Analysing Internet route changes related to the Russia-Ukraine war using BGP historical data

ROMAN KHAVRONA, University of Twente, The Netherlands

Wars and conflicts between independent states cause major shifts in policies between them. The progress of the Internet in the last 20 years made it a part of war and policies countries use to influence each other's Internet traffic. The Russia-Ukraine war that started on February 24, 2022 is no exception and had a significant impact on Internet routing. In our research, we focus on Internet route changes in Ukraine and Russia using Border Gateway Protocol (BGP) historical datasets in the time leading up to the war and during the Russia-Ukraine conflict in 2022. To do this, we used the BGPStream open-source framework for BGP data analysis. After performing the research, we could see the huge impact of the war on Ukraine and especially on those cities located close to Russia. We also observed an impressive cyber response from parties that fight on the Ukrainian side that either slowed down or completely disabled Russian online services. Lastly, we showed the general trend of isolation of Russia caused by the sanctions imposed on it for its unjustified invasion of Ukraine.

Additional Key Words and Phrases: Russia-Ukraine war, BGP, AS, IP address, network prefix

1 INTRODUCTION

Besides the horrible impact of war on people's lives, it also impacts major shifts in policies between conflicting states. Since the Internet has become inherently important in the last 20 years, unfortunately, it has become a part of war too. Hostile countries perform cyber-attacks on each other, but also apply Internet routing changes to reconfigure their network traffic. This is also the case in the Russia-Ukraine conflict that started in 2014. Russia annexed Crimea from Ukraine and tried to change the Internet routing on the peninsula. It took Russia 3 years to mainly centralize its routing from Crimea through Russia's mainland even at the cost of decreased performance [10]. Not only the traffic was altered in Crimea, but also in other regions of Ukraine. Scientists from the University of Paris, Columbia University and the University of Savoie-Mont-Blanc conducted experiments to prove that [9]. To kick off their research, they sent a traceroute from Dnipro (an eastern city under Ukrainian control) to the capital of Russia - Moscow. As a result, the traceroute did not follow the shortest path through the Donbas (an occupied territory by Russian separatists) war front line in the East of Ukraine but instead travelled through 11 hops along Hungary and Austria (or Poland and Czechia), Germany, Poland, Belarus and finally Russia (see Figure 1). In addition, the researchers sent a traceroute from within the territory controlled by separatists - the unrecognised so-called Donetsk People's Republic - to show the existence of a digital front line in Ukraine. The routing time was 6 times faster than of the traceroute sent from Dnipro and instead of 11 hops only 3 were needed to reach the Moscow's network. The complex path of the packet sent from Dnipro resembles the non-optimal routing of Russian airplanes due to the closed air space by European countries after the invasion of Ukraine in 2022.

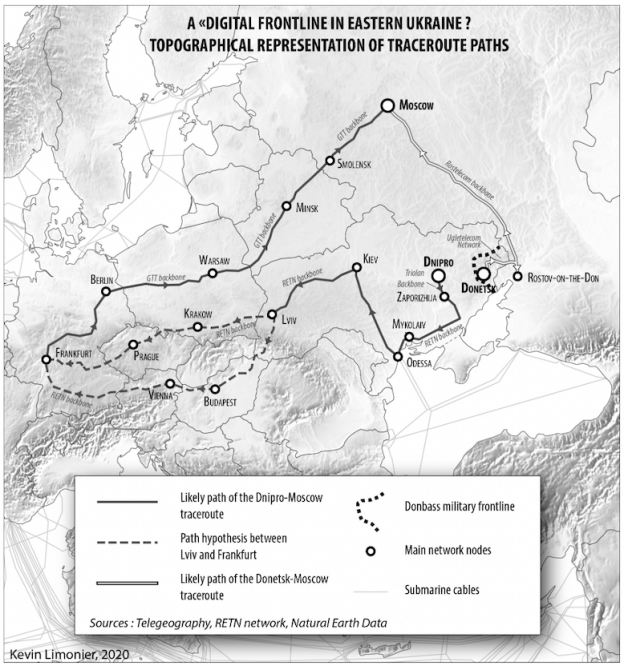

Fig. 1. Topological representation of traceroutes [9]

On the 24th of February 2022, Russian forces invaded Ukraine again, this time officially announcing a full-scale invasion. The United Kingdom's Defence Ministry claimed that the Russian army inflicted significant damage to the country's infrastructure and Internet access was most likely disrupted [14]. The biggest Ukrainian networking company Ukrtelecom reported that Russian airstrikes caused huge damage to its telecommunications [24]. Supporting the above, the Cloudflare content delivery network company reported significantly lower traffic in the first days of the war [3]. Moreover, Cloudflare announced that their data center located in Kyiv was a victim of a large DDoS attack. However, the automatic defense system of the company was able to solve problems by routing incoming packets onto other networks. Not only Ukrainian networks but also Russian governmental and bank websites were a target of massive DDoS attacks [11]. This suggests that there were major network changes in 2022, similar to those that were caused by the Russian invasion of Donbas and Crimea in 2014. **Therefore, our main research goal was to analyse Internet route changes**

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

in Ukrainian and Russian networks caused by the Russian invasion in 2022.

