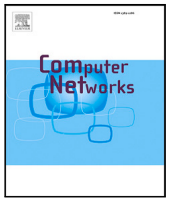
Computer Networks 224 (2023) 109596

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Impact of the first months of war on routing and latency in Ukraine

Valerio Luconi [b,*], Alessio Vecchio [a]

[a] Dip. di Ing. dell'Informazione, Università di Pisa, Largo L. Lazzarino 1, 56122 Pisa, Italy
[b] Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Via G. Moruzzi, 1, 56124 Pisa, Italy

ARTICLE INFO

Keywords:
Internet measurements
Routing
Latency
War

ABSTRACT

Given the fundamental role of the Internet in our lives, a better understanding of its operational status during war times is crucial. In this paper, we analyze the Ukrainian Internet during the first months of war after the Russian invasion occurred in February 2022. The analysis is carried out from two points of view: routing and latency. In terms of routing, there is a substantial increase in BGP announcements and withdrawals which can be due to both the physical unavailability of facilities and cyberattacks. Latency also increased significantly compared to the pre-conflict period, especially when considering paths going from Ukraine to Russia. The increase in latency appears to be due to a partial shift from peering to transit.

1. Introduction and related work

The operations of mass media, businesses, government agencies, and public safety organizations depend on Internet-based communications. Undermining the Internet of a country imposes a severe toll on the operational status of many critical sectors, due to the increasingly interconnected nature of services, communications, and also physical assets. At the same time, the Internet provides access to vital information to single individuals and it is the substrate upon which remote work is made possible. The importance of the Internet is even greater during catastrophic events, such as wars, when receiving news and coordinating activities have an impact on the safety of people. In this paper, we report our findings concerning the operational status of the Ukrainian Internet during the first two months and a half of the war. The analysis is carried out from two points of view: routing and latency. The first allows a better understanding of how the network adapted to the events happening both in the physical world, such as the massive movements of people and the unavailability of communication infrastructure, and in the digital domain, such as cyberattacks. The second allows quantifying the performance loss as perceived by the end-users.

The Ukrainian–Russian conflict roots back in 2014, with the annexation of the Crimean peninsula to the Russian Federation. During the subsequent years, the Internet in Crimea was subject to radical changes in terms of connectivity and regulation, as documented in [1]. Two events were associated with significant changes in routing: the deployment of new cables connecting the Crimean peninsula to Russia through the Kerch strait, and a block imposed by the Ukrainian government on Crimea-originated traffic and directed to Russian social networks, mail services, and search engines. Traffic previously going through Ukraine, increasingly started to be routed through Miranda Media, Rostelecom, Fiord, and UMLC, a set of Russia-based ISPs and transit providers [1]. The geopolitical significance of Internet routes is discussed in [2] with a specific focus on the Donbas region. A longitudinal analysis of the connectivity of the Autonomous Systems (ASes) located in Ukraine, revealed that the ones more closely related to the Donbas region progressively moved from Ukrainian cyberspace to Russian one. In the AS graph, the Donbas cluster appears, in the later years, to be placed at the periphery of the Ukrainian Internet, but still not fully integrated into the Russian one [2]. Some anecdotal evidence also suggested that the physical paths covered at the IP level could be radically different, depending if the source was located in the part of the territory controlled by the Ukrainian government, or in the Luhansk and Donetsk regions [2]. The destination for the two paths was always the same, Moscow, but in the first case the path was circuitous and transited through international carriers to avoid the Ukraine–Russia border, whereas the second one was more direct.

The impact of the 2022 conflict on Internet traffic has been observed by Cloudflare monitoring infrastructure in the 21 Feb - 4 Mar period [3]. Several phenomena are visible in the traffic patterns: there is an increase in the level of traffic in western cities of Ukraine due to the movements of people towards the border, and a decrease in the level of traffic in cities closer or directly involved in battles. At the same time, they observed an increased number of cyberattacks, as layer 3/4 and layer 7 Distributed Denial of Service (DDoS), highlighting how the conflict in the real world is accompanied by hostile activities in cyberspace. The intertwined relationship between the real world and

* Corresponding author.
E-mail addresses: valerio.luconi@iit.cnr.it (V. Luconi), alessio.vecchio@unipi.it (A. Vecchio).

https://doi.org/10.1016/j.comnet.2023.109596
Received 2 September 2022; Received in revised form 21 December 2022; Accepted 25 January 2023
Available online 28 January 2023

cyberspace during the conflict is testified also by the following event: Cloudflare moved the customer encryption key material out of their data centers in Ukraine, Russia, and Belarus still preserving operations via more secure data centers; in addition, the machines were configured to self-brick in case of power or connection losses [4].

DDoS and possible BGP hijacking events occurring in the region were also reported by the Mutually Agreed Norms on Routing Security (MANRS) initiative [5]. The resiliency of the Ukrainian Internet during the first 2–3 weeks was discussed in [6], where the lack of market concentration, as well as the relatively large number of Internet eXchange Points (IXPs) providing connectivity to the country, were found as contributing factors to the rather surprising tolerance of the network despite the major devastation occurred.

The effects of war on the Ukrainian Internet have been studied by means of measurements collected via the M-Lab Network Diagnostic Tool [7]. The Network Diagnostic Tool allows users to estimate the throughput, latency, and loss rate of their connection. Measurements are carried out relying on the nearest server participating in the platform (there are 210 sites, distributed in 47 countries). Results show that during the first 54 days of the war the performance of the Ukrainian Internet was subject to a significant degradation, compared to the pre-invasion period, in terms of packet loss, bandwidth, and latency. A significant increase in the number of paths per connection was also observed.

A recent longitudinal analysis of the DNS and hosting infrastructure showed that Russia is characterized by relatively high levels of domestic provisioning, with approximately 70% of websites fully hosted in the country. Effects caused by sanctions were generally modest, leading to single-digit variations compared to the previous years. Certificate issuance, on the other hand, is still relying on external entities, despite the creation of the Russian Trusted Root CA [8].

The impact of some catastrophic events on the Internet was studied in the past. In [9], the effects of a major earthquake in Japan were analyzed from the point of view of routing and traffic as seen from an ISP. The network outages caused by Hurricane Sandy were evaluated in [10]. The COVID-19 pandemic also had a significant impact on the Internet in terms of traffic and latency [11–13]. The role of the Internet in situations of sociopolitical turmoil was also a matter of attention, in particular concerning the revolts in Egypt that occurred in 2011 [14,15], but in this case the focus was on the Internet as a communication technology. The effects of a potential disaster – solar superstorms – were also evaluated in terms of possible network outages [16]. The impact of potential large-scale disasters was faced also according to simulation-based approaches [17].

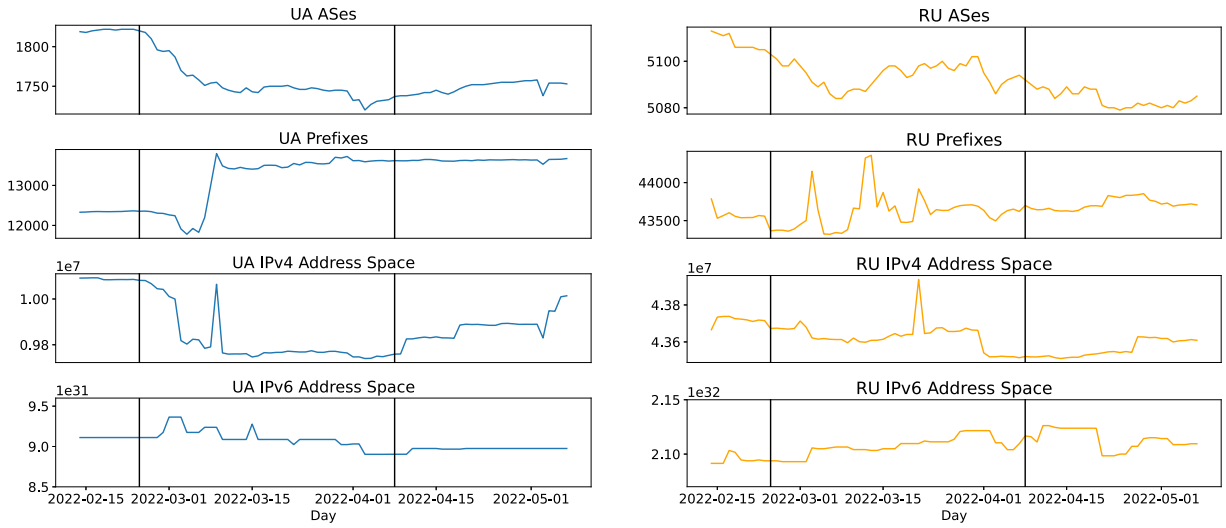
In this paper, we quantify the impact of war on the Internet in Ukraine in terms of routing and latency. The analysis spans approximately 12 weeks, the longest possible period at the time of writing considering the necessary collection, processing, and synthesis of information. As far as we know, this is the first time the Internet is observed during a major conflict in terms of both routing and latency.

