Ukraine, the number of Russian ASes remained relatively stable, hovering around 5,100 ASes and showing a slight decrease from April 2021 (5,180) to October 2023 (5,057). However, as indicated in Table I, some ASes undergo a change in country code, transitioning from Ukrainian to Russian and vice versa. This dynamic is a contributing factor to the relatively modest change in the total number of ASes per country. Specifically, a total of 29 ASes changed their country code from Russian to Ukrainian when comparing the first and last timestamps only. Further analysis across all timestamps reveals that 21 out of these 29 ASes switched from Russian to Ukrainian between October 2022 and April 2023.

2) AS churn in Russia: Examining Figure 5, a notable pattern emerges, particularly during the following two distinct periods.

April 2021 until July 2021: A total of 54 ASes disconnected during this period, marking a substantial increase of 7.4 times compared to the average number of ASes disconnected in other periods we studied. Out of these, 29 ASes (53.7%) were Ukrainian, 6 (11.11%) were from the US, and 19 (35.19%) were from other countries. Categorically, 74.07% were classified as ISPs, 5.56% as cloud providers. The remaining percentage is divided among various categories.

October 2021 until January 2022: During this period, a significant departure of 133 ASes from Russia's infrastructure was observed, an 18.3-fold increase compared to the average number. Of these, 86 (64.66%) were Ukrainian ASes, 41 (30.83%) were from other countries, and 6 (6.51%) were from the US. Categorically, 78.2% were classified as ISPs, 4.51% as cloud providers, and 3.76% as phone providers. Notably, almost all Ukrainian ASes left during this period, just before the launch of the invasion, providing a crucial insight

C. AS Relationships

In this section, we delve into the dynamics of interconnections between Ukraine and non-Ukraine entities, specifically focusing on the relationships involving Ukrainian providers

with foreign clients, foreign providers with Ukrainian clients, and Ukrainian peers with foreign peers. Notably, we observed a significant trend in the set involving Ukrainian providers to foreign clients. Figure 7 illustrates a decline in the number of foreign clients connecting to Ukrainian providers throughout our timeline.

1) Provider-to-Client Change: To gain further insights, we identified the country code for every AS that participates in a Ukrainian provider-to-client relationship. While many clients maintained relative stability, Russian clients experienced a significant reduction. What was once the country with the highest number of AS clients connected to Ukrainian providers now exhibits a nearly nonexistent relationship with them.

Figure 8 illustrates different trends in the results. While the number of foreign clients to Russian providers is decreasing, there is a slight increase in the percentage of Ukrainian clients compared to foreign clients, as probably international networks also start being served by Russian providers. Specifically, we observe a notable decrease in Russian providers serving Ukrainian clients for the April 2022 timestamp, followed by a subsequent increase.

2) Peer-to-Peer Relationships: The Peer-to-Peer connectivity in Ukraine, as depicted in Figure 9, reveals an interesting trend. Starting from October 2022, there is a notable increase in the number of foreign peers connecting to Ukrainian peers from 680 to 1,500, nearly doubling by January 2023, and maintaining that elevated level thereafter. However, during the same period, the percentage of Russian peers compared to total foreign peers drops significantly from 18% to 5%.

Figure 10 illustrates the Peer-to-Peer connectivity in Russia. We observe a decreasing number of foreign peers connecting to Russian peers, dropping from 3,333 at the start to 2,329 by July 2022. Meanwhile, the percentage of Ukrainian peers compared to total foreign peers declined from 5.61% to 2.11% in April 2022, remaining below 2.5% for subsequent timestamps except for October 2023, where it increased to 3.4%.

3) Client-to-Provider Change: The number of foreign providers serving Ukrainian clients remains stable at approximately 135 throughout the entire analyzed period. However, the percentage of Russian providers among these foreign providers decreases. It stays around 36% from April 2021 until October 2022, but then declines to around 20% in January 2023, maintaining this level until the last timestamp.

The number of foreign providers serving Russian clients remained stable around 200 until April 2022. From July 2022 onwards, it decreased steadily, reaching 157 by the last timestamp, with 119 ASes remaining as foreign providers to Russian clients. In contrast, the percentage of Ukrainian providers to foreign providers that serve Russian clients started at 20% in April 2021, declined to 4.8% in January 2023, and further dropped to 3.2% by October 2023.

D. Validation

To validate our results regarding disconnections, we obtained all available PTR records from the Ukrainian IXPs following the methodology outlined in Section IV-F. In total, we collected 1,852 PTR records, and through manual efforts, we successfully associated AS numbers with 1454 of these records. The remaining 398 PTR records posed challenges for AS number retrieval, often due to IXPs using certain IPs as interfaces for their internal machines. In instances where uncertainty arose regarding the associated AS for a specific PTR record, we exercised caution and chose to exclude such records from our analysis. Additionally, if a PTR record matched to more than one AS, we included all corresponding ASes to ensure coverage in our analysis.