In our research, we performed an analysis of Ukrainian and Russian networks to explore Internet route changes and to relate those changes with major events of the Russia-Ukraine war, both in the real and the cyber world. To achieve our goal we analysed historical BGP data using the BGPStream tool. The reason for choosing BGP was due to its irreplaceable role in the definition of routing paths between Autonomous Systems (ASes) [20]. We defined experiments to analyse the Internet route changes in Ukraine and Russia. Firstly, we analysed BGP UPDATE messages and their frequencies. Then, we analysed prefixes' origin AS changes and announcements of subnets of network blocks. The last experiment was the analysis of possible AS path increase caused by the war.

The remainder of the paper is organised as follows: in section 2, we explain what BGP and route collectors are and discuss the selection of route collectors for this research. In section 3, we discuss the datasets we used to conduct our research. Then, we describe our approach and discuss the results of our experiments.

2 BACKGROUND

2.1 BGP

The Internet routing between ASes is dependent on BGP [20]. ASes send UPDATE messages using the BGP to inform each other about changes in their local network prefixes or prefixes learned from their neighbours [15]. Based on the UPDATE messages and local policies, each BGP router maintains the local state about reachability of other network locations. That local state is called the Routing Information Base (RIB) [15].

Hardware equipment failures or reconfigurations may trigger new BGP UPDATE messages being sent between ASes [20]. Reconfigurations (import and export policies) may include addition, deletion or modification of BGP advertisements [2]. As a result, topology changes may impact the routers within ASes such that they select new BGP paths [20]. Since some operators make the information from self-owned routers public for research purposes, we took this opportunity to study the historical BGP data that may give important insights and views into the Russia-Ukraine war in 2022 [15].

Firstly, it can show the urgent need for a change of BGP routes to defend against cyberattacks. For instance, enabling blackhole routes that drop incoming packets that are sent to the targeted IP addresses or specifying more specific prefixes out of larger network blocks [2, 4, 25]. Secondly, the change of routing in Ukraine may be a signal of destroyed infrastructure in cities. Last but not least, the BGP data from the war period can demonstrate applied Internet policies or imposed sanctions not only by Ukraine and Russia but also by neighbouring countries.

2.2 BGP route collectors

The main goal of BGP route collectors is to gather information about routing within the networks [13]. BGP collectors do not forward or broadcast information, but rather collect and create a public perspective on the global routing in the Internet. The pieces of information that BGP collectors are receiving are called BGP UPDATE messages

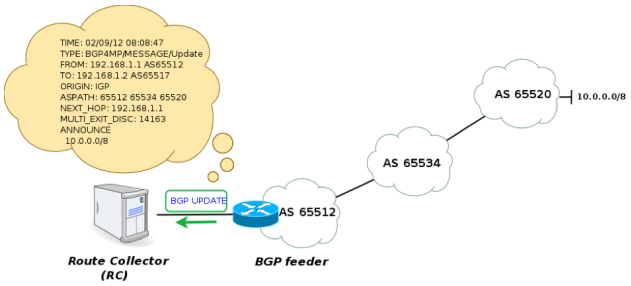

Fig. 2. The example of BGP route collector receiving UPDATE message from its peer [23]

[15, 23]. Those BGP UPDATE messages are sent from the set of established peers who advertise the new best routing paths that were established through peering with other routers (see Figure 2) [23]. Each of the route collectors forms the RIB that is periodically dumped [15]. For our research, we used the RIPE Routing Information Service (RIS) collection of historical routing data, where the RIBs are dumped every 8 hours [21].

For our research, we chose 3 RIPE RIS route collectors that are located in Amsterdam (RRC00), Moscow (RRC13) and Bucharest (RRC22) [22]. The reason for choosing collectors in Moscow and Bucharest is that those two are located closest to Ukraine among all the available collectors of RIPE. For these two collectors, the collection of the data is happening at Internet exchange points (IXPs) peering LANs where those collectors are physically attached [22]. Hence, we can get a local rather than a global impression from these two collectors. We also decided to pick a route collector located in Amsterdam because this city is a very important Internet hub in Europe. Moreover, the BGP collector located in Amsterdam is multihop and so collects data from peers located all around the world and gives a global rather than a local view.

3 DATASETS

3.1 RIPE database of network prefixes

Prior to the analysis of the BGP historical data, we had to find network prefixes in both Ukraine and Russia. For that, we used the publicly available RIPE IP address allocations database [18]. This database contains the IP allocations of IPv4 and IPv6 networks located all around the globe. Each network IP allocation record has a country attribute and so that is how we filtered out the rest of the networks from Ukrainian and Russian allocations. For the IPv4 network allocations, we had to perform an additional step since the network allocations were stored as ranges of IP addresses rather than in CIDR notation. We converted those ranges to CIDR format so we could use them further in our research.

3.2 BGPStream framework

We used the BGPStream tool that is intended for live and historical BGP data analysis. Since for our research we wrote code in Python, we used the PyBGPStream Python package that has bindings to the native libBGPStream library written in C.

There were several PyBGPStream filtering options we could use to filter BGP historical data such as:

(1) Start and end date of BGP records.
(2) Collection points (BGP collectors).
(3) Record types, either RIB dumps or received UPDATE messages [15]
(4) Additional filters, such as a peer from which the BGP messages were received or a network prefix that was mentioned as the destination point of BGP messages.

In our research, we filtered data on the first 3 filters, but not the last one because of the long stream initiation time for each prefix we wanted to get data about. Therefore, we used the py-radix Python library that implements the radix tree structure to build up the tree of prefixes. It gave us the chance to only initiate the stream once and filter on a timeframe, collection points and record types.