2. Dataset

We collected an extensive dataset about routing, latency, Internet paths, and Internet geography involving Russian and Ukrainian ASes, in the period from 14 Feb 2022 to 7 May 2022. The observation period begins ten days before the start of the Russian invasion of Ukraine (24 Feb 2022). These ten days are used as a baseline against which the observations during the war are compared. Data have been collected from multiple sources managed by RIPE NCC [18], which is the Regional Internet Registry for Europe, the Middle East, and parts of Central Asia. Besides this activity, RIPE NCC also handles Internet measurement platforms and publishes all the data free for everyone. We collected data from the following sources:

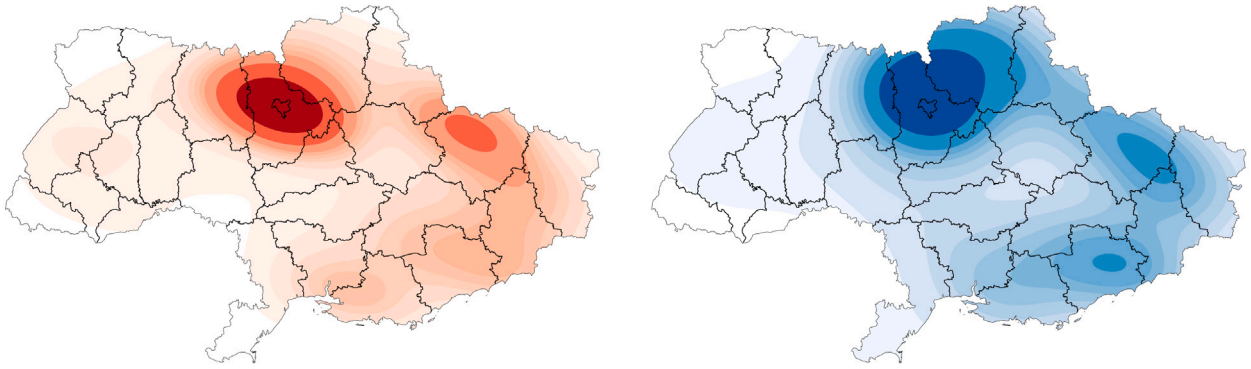
- RIPE RIS [19]. RIPE RIS is a project that collects raw routing data from over 1400 peers spread in 500 cooperating ASes from all over the world via 23 route collectors (at the time of writing). The routing data is in the form of BGP updates and BGP Routing Information Bases (RIBs). BGP is the routing protocol used to establish inter-domain routing across the whole Internet [20]. BGP updates are control messages exchanged by BGP peers to establish or remove Internet routes. In our study, we are interested in two particular messages: *announcements* and *withdrawals*. Announcements are used by ASes to communicate their prefixes reachability. They are propagated to establish or update a path to a prefix (route) from elsewhere in the Internet. Withdrawals are instead used to communicate that a route is no longer available. We collected all BGP updates from 14 Feb 2022 to 7 May 2022, from all the 22 available route collectors in that interval (the 23rd route collector was added subsequently). The BGP updates come in the form of gzipped MRT[1] files, which are published by RIPE once every 5 min per route collector, and contain the BGP updates sent by every peer attached to the given route collector in 5 min. In total, we collected approximately 525 000 files. All the compressed files account for approximately 660 GB of data (5.3 TB of uncompressed data). Each file contains from several dozens to several hundreds of thousands of BGP updates, depending on how many peers peer with a given route collector and the particular moment in time. To collect and parse BGP updates we used BGPStream, a library distributed by CAIDA, which provides an API for collecting and parsing BGP data [22].
- RIPEstat [23]. RIPEstat is a platform that provides an easy-to-use API for downloading aggregated json data extracted from: (i) raw BGP data collected by RIPE RIS, (ii) routing and administrative data from Internet Routing Registries (IRRs), and (iii) prefix geolocation data extracted from MaxMind GeoLite databases. We collected data about all the routed ASes and their routed prefixes in Ukraine and Russia from 14 Feb 2022 to 7 May 2022. Routed ASes are ASes that are seen in BGP data collected by RIPE RIS, while their prefixes are the prefixes that are announced by them via BGP. In addition, we collected geolocation data about all the Russian and Ukrainian ASes. Overall, we downloaded and parsed approximately 80 000 json files from RIPEstat, accounting for 21 GB of data.
- RIPE Atlas [24]. RIPE Atlas is an Internet measurement platform that performs active measurements such as Ping, Traceroute, and HTTP probing. Measurements are carried out by nodes spread all over the world. RIPE Atlas nodes belong to two categories: probes and anchors. Probes are hosted by volunteers, typically in their home networks, or in the network of small-medium companies. Anchors are more powerful nodes and are typically hosted in the networks of larger and well-connected companies or organizations such as IXPs, data centers, and operational centers of ISPs. Probes automatically carry out some network measuring tasks called Anchoring Measurements (AMs), where anchors play the role of targets. The global number of nodes belonging to the RIPE Atlas platform is approximately 12 000 (in particular, ~11200 probes and ~760 anchors), distributed worldwide. For our study, we extracted the results of Ping, HTTP, and Traceroute AMs performed by the Atlas nodes in Ukraine from 14 Feb 2022 to 7 May 2022. The data is provided by devices scattered over a significant part of Ukraine and hosted in different ASes. As a consequence, the data used for the analysis originates from a set of vantage points that is heterogeneous and reasonably stable, and allows observing the phenomena from a country-scale perspective not tied to the specific point of view of a single stakeholder. The number of Ping samples used in the latency study described in

[1] A standard for exporting routing information [21].



(a) Ukraine (b) Russia

Fig. 1. Number of routed ASes and prefixes, and announced IP address space per day for both Ukraine and Russia. Note that the scales of the figures are different to better capture the evolution in time of the different metrics.



(a) Density of the positions of the ASes that showed some loss of connectivity.

(b) Density of the positions of Russian attacks and battles on Ukrainian soil.

Fig. 2. Ukrainian ASes and war events maps.

Section 4 is approximately 675 M. In particular, 54 M samples have been used in the analysis of the Ukraine to Ukraine scenario, 50 M in the Ukraine to Russia scenario, and 571 M in the Ukraine to Europe scenario. Details about the three scenarios are given in Section 4. The number of HTTP latency samples is approximately 2.2 M, whereas the number of paths is 3.8 M.

3. Impact on routing

In this section, we show the impact of the conflict on Internet routing, from the perspective of both countries.