TABLE II
VALIDATION ACCURACY FOR UKRAINIAN IXPS

Internet Exchange Point	Visibility	Results	PTR/IPs	PTRs/ASes
GigaNET IXN	78.23%	248/317	443/512	443/459
Digital Telecom Internet Exchange	73.36%	201/274	336/512	336/370
Ukrainian Internet Exchange	87.62%	184/210	577/768	577/347
1-IX Internet Exchange	79.01%	64/81	129/256	129/204
IF-IX	43.33%	13/30	21/256	21/21

The total number of ASes that are members of Ukrainian IXPs, amounts to 529. Using our methodology, we successfully retrieved information for 407 ASes, resulting in an accuracy rate of 75.3%.

Taking the first row of Table II as an example, out of the 512 IPs associated with GigaNET IXN, we collected 443 PTRs. These 443 PTRs were linked to 459 unique ASes. Subsequently, we compared these 459 ASes with the 317 ASes provided by our datasets. We successfully matched 248 ASes out of 317, providing visibility for 78.23% of the total ASes in GigaNET IXN.

VI. CONCLUSION

Our study shows that de-peering activity by Ukrainian, Russian, and international networks took place in Ukraine and Russia months before Russia's invaded of Ukraine. We attribute this to the preparations for a possible invasion and the bad diplomatic relationships between Russia and Ukraine. Our study also shows that de-peering continued during the first months after the invasion, with moderate changes in the following months until the end of October 2023. Due to the geopolitical setting and sanctions, peerings between Russian and Ukrainian networks and international and Russian networks were significantly impacted. We also observed changes in the country registries for networks in the conflicting countries. Our analysis also shows that parts of the peering infrastructure, especially in eastern Ukraine, were destroyed and are not operational until end of October 2023.

Our future agenda includes studying the changes in the peering relationships, infrastructure, and ecosystem in the region, including neighboring countries to Ukraine and Russia. We also plan to monitor the changes in the country register and assess how these affect peering decisions and how geopolitical tensions influence registrations in the region.

Acknowledgment

We would like to thank the anonymous reviewers and our shepherd, Alexander Garrido Gamero, for their constructive feedback. This work was supported in part by the European Research Council (ERC) under the Starting Grant ResolutioNet (ERC-StG-679158).

References

[1] United Nations, "General Assembly Adopts Resolution Calling upon States Not to Recognize Changes in Status of Crimea Region." [Online]. Available: https://press.un.org/en/2014/ga11493.doc.htm

[2] R. Fontugne, K. Ermoshina, and E. Aben, "The Internet in Crimea: a Case Study on Routing Interregnum," in *IFIP Networking Conference*, 2020.

[3] K. Limonier, F. Douzet, L. Petiniaud, L. Salamatian, and K. Salamatian, "View of Mapping the routes of the Internet for geopolitics," *First Monday*, vol. 26, no. 5, 2021.

[4] R. Stapleton-Gray and W. Woodcock, "National Internet Defense – Small States on the Skirmish Line," *Communications of the ACM*, vol. 54, no. 3, 2011.

[5] Associated Press, "Biden is 'convinced' Putin has decided to invade Ukraine." [Online]. Available: https://apnews.com/article/russia-ukraine-joe-biden-europe-russia-moscow-c2e55b8b2b061b58e2b140d2a6dc1d57

[6] US Office of Foreign Assets Control, "Russia-related Sanctions." [Online]. Available: https://ofac.treasury.gov/sanctions-programs-and-country-information/russia-related-sanctions

[7] European Union, "Sanctions adopted following Russia's military aggression against Ukraine." [Online]. Available: https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en

[8] Reuters, "Russia occupies 20% of Ukraine's territory." [Online]. Available: https://www.reuters.com/world/europe/russia-occupies-20-ukraines-territory-zelenskiy-2022-06-02/

[9] BBC, "Ukraine in maps: Tracking the war with Russia." [Online]. Available: https://www.bbc.com/news/world-europe-60506682

[10] F. Douzet, L. Pétiniaud, L. Salamatian, K. Limonier, K. Salamatian, and T. Alchus, "Measuring the fragmentation of the Internet: the case of the Border Gateway Protocol (BGP) during the Ukrainian crisis," in *International Conference on Cyber Conflict*, 2020.

[11] V. Luconi and A. Vecchio, "Impact of the First Months of War on Routing and Latency in Ukraine," *Computer Networks*, vol. 224, no. 5, 2023.

[12] T. Mizrahi and J. Yallouz, "Internet Performance in the 2022 Conflict in Ukraine: An Asymmetric Analysis," *arXiv preprint arXiv:2205.08912*, 2022.