4 APPROACH

4.1 BGP UPDATE messages

The first step of our research was to compare frequencies of BGP UPDATE messages that contained destination network prefixes located in Ukraine and Russia. This approach is informative since the analysis of BGP UPDATE messages is a good tool to analyse Internet routing dynamics [15]. The number of BGP UPDATE messages may change on a daily or hourly basis but still should follow a similar pattern if there are no anomalies. To inspect it, we counted BGP UPDATE messages on a daily basis from the 1st of February to the 30th of April in both 2021 and 2022. The reason for analysing the previous year's data was to prove that the changes that were happening in Ukraine and Russia in 2022 were not usual BGP message exchanges. We also expected that the countries located far from the conflict area should not be hugely affected by the war events in Ukraine. That is why we picked Italy as an extra measure to show the significance of the war's impact on both Ukraine and Russia. We expected that there would be unusual changes in Ukraine and Russia, while the frequencies of BGP UPDATE messages regarding Italian network prefixes would stay at the same level.

4.2 BGP RIBs

4.2.1 Prefixes and their origin ASes. The next step we performed was the analysis of the changes of prefixes' origin ASes. The origin changes are a rare event and happen sometimes in the case when some ASes cannot host their network prefixes anymore and need temporary or permanent help from other ASes. We analysed network prefixes and their origin ASes on a daily basis from the 1st of February to the 30th of April in 2022. For each day we compared the origin ASes of each prefix with the previous day. If there was any change, we added *1* to the total number of changes of the day. This approach is informative since the rapid peaks in the data are unusual. Again, Italy was picked as a baseline country that should not have any anomalies.

4.2.2 Prefixes and their subnets. In this subsection, we discuss our analysis over 3 months time from February to the end of April of Ukrainian, Russian and Italian prefixes and the number of their subnets. As for previous approaches, Italy was chosen as a country that would help to show the impact of the war on both Ukraine and Russia as most likely Italy would not have any detected anomalies. For each day we compared each prefix's subnet count with the previous day. Then, we summed up all the differences on a daily basis for the aforementioned time frame. The event when new subnets are announced is not that uniquely rare, but also should not have definite rapid increases if there are no events that evoke such changes.

A massive or highly increased number of newly announced subnets may be linked to the cyberattacks performed on the countries' services as the victims have to announce more specific prefixes to still make some of the services available. We inspected the Russian military website mil.ru and were able to see that during the first days of the war there were many more specific prefixes announced probably to counter massive DDoS attacks.

4.2.3 Path inflation. The last step of our research was to analyse the Internet path inflation. No doubt, even before the war there were already Internet path inflations in the world because of the applied policies by different countries. We assumed that the path inflation should dramatically increase to those IP addresses located in Russia as part of the policies against the Russian invasion in 2022. We expected to see a significant increase in inflation after the start of the war in Ukraine too because of infrastructure damage, cyberattacks, and also because some of the territories were captured by Russians. For Italy, we expected to not have a path inflation increase as it is located rather far from the conflict area.

For each prefix located in Ukraine, Russia and Italy we counted the number of unique ASes leading to them from the set of established peers of BGP route collectors. Then, we summed up all of them on a daily basis from the 2nd of February to the 30th of April and compared them with the 1st of February. We did not do the same as for previous BGP RIBs approaches where we compared changes day by day since in this one we were interested in when the inflation increased and how long it lasted, rather than when the inflation changed.

5 RESULTS

5.1 BGP UPDATE messages

For the time frame from the 1st of February to the 30th of April in 2021, there were only slight changes and if they occurred, they were rather smooth in all three countries. In contrast, in 2022 there were a few huge spikes for both Russia and Ukraine (see Figure 3). For Ukraine, the huge spike was on the 24th of February, the official start of the war in 2022, and in the period from the 19th to the 23rd of March. For Russia, the enormous spike was on the 27th of February and for Italy, as expected, there were no unusual changes.

We looked in more detail (on an hourly basis) at the period from the 23rd to the 28th of February to investigate those peaks for Ukraine and Russia. The first interesting thing to notice was the extreme local peak for Russia between 22:00 UTC and 23:00 UTC on the 23rd of February and so before the official start of the war that happened a few hours later. We found that the four most affected ASes which were the destinations of BGP UPDATE messages were AS3216, AS12418, AS35048 and AS31514. AS3216 is PJSC "Vimpelcom" and most of its IP addresses are located in Moscow. AS12418

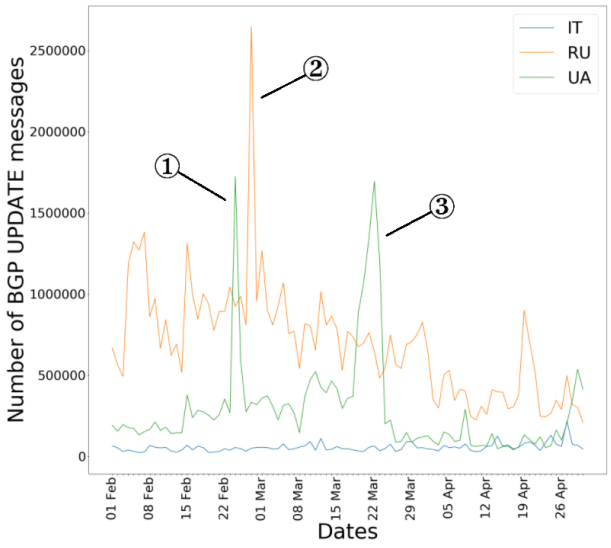

Fig. 3. The number of BGP UPDATE messages regarding Ukrainian, Russian and Italian network prefixes from 1st of February to the 30th of April in 2022