3.1. Routed ASes and prefixes

Fig. 1 shows the evolution over time of the number of routed ASes, prefixes, and IPv4 and IPv6 announced address space (i.e., the total number of addresses in the routed prefixes) in both the Ukrainian and Russian Internet. Let us first consider the case of Ukraine (Fig. 1(a)). As it can be observed, the number of routed ASes starts decreasing right after the start of the war, from a maximum of 1822 right before the start of the conflict to a minimum of 1720 occurring approximately around 3 Apr 2022. Around this date, the Russian forces were starting to abandon northern Ukraine to concentrate their efforts on the southeast side of the country. In fact, from the start of the second phase of the war around 8 Apr 2022, the number of routed ASes slowly increases. In the considered period some of the ASes that lost connectivity showed intermittent behavior, by going offline and back online at different times. The total number of ASes that showed some loss of connectivity is 307. Some of the reasons underlying the loss of routed ASes could include the bombings and battles that happened on Ukrainian soil, which possibly destroyed part of those ASes' infrastructure or made them shut down their services due to power unavailability or evacuation. To confirm this, we gathered from RIPEstat the geolocation of the 307 Ukrainian ASes that showed some loss of connectivity in the war period, and from Wikipedia the position of Russian attacks and battles [25]. In Fig. 2, we show the densities of the positions of ASes and the position of attacks. We can observe an evident graphic correlation between the two sets of positions.

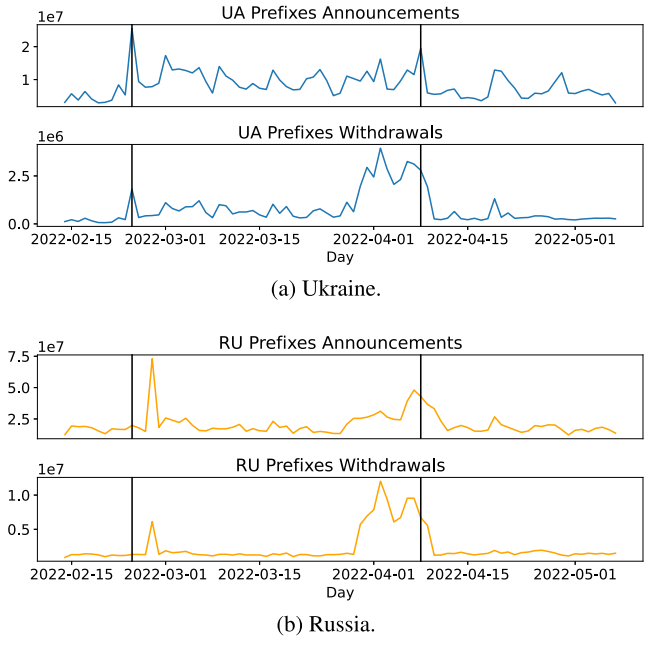
The number of routed prefixes starts at 12 330, then it shows a slight decrease after the first week of the war, down to a minimum of 11 779 routed prefixes, and then a sudden increase, with a number of routed prefixes even higher than in the baseline period, reaching a maximum of 13 796. The numbers of announced IPv4 and IPv6 addresses per day show limited variations, accounting for just 1%–2%. However, it

is worth noticing that the decreasing trend of the IPv4 address space is similar to the one of routed ASes. This could happen for multiple reasons. War, as known, spans also the cyber domain, and, in particular, Internet prefixes can be subject to cyberattacks such as BGP hijacking. In short, a BGP hijacking attack occurs when a prefix is announced by an AS other than the owner AS, with the purpose of redirecting traffic for multiple aims, including denial of service, and traffic interception (more details about BGP hijacking attacks are provided in Section 3.4). A way to hinder certain BGP hijacking attacks is to announce more specific sub-prefixes of the attacked prefix, as the Internet routing is based on the longest prefix match. By analyzing the data, we discovered multiple cases in which new prefixes were announced by Ukrainian ASes. First, some Ukrainian ASes simply started announcing new prefixes they never announced before. The reasons behind such behavior are inscrutable using the collected data. Possible explanations that we imagine include that these ASes moved their services to new prefixes to avoid attacks (either BGP or other kinds of cyberattacks), or they moved to new facilities due to damages. Second, some Ukrainian ASes started announcing sub-prefixes of their own prefixes. This practice has been implemented in different ways. Some ASes divided all their prefixes into /24 subnets (i.e., networks with 256 IP addresses). This could allow mitigating the effect of possible BGP hijacks, as attackers should target smaller prefixes (the reader should note that a /24 network is already quite small), and a higher number of prefixes to be effective. In other cases, Ukrainian ASes started announcing /32 prefixes, i.e., single IP addresses. The efficacy of this practice is however limited, as pointed out in Section 3.3. However, in certain cases, these prefixes still went offline after a certain amount of time. Particularly interesting is the following case. In the late hours of 8 Mar 2022 and the early hours of 9 Mar 2022, a Ukrainian AS announced ∼ 200 prefixes owned by Russian ASes. This peak can also be observed in the announced IPv4 address space. The duration of this phenomenon has been of few hours, and we cannot be sure if this has been a deliberate tentative of BGP hijacking or if it is the result of routers' misconfiguration. We will deepen the analysis of BGP hijacking attacks between Russia and Ukraine in Section 3.4.

For Russia, the picture is quite different (Fig. 1(b)). The number of routed ASes decreases over time but in a very small percentage. The number of routed ASes per day fluctuates between approximately 5110 and 5080. The total number of ASes that showed loss of connectivity is 335, very similar to the Ukrainian number, but it represents a much smaller percentage, approximately 7% of the total compared to 17%. The number of prefixes also fluctuates, between approximately 43 300 and 44 400. Thus, the fluctuations are much less evident than in the Ukrainian case. However, a certain degree of instability is observed in the first phase of the war, with some peaks around 3 Mar 2022 and 12–13 Mar 2022. Especially in those days, some Russian ASes started announcing sub-prefixes of their prefixes. For example, a Russian operator split its prefixes into /30 and /32 prefixes on 3 Mar and 12 Mar, for an amount of over 1400 prefixes announced. These announcements lasted just a few hours on both days. As for the Ukrainian case, this could be an attempt to recover from BGP hijacking attacks. As mentioned above, we will deepen the analysis of this aspect in Section 3.4. The announced IPv4 and IPv6 address space shows again small fluctuations in the order of less than 1%, thus it is generally stable.

3.2. BGP activity

In this section, we consider the number of BGP announcements and withdrawals per day for both Ukrainian and Russian prefixes, as shown in Fig. 3. As described in Section 2, RIPE RIS collects BGP updates from cooperating peers. Not all peers are available all the time, and this could alter the results if the set of peers is not consistent enough, hence we performed the following preliminary analysis. In the considered time interval, the total number of peers was 1443. We extracted those



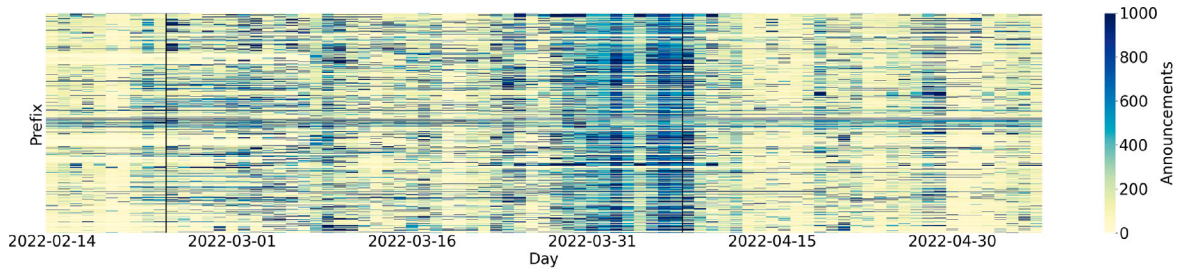
(a) Ukraine.

(b) Russia.