[13] R. Khavrona, "Analysing Internet route changes related to the Russia-Ukraine war using BGP historical data," B.S. thesis, University of Twente, 2022.

[14] K. Limonier, F. Douzet, L. Petiniaud, L. Salamatian, and K. Salamatian, "Mapping the routes of the internet for geopolitics: The case of eastern ukraine," *First Monday*, vol. 26, 04 2021.

[15] A. Siddiqui, "Did Ukraine suffer a BGP hijack and how can networks protect themselves?" 2022. [Online]. Available: https://manrs.org/2022/03/did-ukraine-suffer-a-bgp-hijack-and-how-can-networks-protect-themselves/

[16] E. Aben, "The Resilience of the Internet in Ukraine," 2022. [Online]. Available: https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine/

[17] ——, "The Resilience of the Internet in Ukraine - One Year On," 2023. [Online]. Available: https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine-one-year-on/

[18] J. Graham-Cumming, "Internet traffic patterns in Ukraine since February 21, 2022," 2022. [Online]. Available: https://blog.cloudflare.com/internet-traffic-patterns-in-ukraine-since-february-21-2022

[19] M. Prince, "Steps we've taken around Cloudflare's services in Ukraine, Belarus, and Russia," 2022. [Online]. Available: https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/

[20] C. Trusin, L. Bertholdo, and J. J. Santanna, "The Effect of the Russian-Ukrainian Conflict from the Perspective of Internet eXchanges," in *International Conference on Network and Service Management (CNSM)*, 2022, pp. 261–267.

[21] E. Aben, "How is Russia connected to the wider Internet?" 2022. [Online]. Available: https://circleid.com/posts/20220329-how-is-russia-connected-to-the-wider-internet

[22] J. Tome, D. Belson, and K. Berdan, "One year of war in Ukraine: Internet trends, attacks, and resilience," 2022. [Online]. Available: https://blog.cloudflare.com/one-year-of-war-in-ukraine

[23] R. Singla, S. Srinivasa, N. Reddy, J. M. Pedersen, E. Vasilomanolakis, and R. Bettati, "An analysis of war impact on Ukrainian critical infrastructure through network measurements," in *Network Traffic Measurement and Analysis Conference (TMA)*. IEEE, 2023, pp. 1–10.

[24] Google Threat Analysis Group, "Fog of war: how the Ukraine conflict transformed the cyber threat landscape." [Online]. Available: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

[25] RIPE NCC, "The RIPE NCC and Ukraine/Russia," 2022. [Online]. Available: https://www.ripe.net/membership/member-support/the-ripe-ncc-and-ukraine-russia/

[26] E. Carisimo, A. Gamero-Garrido, A. C. Snoeren, and A. Dainotti, "Identifying ASes of State-owned Internet Operators," in *ACM IMC*, 2021.

[27] U. Yacobi-Keller, E. Savin, B. Fabian, and T. Ermakova, "Towards Geographical Analysis of the Autonomous

System Network," *Int. J. Netw. Virtual Organisations*, vol. 21, no. 3, 2019.
[28] M. Ziv, L. Izhikevich, K. Ruth, K. Izhikevich, and Z. Durumeric, "ASdb: a system for classifying owners of autonomous systems," in *ACM IMC*, 2021.
[29] CAIDA, "Inferred AS to Organization Mapping Dataset." [Online]. Available: https://www.caida.org/catalog/datasets/as-organizations/
[30] RIPE NCC, "RIPEstat UI," https://stat.ripe.net/app/.
[31] PeeringDB, "PeeringDB: The Interconnection Database," https://www.peeringdb.com/.
[32] Hurricane Electric, "Internet Exchange Report," https://bgp.he.net/report/exchanges.
[33] PCH, "Packet Clearing House," https://www.pch.net/.
[34] Internet Archive, "Internet Archive Wayback Machine." [Online]. Available: https://web.archive.org/
[35] Euro-IX, "IXP Database." [Online]. Available: https://ixpdb.euro-ix.net/en/
[36] V. Giotsas, G. Smaragdakis, B. Huffaker, M. Luckie, and kc claffy, "Mapping Peering Interconnections at the Facility Level," in *Proceedings of ACM CoNEXT 2015*, Heidelberg, Germany, December 2015.
[37] CAIDA, "AS-relationship Dataset." [Online]. Available: https://publicdata.caida.org/datasets/as-relationships/serial-1/
[38] RIPE NCC, "RIPE Atlas," https://atlas.ripe.net/.
[39] T. Heichenko, "Citizenship of resources," *RIPE 87*, 2023. [Online]. Available: https://ripe87.ripe.net/wp-content/uploads/presentations/60-H-ASN_citizenship.pdf