has some IP allocations in Moscow, Vladimir, Nizhny Novgorod and most of its allocations in Saint Petersburg. For AS35048 most of the IP addresses are located in Zelenograd and for AS31514 in Korolyov. Both of these cities are located less than 50 kilometers from Moscow city. In order to get a complete picture of which cities were destinations of BGP UPDATE messages, we determined the locations of destination network prefixes and plotted a heat map of frequencies of BGP UPDATE messages. Unfortunately, it was impossible to get the exact latitude and longitude of IP prefixes because those are ranges of many IP addresses usually located in adjacent places. However, the IP addresses from a range still usually belong to the particular city and hence were still relevant for us. We decided to pick the first IP address of the prefix range to find the approximate coordinates of each network. After plotting the heat map, what we saw was that many Russian cities were affected, but the significant changes were only regarding network prefixes located in Moscow and Saint Petersburg. This mainly shows that Russian main services and IP ranges are located on the Western front of the country and those changes may have been preparations for the digital war with other countries.

We also noticed a local peak for Ukraine from 22:00 UTC on the 23rd of February to 01:00 UTC on the 24th of February. The reason for this peak may be linked to the reports about Russian cyberattacks performed on Ukrainian networks [5]. Researchers at security company ESET reported numerous cyberattacks that were launched shortly before the start of the war and described that those attacks were aimed at erasing the contents of the hard drives of affected computers. There were also reports about massive DDoS attacks on the news, banking and government departments' websites on the 23rd of February shortly before the start of the invasion [7].

The next increase in the number of BGP UPDATE messages in Ukraine began from the start of the war and ended on the 25th of February (see ① in Figure 3). The most probable reason for that is the damage to Ukrainian infrastructure and cyberattacks performed on Ukrainian networks ([14]). Those cyberattacks included attacks on news and governmental websites and malware attacks such as "AcidRain" or "IsaacWiper" [7]. The "AcidRain" attack was aimed to disable modems that communicate with the Viasat satellite, which provides Internet access to the citizens of Ukraine, and "IsaacWiper" was aimed at recursively wiping each file of a hard drive of the affected machine [7, 19].

To get more insight into the affected cities, we determined the locations of network prefixes located in Ukraine and created heat maps of frequencies of BGP UPDATE messages from the 20th of February to the 5th of March. The most significant changes were on the 24th of February, 27-28th of February and 3-4th of March (see Figure 4).

On the 24th of February, the day of the invasion of Russian forces, the increase of BGP UPDATE messages was spotted in all the parts of Ukraine. But, the most significant increase happened in Kyiv, Poltava, Kharkiv, Dnipro, Zaporizhzhia, Kherson and Odesa. Kharkiv is located very close to the Russian border in the North East of Ukraine and was one of the earliest attacked cities on the day of the invasion. Therefore, we think that the most probable reason for the significant increase of BGP UPDATE messages regarding network prefixes located in Kharkiv was due to infrastructure damage. Most likely the same reason applies to Kherson, which is located North of the annexed Crimea peninsula. However, as was already mentioned, Ukraine suffered from DDoS attacks and this factor, without a doubt, is one of the main causes of changes in the frequency of BGP UPDATEs regarding all the Ukrainian prefixes.

On the 27-28th of February, in addition to a few previously mentioned cities, we could see that there were significant route changes in Sumy and Mariupol. Most likely that was due to the intensified assault on those cities that resulted in destroyed infrastructure. We could also identify that Donetsk, occupied by Russia since 2014, was a place of change. We are unsure about the possible reasons for those changes, but our assumption is that European network providers were adopting some policies regarding Donbas prefixes on those days.

On the 3-4th of March, the new cities that experienced Internet changes were Lviv, Uzhhorod and Severodonetsk. Both Lviv and Uzhhorod are located far from the war events in the Western part of Ukraine. That is why we think that the changes there were linked to the applied policies of the aggressor. Severodonetsk is located rather close to the war front line in eastern Ukraine, but we still assume that changes regarding prefixes located in that city were mainly due to changes in policies of Russian peers. This is due to the fact that there were no heavy fights yet in Severodonetsk on the 3-4th of March. To prove that those BGP UPDATE messages were produced by Russian peers on the 3-4th of March, we chose only Moscow's BGP collector with most of its peers located in Russia and calculated the BGP UPDATE messages regarding Ukrainian network prefixes for those two days again. After comparing the BGP UPDATE messages count between three collectors and the one located in Russia, we saw that 82% of UPDATE messages on the

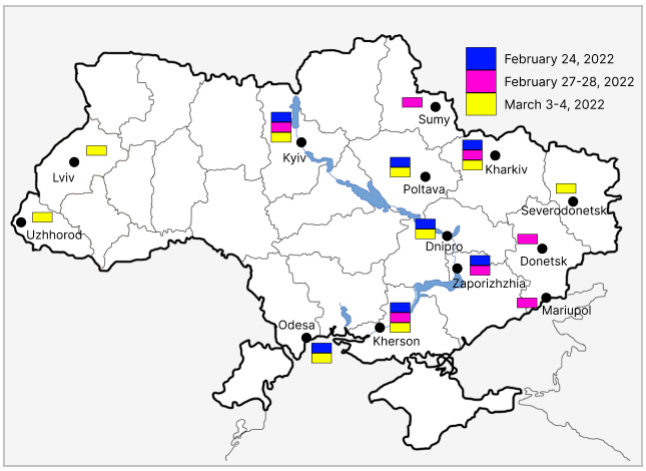

Fig. 4. Most affected cities in Ukraine in the period from 20th of February to 5th of March according to the results of the *BGP UPDATE messages* approach

3-4th of May were sent by Russian peers, while only 18% from peers from Romanian collector and peers from multihop collector located in Amsterdam.