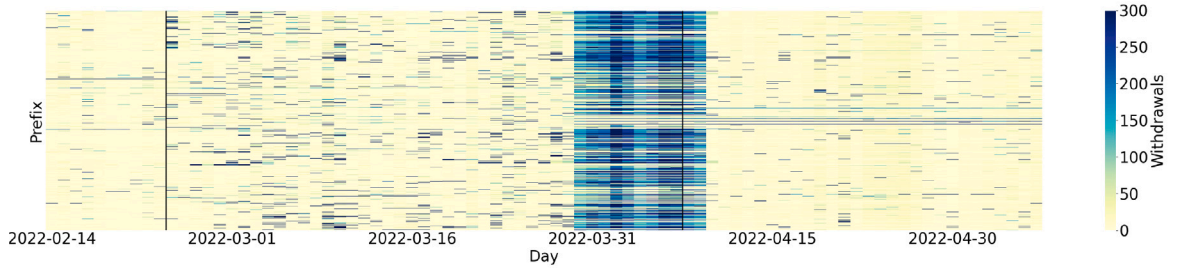
Fig. 3. Number of BGP announcements and withdrawals per day for both Ukrainian and Russian prefixes. Note that the scales of the figures are different to better capture the evolution in time of the different metrics and phenomena.

which were fairly stable, i.e. present 90% of the time. The number of such peers is 1330. On average, the peers that send BGP updates on Russian or Ukrainian prefixes are approximately 800 per day, and approximately 30 of them are not active for at least 90% of the time. We computed the contribution in terms of BGP updates of these less active peers, and we found that they produce an average of 4% of BGP updates. The percentage is stable across the entire time interval, ranging from 3% to 6%. We thus believe that their contribution does not affect the validity of our analysis, and we decided not to filter out their updates, because, given that our interest is to study an unprecedented phenomenon, we believe that even the small changes are interesting, if properly contextualized, and we prefer to highlight the potential occurrences of these small changes together with their magnitude instead of filtering them out a priori.

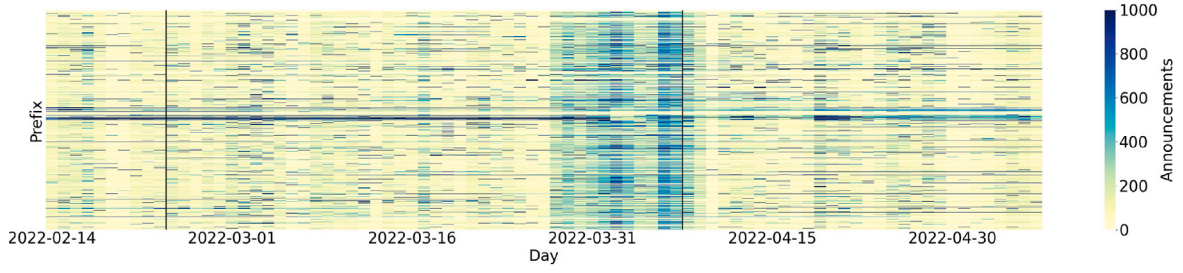
Let us first consider the Ukrainian case. As it can be observed in the first plot of Fig. 3(a), the number of BGP announcements per day grows significantly as the Russian invasion starts. This can indicate a cyber warfare scenario as described above, or simply that the Ukrainian Internet needed to reconfigure due to damage or destruction of the infrastructure. Fig. 4 shows the number of BGP updates per day and per prefix for both Ukrainian and Russian prefixes. Each line on the y-axis of the four subfigures represents an announced prefix, and the color represents the number of updates on a specific day. As shown in Fig. 4(a), the increment of BGP announcements is spread over the vast majority of prefixes and begins two–three days before the start of the war. However, the activity on 24 Feb 2022, which corresponds to a peak in the first plot of Fig. 3(a), seems to involve a limited number of prefixes, while in the period between 28 Mar 2022 and 9 Apr 2022 there is an intense activity of BGP announcements widely diffused in all prefixes, even if the total number of announcements per day is smaller than in 24 Feb 2022. Particularly interesting is the total number of BPG withdrawals per day, which in the second plot of Fig. 3(a) shows a substantial increment in the war period, especially in the days from 28 Mar 2022 to 9 Apr 2022. On those days, an evident bump can be observed: the number of withdrawals is from 4 to 8 times higher than in every other day of the conflict. Fig. 4(b) shows that the increment is spread over almost all the prefixes, with very few exceptions. On the



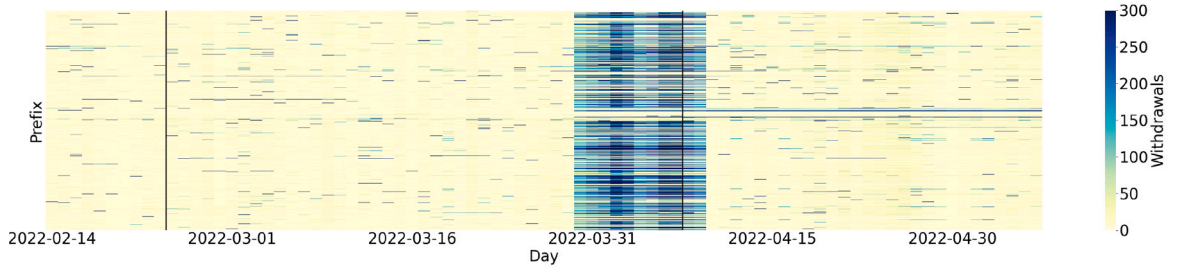
(a) Ukraine announcements.



(b) Ukraine withdrawals.



(c) Russia announcements.



(d) Russia withdrawals.

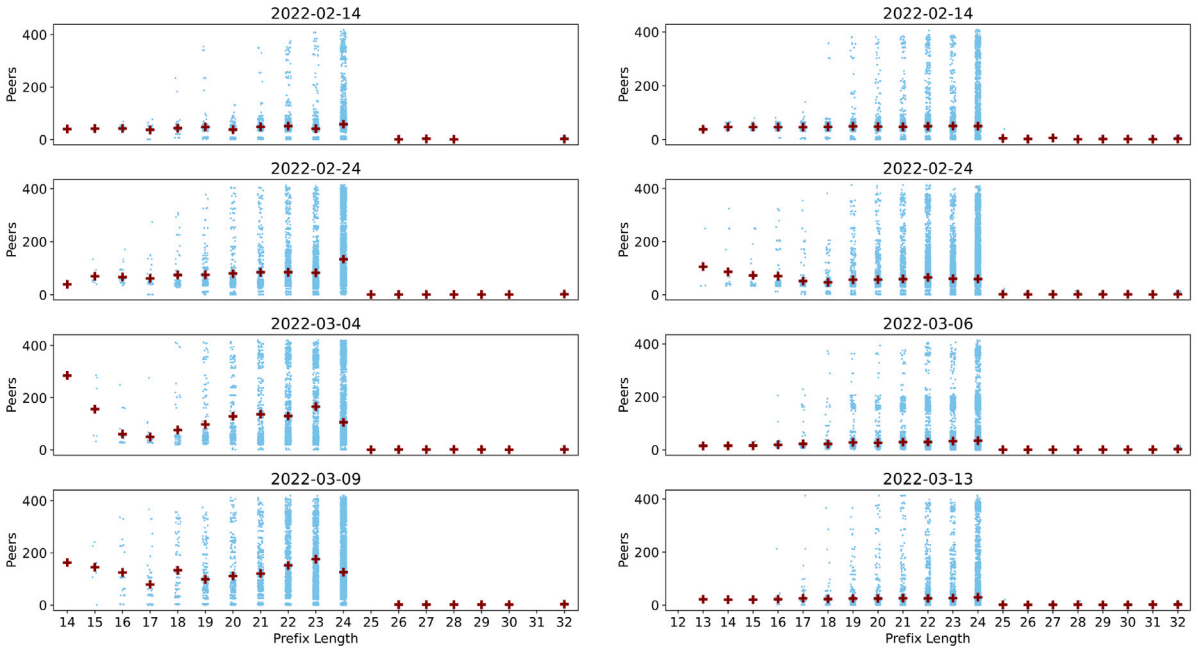
Fig. 4. Heatmaps showing the number of BGP updates per day per prefix for both Ukrainian and Russian prefixes. Each line on the *y*-axis represents an announced prefix, the *x*-axis shows the time, and the color represents the number of updates, as shown in the color map on the right. Note that the scales of the color maps for announcements and withdrawals are different to better capture the evolution in time of the two different metrics.

other war days, a slightly incremented activity is visible, with peaks for a few isolated prefixes, especially during the first phase of the Russian invasion. By observing Fig. 4 in its entirety, we can conclude that in the period going from 28 Mar 2022 to 9 Apr 2022 there has been some event that triggered an extremely anomalous number of BGP updates in (almost) all Ukrainian ASes. We will deepen the analysis on this phenomenon in Section 3.3.