The highest peak among all the detected changes was found in Russia on the 27th of February (see ② in Figure 3). One and probably the main reason for this huge peak is the numerous cyber-attacks performed against Russian network services. IT ARMY of Ukraine, BlackHawk, Anonymous and many other organisations helped Ukraine in the cyber war against the aggressor [17]. IT ARMY of Ukraine posted many screenshots indicating that many Russian services and websites such as mil.ru, kremlin.ru, sberbank.ru were DDoSed and so were not responding for at least a few days. Anonymous leaked a tremendous amount of data related to Russian governmental and military services. During the early days of the war, they breached and leaked the database of the aforementioned Russian Ministry of Defence website mil.ru [12]. Hence, we think that the data breaches and DDoS attacks resulted in major Internet route changes regarding Russian network prefixes on the 27th of February.

The last time frame we investigated using the approach of calculating BGP UPDATE messages was from the 19th to the 23rd of March (see ③ in Figure 3). This increase may be connected to the fact that Russian forces were close to Kyiv, Kharkiv, Mykolaiv, Severodonetsk, Izium and other cities and were damaging lots of infrastructure. There were also many Russian cyberattacks performed on TV networks, popular media and enterprises using DDoS, malware and phishing techniques [7].

5.2 BGP RIBs

5.2.1 Prefixes and their origin ASes. As a result of performing this approach, we could see that Italy, as expected, did not have unusual changes. In contrast, there were enormous peaks for Ukraine and some high peaks for Russia (see Figure 5). For Ukraine, those enormous peaks happened on the 24th of February and from the 1st to the 4th of March. There were also some unusual changes in Ukraine from the 10th to the 14th of March and from the 24th to the 26th of March. While we already discussed the possible reasons for changes during the first week of the war, we will further analyse the time frames for Ukraine in March. Russia also had some higher peaks from the 1st to the 5th of March and some less significant peaks at the end of March and in April.

We will firstly discuss the time frame for Ukraine from the 1st to the 5th of March (see ② in Figure 5). We determined the city locations of prefixes that suffered changes in their origin AS/ASes. On the 1st of March, we could count around 50 prefix origin AS changes in Kharkiv. We think that the most probable reason for that is very heavy bombings of the city that even included missile attack on Kharkiv Regional State Administration [28]. Kharkiv was the most affected city based on the results of this approach and got a peak of changes in prefixes' ASes on the 4th of March. This links to the results we got from *BGP UPDATE messages* approach, where we plotted heat maps of frequencies of BGP UPDATE messages and saw that Kharkiv was significantly affected on the 3-4th of March. As we could identify, Kherson, Mykolayiv, Mariupol, Sumy, Donetsk, Irpin, Kyiv and some other cities were affected too. Quite possibly, the reasons for changes in Kherson, Mykolayiv, Mariupol, Sumy, suburban city of Kyiv - Irpin and Kyiv itself were heavy fights in or around those cities, when Russian pressure was at its peak in the North and South directions of Ukraine. We noticed that the significant increase of changes in Mykolaiv happened on the 3rd of March and this links up to the fact that Russian forces were heavily attacking that city after getting control over Kherson at the start of March. Except for physical damage, on the 5th of May Ukraine's State Service of Special Communications and Information Protection claimed that Russian digital forces were performing huge DDoS attacks on Ukrainian services on a daily basis [1].

The next time frames to analyse were from the 10th to the 14th of March and from the 24th to the 26th of March (see ④ and ⑤ in Figure 5). Around the first time range, Russian forces were trying to capture Kyiv from both Western and Eastern parts and in the Western part they were able to occupy parts of the M06 highway that links Kyiv and Zhytomyr. They also partially surrounded Mykolaiv and Mariupol. Overall, during that time very many Ukrainian cities were heavily bombed. On top of the physical damage, there were numerous cyberattacks performed on Ukrainian services in mid-March. On the 16th of March, TV Station Ukraine 24 was hacked to broadcast a ticker that displayed information that the President of Ukraine urged Ukrainians to stop fighting and surrender [7]. On the same day, the deep fake video of the Ukrainian president was posted with the same appeals to surrender. On the 17th of March, the Security Service of Ukraine reported via Telegram that there was a large-scale cyber attack performed on Ukrainian popular media websites [6, 7, 26]. During the same day, the Ukrainian Ministry of Defense notified about large phishing attacks aimed at government and military entities.

We could not find any information about cyberattacks performed during the time frame for Ukraine from the 24th to the 26th of March. But we observed that there were intense fights in the Izium direction and liberation fights in the Kyiv region. So, probably physical damage resulted in some prefixes being hosted partially or fully by other ASes at the end of March.