The Russian case shows some similarities but also some differences. The announcement and withdrawal activities remain approximately unchanged during the whole observation period, with two notable exceptions. Both announcements and withdrawals show a peak corresponding to 27 Feb 2022, and a bump in the days from 28 Mar 2022 to 9 Apr 2022. In those days the announcements activity almost doubles, and the withdrawal activity grows six or seven times (first and second plots of Fig. 3(b)). The Russian and Ukrainian withdrawal bumps are almost overlapped, except for the absolute number of updates, which for Russia is much greater. Fig. 4(c) shows that the announcement activity in correspondence with the first peak (27 Feb 2022) does not seem to be spread over all the prefixes. The same happens for withdrawals, as shown in Fig. 4(d). Instead, the announcement and withdrawal activity observed between 28 Mar 2022 and 9 Apr 2022 is spread over almost all prefixes, as in the Ukrainian case.

3.3. Propagation of prefixes and BGP updates

In this section, we go back to the findings of Sections 3.1 and 3.2 and add some considerations based on the propagation among route collectors and peers of the highlighted phenomena.



(a) Ukraine. The four plots are relative to four days: the first day of observation (14 Feb 2022), the day in which war activities started (24 Feb 2022), the day in which the lowest number of announced prefixes were reached (4 Mar 2022), and the day in which the highest number of announced prefixes was reached (9 Mar 2022).

(b) Russia. The four plots are relative to four days: the first day of observation (14 Feb 2022), the day in which war activities started (24 Feb 2022), the day in which the lowest number of announced prefixes were reached (6 Mar 2022), and the day in which the highest number of announced prefixes was reached (13 Mar 2022).

Fig. 5. Propagation of IPv4 prefixes among peers. Each light blue dot is related to a single prefix and shows how many peers received BGP updates for that prefix. Prefixes are grouped per length. Dark red plus markers represent the average number of peers for each group. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

We first consider the case of the routed prefixes. For simplicity and statistical significance, we consider only the case of IPv4 prefixes, as IPv6 prefixes are a negligible percentage (approximately 5%), and similar considerations apply. We computed, for each prefix, the number of RIPE RIS peers that received a BGP update for that prefix. In Fig. 5, we show the results for both Ukraine and Russia. For each country, we chose four days that we consider meaningful. The first two days are common for both countries: the first day of the observation period which we use as a baseline (14 Feb 2022), and the first day of the war (24 Feb 2022). The other two days are the day in which the lowest number of announced prefixes was reached (4 Mar 2022 for Ukraine and 6 Mar 2022 for Russia), and the day in which the highest number of prefixes was reached (9 Mar 2022 for Ukraine and 13 Mar 2022 for Russia). For each prefix, the plot shows the number of peers that received BGP updates for that prefix, grouped per prefix length.

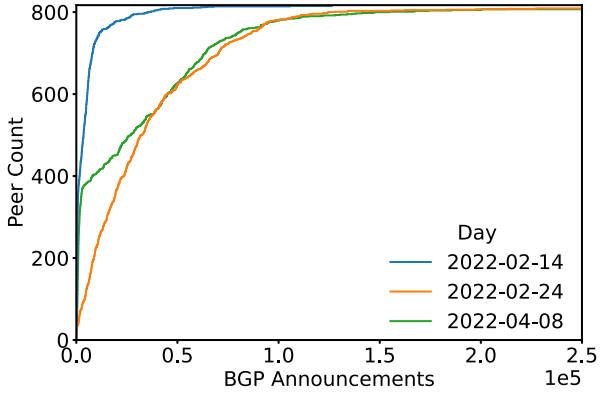
Let us first consider the Ukrainian case. As shown in Fig. 5(a), as long as the war activities go on, the prefixes propagate to a higher number of peers, but only for prefixes up to /24 prefix length, which account for the vast majority of announced prefixes. The number grows higher on 4 Mar 2022 and on 9 Mar 2022. These are the days in which the number of announced prefixes reach their minimum and maximum, respectively, as observed in Fig. 1(a). These two findings combined could suggest a reorganization of the Ukrainian Internet connectivity. This shows how the intense BGP activity has a significant echo perceived over the BGP measuring infrastructure, which is worldwide spread. More specific prefixes, from /25 to /32, have however a very limited propagation. This can happen as operators may apply filters to hyper-specific prefixes for various traffic engineering and security reasons, as also pointed out in [26]. Even if the number of these prefixes grows after the start of the war (from 54 on the first day to 201, 164, and 172, respectively, in the other three days) their BGP updates are able to reach just two or three peers each. In the case that these hyper-specific prefixes are announced as a countermeasure against BGP hijacking attacks, this would pose a limit to the efficacy of this practice.

In Russia, the day of the start of the war shows a slight increase in the propagation of prefixes (Fig. 5(b)), which is not of the same magnitude as the Ukrainian one, and, in addition, is not maintained in the subsequent days. As discussed in the previous sections, Russian connectivity did not experience events as extreme as the Ukrainian ones and remained fairly stable. If the connectivity is stable and paths remain substantially unchanged, the propagation of updates is lower for two reasons. First, if there are no changes, it is not necessary to send updates for a given prefix. Second, BGP allows route aggregation, thus in presence of only small changes, the routes can at a certain point be aggregated and an update is not propagated.

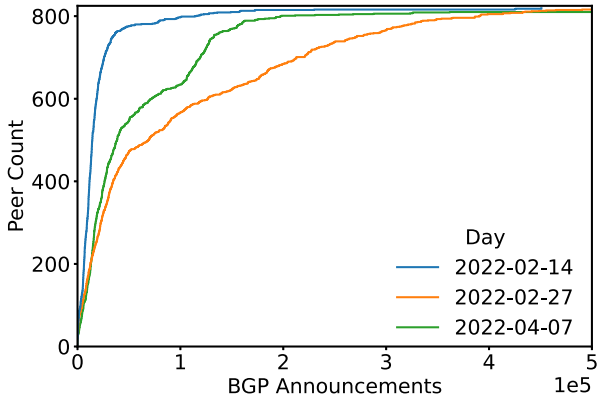
We now focus on the propagation of BGP updates. In particular, for both Ukraine and Russia, we computed the number of BGP announcements received by each RIPE RIS peer per day. We chose to show, for each country, three days that we consider meaningful: the first day of observation (14 Feb 2022), and the two days with the highest peaks of BGP announcements, which for Ukraine are 24 Feb 2022 and 8 Apr 2022, and for Russia are 27 Feb 2022 and 7 Apr 2022. It must be noticed that the third day chosen is included in the bump shown in Section 3.2, for both Ukraine and Russia. Fig. 6 shows the cumulative count of peers that receive a given number of BGP announcements. In other words, for each value of BGP announcements, the plot shows the number of peers that receive less or equal announcements. As can be observed, with respect to the first day of the observation period, in the other two days the propagation of BGP announcements is extremely higher (the distributions are shifted to the right), however with different trends. In the first days of the war (24 Feb 2022 and 27 Feb 2022 for Ukraine and Russia respectively), the propagation is higher. This is evident, especially in Russia. On the third day considered, the propagation is generally lower than on the second day. This suggests that the peaks of the last day could be observed by a smaller number of peers. As further evidence of this, the distributions of the second and third day, for both Ukraine and Russia, show a very long tail. To investigate further, we computed the contribution in terms of BGP

Table 1
Top five route collectors and peers per total number of updates in the interval between 28 Mar 2022 and 9 Apr 2022. The route collectors are rrc00 in Amsterdam, NL, which collects BGP updates via multi-hop BGP sessions all over the world, rrc01 in London, GB, which collects BGP updates at the IXP peering LANs of LINX and LONAP, rrc03 in Amsterdam, NL, which collects BGP updates at the IXP peering LANs of AMS-IX and NL-IX, rrc11 in New York, US, which collects BGP updates at the IXP peering LAN of NYIIX, rrc12 in Frankfurt, DE, which collects BGP updates at the IXP peering LAN of DE-CIX, and rrc20 in Zurich, CH, which collects BGP updates at the IXP peering LAN of SwissIX.

BGP updates type	Ukraine				Russia			
	RC	# Updates (%)	Peer	# Updates (%)	RC	# Updates (%)	Peer	# Updates (%)
Announcements	rrc00	55 480 407 (30.8%)	23.129.32.61 (rrc00)	18 016 270 (10.0%)	rrc00	140 900 051 (30.7%)	23.129.32.61 (rrc00)	48 931 354 (10.7%)
	rrc12	17 179 589 (9.5%)	45.136.136.5 (rrc00)	9 413 532 (5.2%)	rrc12	48 409 215 (10.6%)	45.136.136.5 (rrc00)	21 263 321 (4.6%)
	rrc20	16 051 109 (8.9%)	2a09:4c0:100:5eb1::7afb (rrc00)	3 318 308 (1.8%)	rrc20	44 744 174 (9.8%)	2a09:4c0:100:5eb1::7afb (rrc00)	9 561 264 (2.1%)
	rrc01	13 961 897 (7.7%)	94.177.122.251 (rrc00)	3 184 517 (1.8%)	rrc03	37 702 429 (8.2%)	94.177.122.251 (rrc00)	9 165 701 (2.0%)
	rrc03	13 668 020 (7.6%)	91.206.52.126 (rrc20)	1 591 859 (0.9%)	rrc01	30 349 329 (6.6%)	91.206.52.127 (rrc20)	4 543 613 (1.0%)
Total		116 341 022 (64.5%)		35 524 486 (19.7%)		302 105 198 (65.9%)		93 465 253 (20.4%)
Withdrawals	rrc00	25 512 199 (81.4%)	23.129.32.61 (rrc00)	18 273 032 (58.3%)	rrc00	69 706 060 (78.4%)	23.129.32.61 (rrc00)	48 811 569 (54.9%)
	rrc01	814 455 (2.6%)	2a09:4c0:100:5eb1::7afb (rrc00)	3 101 751 (9.9%)	rrc20	4 748 656 (5.3%)	2a09:4c0:100:5eb1::7afb (rrc00)	8 952 025 (10.1%)
	rrc12	731 657 (2.3%)	94.177.122.251 (rrc00)	3 038 483 (9.7%)	rrc03	2 008 131 (2.2%)	94.177.122.251 (rrc00)	8 759 004 (9.9%)
	rrc20	654 206 (2.1%)	2602:fed2:fc0:5e::1 (rrc00)	296 923 (0.9%)	rrc12	1 909 392 (2.1%)	91.206.52.177 (rrc20)	1 752 578 (2.0%)
	rrc03	580 685 (1.9%)	198.32.161.23 (rrc11)	177 548 (0.6%)	rrc01	1 901 212 (2.1%)	2001:7f8:24::b1 (rrc20)	1 752 271 (2.0%)
Total		28 293 202 (90.2%)		24 887 737 (79.4%)		80 273 451 (90.3%)		70 027 447 (78.8%)



(a) Ukraine.



(b) Russia.

Fig. 6. Cumulative count of peers that receive up to a given number of BGP announcements.

announcements for each peer in the three days for both countries, and we found that in the first two days the maximum contribution for each peer is 2%–4%, in the last day there is a single peer that contributes for approximately 8% of announcements in Ukraine and 10% in Russia. The peer is the same for both countries. Since the third day for both Ukraine and Russia is part of the bump shown in Fig. 3, we believe this deserves a deeper analysis.

We thus computed the top five route collectors and peers per total number of updates in the interval corresponding to the bump of Fig. 3, i.e. between 28 Mar 2022 and 9 Apr 2022. Table 1 shows the results per country and type of BGP updates: announcements and withdrawals. The results for the BGP announcements are very similar for Ukraine and Russia. The top five route collectors are the same, and together cover approximately 65% of the total number of announcements in the time interval. The remaining seventeen route collectors account for just 35% of the announcements. Rrc00, located in Amsterdam, NL, collects alone approximately 31% of the BGP announcements. The remaining 34% of announcements are almost evenly spread among the other four route collectors. The top five peers are the same in Ukraine and Russia and account for approximately 20% of the total. They are connected all to rrc00 except the last one, which is connected to rrc20, located in Zurich, CH (the two IPs belong to the same AS, SwissIX). The first peer, which is owned by 10VPN, a BGP research network, provides alone approximately 10% of announcements. From the point of view of the propagation of BGP announcements, the results show a certain polarization among a few route collectors, which however cover approximately 50–100 peers each. The top five peers do not cover approximately 80% of the announcements, thus we can conclude that the BGP announcements in the considered period are fairly spread.

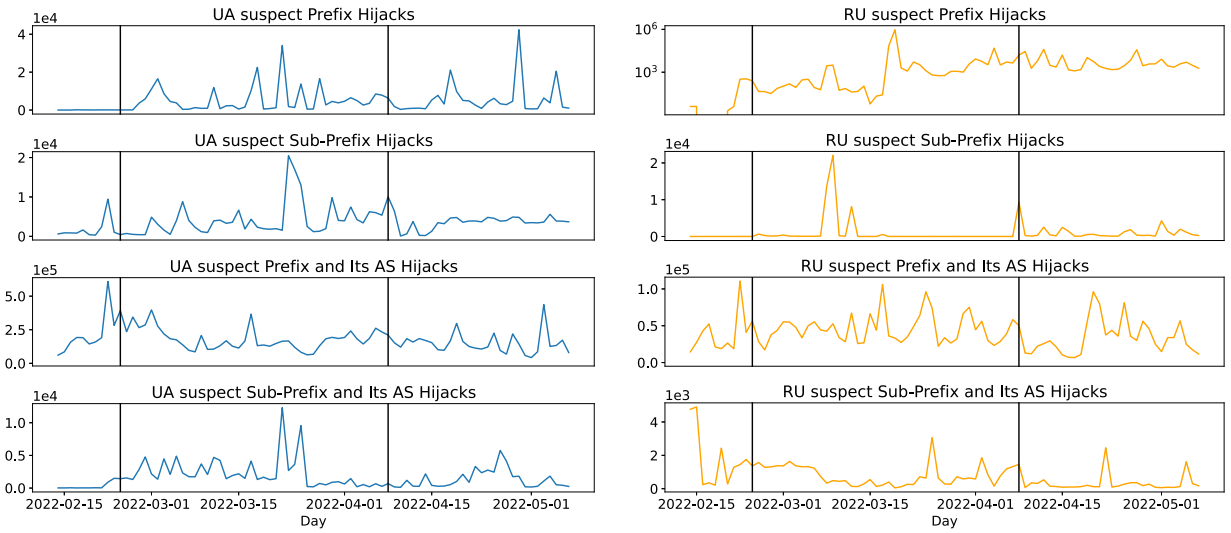
The picture is different for the withdrawals. The first route collector of the top five covers approximately 80% of the withdrawals in both Ukraine and Russia, and the first peer, which is first also for the announcements, covers approximately 55% of the withdrawals alone. These results show an extremely high polarization of the BGP withdrawals in a few route collectors and peers (the top five route collectors cover 90% of the total, and the top five peers 79%). These findings indicate poor propagation for this type of BGP updates.

To further inspect the propagation of updates in the considered period, we analyzed the prefixes that experienced a high BGP activity. We analyzed separately BGP announcements and BGP withdrawals. For announcements, we selected all the prefixes with at least 500 announcements per day. For these prefixes, we computed the percentage of prefixes whose announcements reached at least five route collectors and at least fifty peers. For Ukraine, the values are 100% and 86.1% on average for all the days of the considered period. For Russia, the values are 100% and 73.5%. For withdrawals, we repeated the analysis for the prefixes with at least 200 withdrawals per day. For Ukraine, the values are on average 40.0% and 23.5%. For Russia, the values are 33.9% and 16.9%. This is further evidence that in the period between 28 Mar 2022 and 9 Apr 2022 the propagation of the observed BGP withdrawals is limited to a few route collectors and peers.