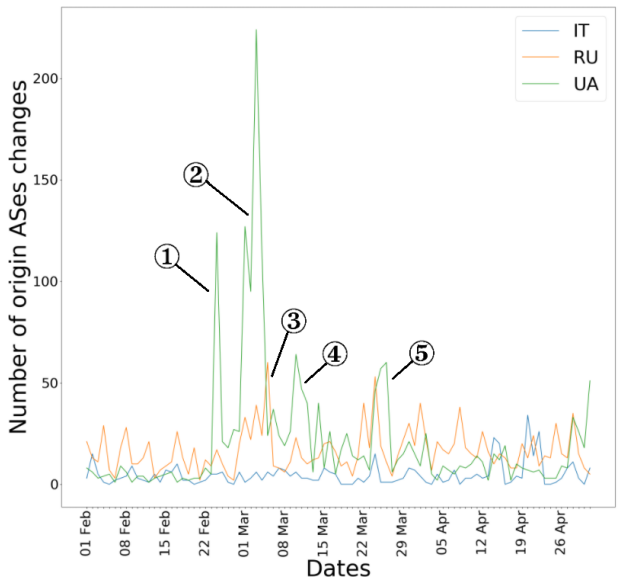

Fig. 5. The number of prefixes' origin ASes changes from the 1st of February to the 30th of April in 2022

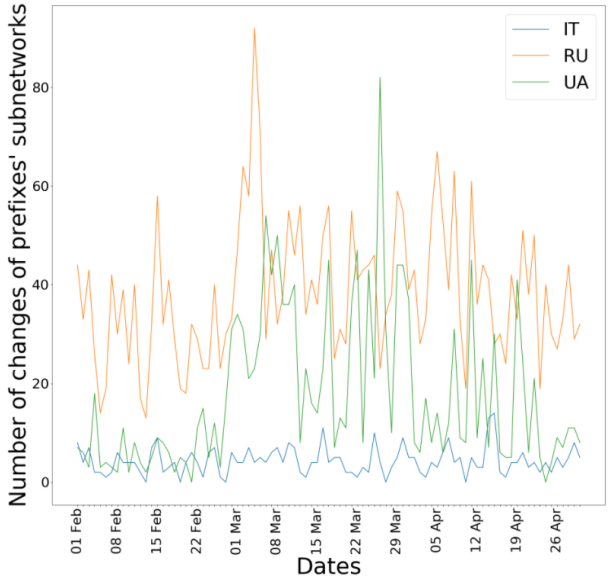

Fig. 6. The number of changes of prefixes' subnets from the 1st of February to the 30th of April in 2022

For Russia, the first time frame to discuss is the range from the 1st to the peak on the 5th of March (see ③ in Figure 5). We believe that the reason for that is the hacker attacks performed a few days after the start of the war by many different organisations that declared digital war on Russia. On the 3rd of March, Reuters posted that a new set of online targets were set in Russia that included a homegrown satellite-based navigation system, GLONASS [16]. Moreover, on the 5th of March Anonymous claimed that the Federal Security Service (FSB) websites of Russia were taken down by their organisation [1]. They also claimed that they had already taken down 2500 websites in Russia and Belarus as support in the digital war against the aggressor.

There were more peaks in Russia as can be seen in Figure 5, but they were on average less significant and we leave their analysis for future work.

5.2.2 Prefixes and their subnets. As discussed in 4.2.2, rapid increase in newly announced subnets may be linked to the cyberattacks performed on the countries' online services as the victims may announce new subnets to recover some of their services.

From the results of this approach we can see that Italy did not experience any significant changes (see Figure 6).

For Ukraine, we can see huge spikes starting from the 28th of February and became lower on average starting from April. This may be linked to the fact that Russian troops started withdrawing from the Kyiv and Chernihiv directions in the end of March and fully withdrawn at the start of April [8, 27].

For Russia, we can see peaks during the first half of March. This perfectly links to the report of the Rostelecom-Solar, cybersecurity part of the largest Russian digital provider Rostelecom, that an enormous amount of cyberattacks was performed on Russian websites at the start of March, with the number of DDoS attacks already exceeding those performed in February [1]. They also reported that many governmental companies were attacked including Kremlin, Aeroflot airlines and Sberbank banking websites. Hence, it could be that Russian network operators were defining subnets to recover some services as fast as possible.

5.2.3 Path inflation. We can see that the inflation increase can be observed in Ukraine starting from the 24th of February (see Figure 7). On the 3rd and 4th of March, the path inflation had already tripled in comparison with the first day of the war. We can observe two very high peaks on the 10th and 14th of March and very high and rather long peaks from the 16th to the 31st of March. Following that, we can see a significant drop during the start of April. We think the main reason for that significant change, as lines up with the discussions in *Prefixes and their subnets* approach, is that Russian forces withdrew from Kyiv and Chernihiv directions around the start of April [8, 27]. The selection of Italy in this approach helps to outline the severe consequences of the invasion of the aggressor in Ukraine, as we do not see any inflation increase regarding Italian prefixes.

The line representing path inflation change towards Russian IP networks in Figure 7 shows the overall attitude of the world towards the cruel and unjustified invasion of Russian forces. We can see that the inflation starts growing more and more starting from the end of February. In comparison with Ukraine, we can see that the inflation towards Russian IP network addresses only rose on average and did not fall back. We are sure that this is linked with the fact that more and more policies were and, during the time of writing this article, are being introduced against Russia.