3.4. Suspect cases

In this section, we analyze BGP updates that could indicate the occurrence of BGP hijacking attacks. We rely on the classification of BGP hijacking attacks provided in [27], which we report briefly. BGP hijack attacks are classified as:

1. *Prefix Hijack*. In this case, the attacker announces an existing prefix of the victim, as if it was the owner.



(a) Ukraine. (b) Russia.

Fig. 7. Number of BGP announcements showing suspect BGP hijack cases. Note that the scales of the figures are different to better capture the evolution in time of separate phenomena. Note also that the scale of the first plot of Fig. 7(b) is logarithmic.

2. *Prefix and Its AS Hijack*. In this case, the attacker generates an announcement for an existing prefix of the victim as if the victim was directly connected to the attacker. The victim still appears as the owner of the prefix.
3. *Sub-Prefix Hijack*. This case is identical to the first case, except that instead of a prefix, the attacker announces a sub-prefix of an existing prefix of the victim.
4. *Sub-Prefix and Its AS Hijack*. This case is identical to the second case, except that instead of a prefix, the attacker announces a sub-prefix of an existing prefix of the victim.
5. *Hijack a Legitimate Path*. In this case, the attacker propagates an existing announcement but puts itself as if it was a neighbor of the victim. In practice, this last case is almost indistinguishable from the second case, as when an announcement is collected we are unable to tell if it has been manipulated or generated from scratch.

We found some cases of suspect BGP hijacking from Russian attacker ASes to Ukrainian victim ASes, and vice-versa. To identify such possible BGP hijacking cases, as a baseline we built a table with the prefixes belonging to Ukrainian and Russian ASes collected on 14 Feb 2022 from RIPEstat, coupled with their owner AS. We checked the prefixes with data from Internet Routing Registries RIPE and RADB to be sure that they were assigned to the correct AS. Then, we collected from RIPE RIS all the BGP updates from 14 Feb 2022 to 7 May 2022, as explained in Section 2. We only considered BGP announcement updates. We identified suspect cases with the following procedure. From a BGP announcement we extract the announced prefix, the AS_PATH, and, from the AS_PATH, the origin AS. The AS_PATH indicates the path that the announcement has traveled from the AS that originated the BGP update to the AS that receives it, in terms of traversed ASes. The origin AS is the AS that is originating the BGP update, i.e. that is announcing the prefix, and it can be found as the first AS in the AS_PATH. We consider BGP announcements whose origin AS is one of the Russian or Ukrainian ASes previously identified. We then check the prefix against the prefix table that we previously built.

Fig. 7 shows the number of suspect cases of BGP hijack attacks, for both Russia and Ukraine, in Fig. 7(a) in blue those made by Russian possible attackers against Ukrainian possible victims and in Fig. 7(b) in orange those made by Ukrainian possible attackers against Russian possible victims. In the first row are the suspect Prefix Hijacks, in the second the suspect Sub-Prefix Hijacks, in the third the suspect Prefix and Its AS Hijacks, and in the fourth the suspect Sub-Prefix and Its AS Hijack (four of the five previously mentioned categories).

We first consider suspect cases of Prefix Hijacks. In this case, the prefix of the announcement is contained in the table that we previously built, and owner AS and origin AS are different and from different countries (i.e., Russian origin and Ukrainian owner, and vice-versa). As can be observed from the first row of Fig. 7(a) and Fig. 7(b), the number of suspect Prefix Hijacks is extremely low before the start of the Russian invasion (almost zero cases), and increases rapidly as the war starts, with peaks between 10 000 and 40 000 announcements for Ukraine, and almost 1 000 000 for Russia. In the case of Ukrainian possible attackers, the number of announcements showing suspect Prefix Hijack cases grows on average by two orders of magnitude during the first phase of the war. In the case of Russian possible attackers instead, the activity is intermittent. It must be noted that in both cases the suspect activity does not seem to decrease when the second phase of the war starts. To better quantify the magnitude of the events, we computed the number of target prefixes of these suspect BGP updates, and the number of ASes owners of these prefixes. For Ukraine, the average number of targeted prefixes per day before the start of the war is 0.7 and 10.3 during the war phases. These prefixes belong to an average of 0.7 ASes before the start of the war and 3.4 ASes per day during the war phases. The total number of targeted prefixes in the entire considered time interval is 18, spread over 8 ASes. We thus observe an increase of suspect activities also from the point of view of targeted prefixes, but not so substantial. For Russia, the average number of targeted prefixes per day is 0.7 before the start of the war and 18.4 after, spread in on average 6.1 ASes. The total number of targeted prefixes is 633, spread over 124 ASes. It must be noticed that on 8–9 Mar 2022 the number of Russian targeted prefixes was 465 and 238, spread over 100 and 54 ASes, a phenomenon already partially observed in the previous sections. In Russia, the phenomenon of suspect Prefix Hijacks seems to have a wider magnitude also from the point of view of targeted prefixes and ASes, even if the daily activity is not so evident.

The second row of Fig. 7(a) and Fig. 7(b) shows cases of suspect Sub-Prefix Hijack from Russian attackers to Ukrainian victims and vice-versa. In this case, the prefix of the announcement is a sub-prefix of a prefix in our table, and the origin AS and the owner AS are different and from different countries. As can be observed, in the case of Ukrainian victims and Russian attackers, the activity starts a few days before the invasion, and continues all over the duration of the observation period, with peaks reaching 20 000 announcements per day. In the case of

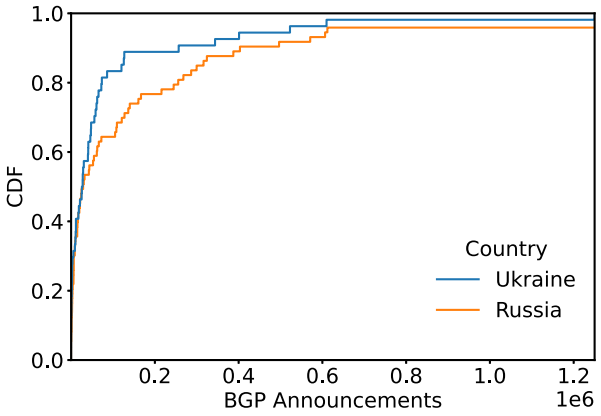


Fig. 8. Cumulative proportion of suspect attacker ASes that send a given number of suspect BGP announcements per country.

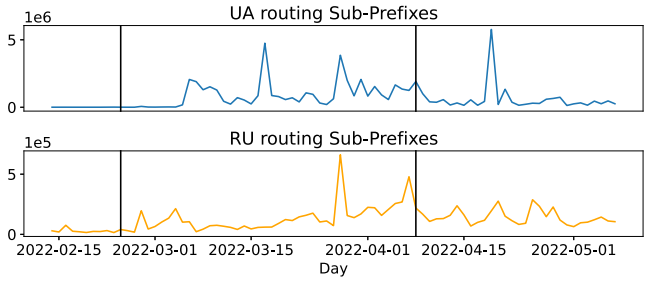


Fig. 9. Number of BGP announcements showing ASes routing their sub-prefixes. Note that the scales of the figures are different to better capture the evolution in time of the separate phenomena.

Ukrainian attacks, the occurrence of these suspect cases is limited to a few days. In the second phase of the war, the activity seems more frequent, albeit with a limited number of announcements per day. The average number of targeted prefixes per day for Ukraine is 6.5 before the start of the war, and 5.1 after, however, the average number of ASes per day is 1.8 and 2.5. In total the Ukrainian targeted prefixes are 16, spread over 5 ASes. As in the previous case, the magnitude of the Ukrainian suspect Sub-Prefix Hijacks seems to be rather limited. In Russia, the average number of targeted prefixes per day is 0.1 before the start of the war and 46.5 during the war, which are spread on average on 0.1 and 3.7 ASes, respectively. The total number of targeted prefixes is 3035, spread over 152 ASes. Again, it has to be noted that on 8–9 Mar 2022 there is a peak in targeted prefixes (1798 and 1528) and targeted ASes (91 and 112), which follows the pattern of the Prefix Hijack attacks.