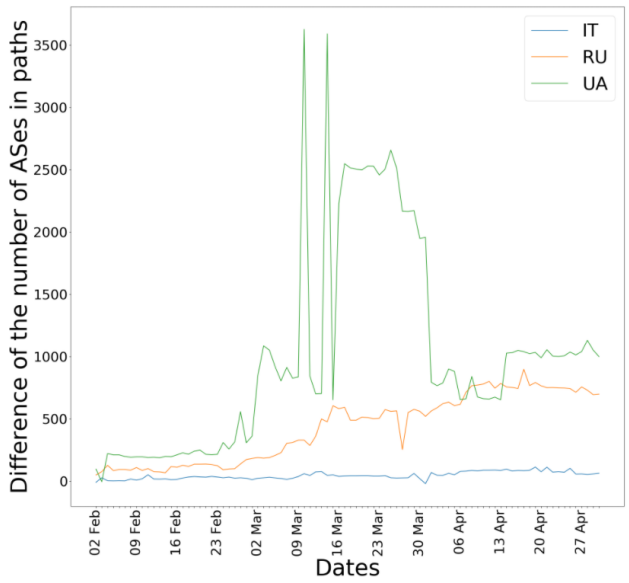

Fig. 7. Difference in the number of ASes in paths regarding Ukrainian, Russian and Italian prefixes from the 2nd of February to the 30th of April in comparison with the 1st of February

6 CONCLUSION

In our research, we analysed the Internet route changes in Ukraine, Russia and Italy. While the first two countries are direct participants of the war, Italy was picked as a neutral country to ensure that the results we get for Ukrainian and Russian networks are not a coincidence and usual BGP routing processes. The selection of Italy also helped us to show the huge impact of the war on Ukraine.

In the *BGP UPDATE messages* approach we could see that in almost all Ukrainian cities there were Internet route changes, but especially significant in Kyiv, Kharkiv, Sumy, Kherson, Mariupol, Severodonetsk, Poltava, Dnipro, Zaporizhzhia and Odesa. We could also see that on the 3rd and 4th of March there were many Internet route changes regarding the IP network allocations located in Lviv and Uzhhorod in the Western part of Ukraine.

During the analysis of this approach, we could also see an enormous amount of BGP UPDATE messages regarding Russian network prefixes on the 27th of February. We believe that the reason for this are the cyberattacks performed by a variety of different hacker and cyber volunteer groups, most notably by the IT ARMY of Ukraine and Anonymous. Moreover, we could see local peaks in Russia even before the start of the war. This may show that Russia made its last preparations before the war that included Internet route changes within their networks. There were also some changes regarding Ukrainian prefixes slightly before the start of the war. This perfectly links up with the reports of cyberattacks performed on Ukrainian networks shortly before the 24th of February.

We also analysed RIBs of BGP collectors. According to the results of the *Prefixes and their origin ASes* approach, we could see significant changes in Ukrainian networks at the start day of the war and also enormous changes at the start of March. After performing a few additional steps to determine prefixes' locations, we could see that very many Ukrainian cities that are located close to the Russian border were most strongly affected. The biggest changes at the start of March were detected in Kharkiv as this city was heavily bombed at that time. We also identified significant changes in Russia that were most likely caused by the massive cyberattacks performed on Russian networks.

The *Prefixes and their subnets* and *Path inflation* approaches of the analysis of BGP RIBs showed the effect of the war on both Ukraine and Russia. In these approaches we could see that enormous changes for Ukraine started in February and decreased more by than half in April. We believe the reason for that decrease in April is caused by the withdrawal of Russian forces from the North of Ukraine. In the *Path inflation* approach we also saw that the Internet path inflation towards Russian prefixes was accumulating more and more. This clearly shows the attitude of the world towards the criminal acts of the Russian government and military.

7 FUTURE WORK

By the time of writing this article, the war was at its peak in the eastern part of Ukraine. During the three-month time we analysed, we could see the huge impact of the war on Ukraine and Russia. But, we will probably see more and more interesting patterns of Russian networking changes as the war progresses to the later stages and more sanctions will be applied against the aggressor. So, the first and most important extension of our research may be the analysis of each subsequent month after April 2022. This will likely provide us with more information on routing changes in the occupied territories of Ukraine as a consequence of new policies implemented by Russia there. Moreover, it may be the case that more and more Ukrainian territories will be liberated and as a result, we may be able to notice many new routing changes regarding Ukrainian prefixes.

The other aspect that can be part of the future work of this research is the analysis of traceroutes. As discussed in the section 1, some researchers already used this method as the initial step of their research to analyse Internet route changes in Ukraine after the start of the conflict in 2014. To get a more visual representation of the Internet route changes caused by the Russia-Ukraine war in 2022 one can plot similar maps to Figure 1.

REFERENCES

[1] Cynthia Brumfield. 2022. Russia-linked cyberattacks on Ukraine: A timeline. Retrieved June 20, 2022 from https://www.csoonline.com/article/3647072/a-timeline-of-russian-linked-cyberattacks-on-ukraine.html?page=2
[2] Matthew Caesar and Jennifer Rexford. 2005. BGP routing policies in ISP networks. *IEEE network* 19, 6 (2005), 5–11.
[3] John Graham-Cumming. 2022. Internet traffic patterns in Ukraine since February 21, 2022. Retrieved April 30, 2022 from https://blog.cloudflare.com/internet-traffic-patterns-in-ukraine-since-february-21-2022/
[4] Nico Hinze, Marcin Nawrocki, Mattijs Jonker, Alberto Dainotti, Thomas C Schmidt, and Matthias Wählisch. 2018. On the potential of BGP flowspec for DDoS mitigation at two sources: ISP and IXP. In *Proceedings of the ACM SIGCOMM 2018 Conference on Posters and Demos*. 57–59.
[5] Frank Hofmann. 2022. The hybrid war that began before Russia invaded Ukraine. Retrieved June 19, 2022 from https://www.dw.com/en/hybrid-war-in-ukraine-began-before-russian-invasion/a-60914988
[6] Slovo i Dilo. 2022. The SBU reported a massive hacker attack on the sites of popular online publications in Ukraine. Retrieved June 20, 2022 from https://www.slovoidilo.ua/2022/03/17/novyna/suspilstvo/sbu-povidomyla-pro-masovu-xakersku-ataku-sajty-populyarnyx-onlajn-vydan-ukrayini

[7] CyberPeace institute. 2022. UKRAINE: Timeline of Cyberattacks on critical infrastructure and civilian objects. Retrieved June 19, 2022 from https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/

[8] Dan Lamothe Karoun Demirjian. 2022. Pentagon: Russia has fully withdrawn from Kyiv, Chernihiv. Retrieved June 20, 2022 from https://www.washingtonpost.com/national-security/2022/04/06/pentagon-russia-withdraws-kyiv-chernihiv/

[9] 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* 26, 5 (2021).

[10] Sebastian Moss. 2022. How Russia took over the Internet in Crimea and Eastern Ukraine. Retrieved April 30, 2022 from https://www.datacenterdynamics.com/en/analysis/how-russia-took-over-the-internet-in-crimea-and-eastern-ukraine/

[11] Sebastian Moss. 2022. Russian government websites go down after country invades Ukraine. Retrieved April 30, 2022 from https://www.datacenterdynamics.com/en/news/russian-government-websites-go-down-after-country-invades-ukraine/

[12] Metro News. 2022. Anonymous leaks Russian MoD database in major victory during cyberwar. Retrieved June 19, 2022 from https://metro.co.uk/2022/02/26/anonymous-leaks-russian-mod-database-in-major-victory-during-cyberwar-16179039/

[13] MDC Newsroom. 2020. The difference between a route collector a route server. Retrieved June 18, 2022 from https://www.mdcdatacenters.com/company/blog/the-difference-between-a-route-collector-a-route-server/

[14] Mauro Orru. 2022. U.K. Sees Russian Strikes Disrupting Ukraine's Internet Access. Retrieved April 30, 2022 from https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-07/card/u-k-sees-russian-strikes-disrupting-ukraine-s-internet-access-4eJQ7fs7aAhEfb0ExBn5#:~:text=Internet%20access%20in%20Ukraine%20is,the%20last%20week%2C%20it%20said.

[15] Chiara Orsini, Alistair King, Danilo Giordano, Vasileios Giotsas, and Alberto Dainotti. 2016. BGPStream: a software framework for live and historical BGP data analysis. In *Proceedings of the 2016 Internet Measurement Conference*. 429–444.

[16] James Pearson. 2022. Ukraine's 'IT army' targets Belarus railway network, Russian GPS. Retrieved June 20, 2022 from https://www.reuters.com/world/europe/ukraines-it-army-targets-belarus-railway-network-russian-gps-2022-03-03/

[17] SOCRadar Platform. 2022. What You Need to Know About Russian Cyber Escalation in Ukraine. Retrieved June 19, 2022 from https://socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/

[18] RIPE registry. 1992. RIPE database. https://ftp.ripe.net/ripe/dbase/split/

[19] ESET Research. 2022. IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine. Retrieved June 19, 2022 from https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/

[20] Jennifer Rexford, Jia Wang, Zhen Xiao, and Yin Zhang. 2002. BGP routing stability of popular destinations. In *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*. 197–202.

[21] RIPE RIS. 2022. Route Collection Raw Data: MRT Files. Retrieved June 18, 2022 from https://ris.ripe.net/docs/20_raw_data_mrt.html#name-and-location

[22] RIPE RIS. 2022. Route collectors. Retrieved June 18, 2022 from https://ris.ripe.net/docs/10_routecollectors.html

[23] Luca Sani. 2017. Isolario improving understanding of AS ecosystem. Retrieved June 18, 2022 from https://blog.apnic.net/2017/04/25/isolario-improving-understanding-ecosystem/

[24] Gadjo Sevilla. 2022. Russian invasion is taking a toll on internet access in Ukraine. Retrieved April 30, 2022 from https://www.emarketer.com/content/russian-invasion-taking-toll-on-internet-access-ukraine

[25] Soon Tee Teoh, Kwan-Liu Ma, S Felix Wu, and Xiaoliang Zhao. 2002. A visual technique for internet anomaly detection. In *IASTED International Conference on Computer Graphics and Imaging*. Citeseer.

[26] SBU Ukraine. 2022. Regarding the investigation of a hacker attack on Ukrainian news sites. Retrieved June 20, 2022 from https://t.me/SBUkr/3930

[27] Christina Wilkie. 2022. Russia repositions troops away from Kyiv, marking a shift in the war. Retrieved June 20, 2022 from https://www.cnbc.com/2022/03/29/russia-repositions-troops-away-from-kyiv-marking-a-shift-in-the-war-.html

[28] Natalia Zinets. 2022. Kharkiv official says Russian missiles hit administration building, residential areas. Retrieved June 20, 2022 from https://www.reuters.com/world/europe/kharkiv-official-russian-missiles-hit-city-administration-residential-areas-2022-03-01/