The suspect Prefix and Its AS Hijacks, shown in the third row of Fig. 7(a) and Fig. 7(b), are identified in the following way. In an announcement, we check that the prefix has the correct origin, i.e. corresponding to the owner AS from our table. Then, we observe the AS_PATH, and we identify the nationality of all the ASes in the path, as Russian, Ukrainian, or other country. If the second AS in the path (the one after the origin) is Russian for Ukrainian origin or Ukrainian for Russian origin, we flag the announcement as suspect. We then consider only announcements whose peer AS (i.e., the AS communicating with the route collector) is of a different country from the suspect attacker. Thus, if the origin AS is Ukrainian, and the suspect attacker is Russian, the peer has to be not Russian, and vice-versa. This is because if the announcement is destined to the same country of the suspect attacker, it could be just a normal path traversing that country. As can be observed, in both Ukraine and Russia, the number of suspect Sub-Prefix and Its AS Hijacks shows a peak two days before the start of the war. The peak reaches approximately 600 000 announcements for Ukrainian AS victims, and 100 000 announcements for Russian AS victims. In both cases, the trend of these suspect attacks is intermittent during the war period. However, in the first days of the war, the activity seems more prominent for Russian suspect attacks. In Ukraine, the average number of targeted prefixes per day is 921.3 before the start of the war and 638.8 after, spread in on average 113 and 95.3 ASes. This happens because of the contribution of the peak a couple of days before the start of the war. The total number of targeted Ukrainian prefixes is 4686, spread in 244 ASes. For Russia, the phenomenon is smaller and basically flat, with 112.1 daily average targeted prefixes before the start of the war and 92.9 after, spread in 38.3 and 33.6 ASes. The total number of targeted prefixes for Russia is 719, in 111 ASes. These numbers seem to confirm the previous considerations made on BGP updates.

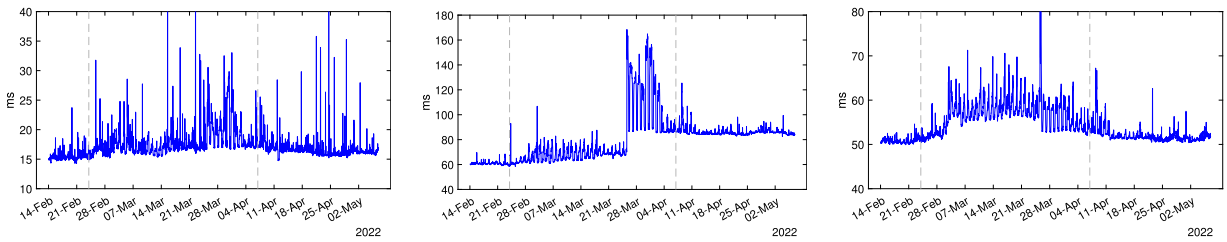
We then consider the suspect Sub-Prefix and Its AS Hijacks, shown in the fourth row of Fig. 7(a) and Fig. 7(b). We identify these announcements as in the previous case, but, in this case, we consider sub-prefixes of the prefixes in our table. For Ukrainian attackers and Russian victims, the activity is not so clear: the plot starts with a peak of over 4000 announcements, then shows some other peaks, but, in general, the activity seems quite marginal. Instead, in the case of Russian attackers and Ukrainian victims, the plot shows almost no activity before the start of the invasion, and a more pronounced activity during the war period, especially in the first phase of the war. The average daily number of Ukrainian targeted prefixes is 16.1 before the start of the war and 51.2 after (1.8 and 4.2 ASes). In four days, respectively on 7–8 Mar 2022 and 16–17 Mar 2022, the number of targeted prefixes is particularly high, ranging between 102 and 273. This increment is not reflected in the targeted ASes. The total number of Ukrainian targeted prefixes is 1573, in just 15 ASes. In Russia, the average number of targeted prefixes is 5.6 before the start of the war, and 2.3 after, spread in 1.3 and 1.1 ASes respectively. This reflects the peak in the BGP updates highlighted above. The total number of Russian targeted prefixes is 46, spread over 5 ASes. This confirms that this type of suspect activity is quite marginal in Russia.

For all the considered cases, we computed the number of suspect attackers per country in the entire observation period. For Ukraine, the total number of suspect attackers is 54, and for Russia 73. To highlight the individual contribution, we computed the number of suspect BGP announcements per possible attacker, and we plotted the distribution for both countries (Fig. 8). The long tail of the distribution prevents the observation of the details, however, half of the suspect attackers in both Ukraine and Russia are involved in over 20 000 BGP announcements. However, the top attackers in Ukraine and Russia are involved in 1.25 and 5.25 million BGP announcements, respectively, which account for 25.8% and 34.2% of the total suspect BGP announcements for their countries. The top 10% of suspect attackers account for approximately 70% of suspect BGP announcements. This highlights how the suspect BGP hijacks are mainly concentrated among just a handful of attackers.

Finally, we show an interesting phenomenon, which was already partially highlighted in the previous sections. In Fig. 9, we show the number of BGP announcements produced by Ukrainian and Russian ASes that started routing their own sub-prefixes. As can be observed, for both countries, the activity goes from almost zero to very high peaks, i.e., 6 000 000 announcements for Ukraine and 600 000 announcements for Russia. This activity could be due to ASes that try to defend from hijack attacks, or Sub-Prefix and Its AS attacks carried out by other ASes that are neither Russian nor Ukrainian. However, as pointed out in [27], BGP activity can be triggered also by malfunctions or attacks in other cyber domains, such as worms or viruses spread.

3.5. Discussion

In this section, we provided a quantitative analysis of the phenomena that occurred in the Russian and Ukrainian Internet during the



(a) UA (b) RU (c) Europe

Fig. 10. Average latency, 30 min buckets, from UA-located probes to targets located in UA, RU, and Europe.

Russian invasion of Ukraine, from an inter-domain routing standpoint. We also provided some of the reasons that could explain these phenomena, however, explaining the true reasons behind them is almost impossible, as it would require being on site where and when the actions occur. This is obviously beyond the authors' possibilities and the scope of this paper. However, despite the hypothetical nature of a few considerations, we strongly believe that the value of the quantitative analysis underlying them provides an unprecedented measure of the conflict impact on the Internet.

4. Impact on latency

We collected raw latency data about the Ukrainian Internet using RIPE Atlas [24]. Atlas is an Internet measurement platform managed by RIPE NCC, with an extensive presence in Europe and thus particularly suitable for observing the performance of the Internet in Ukraine.

The results of Atlas measurements are collected and stored in the Atlas backend infrastructure. Such measurements have been frequently used in the past for monitoring the status of critical Internet infrastructure, such as DNSMON [28], or for research purposes, such as evaluating the locality of Internet paths [29,30]. Internet performance is monitored using classical network tools. In particular, latency is observed using the ICMP-based version of ping. Each time a latency measure is triggered, a probe collects three RTT samples toward the considered target.

AMs are particularly useful to observe the presence of possible variations in the performance of the Internet in a region because they are generally periodic. This allows comparing the performance of some networks at a given time to a stable baseline. Similarly to the routing analysis, we used the AMs falling in the period from 14 Feb 2022 to 7 May 2022, and the initial ten days are the baseline against which the performance during the war is compared. To avoid that some pairs of nodes participating in the measurements were available only during a small fraction of the considered period, we removed all the measurements originated by source–target pairs that were unavailable for more than 50% of the period. The position of Atlas nodes is known, as it has to be provided by the hosting individual or organization. Latency values have been aggregated using bins with a duration of 30 min. In particular, we computed the average value of the three samples collected at each measurement attempt, and then computed the average for all the values falling in the same bin. Each different source–target pair has been included only once per bin, so that the result is not biased by pairs that produce more results than other pairs.

We studied the impact of the war on the latency of the Internet in Ukraine when both source and destination are in Ukraine (UA→UA), and when the source is in Ukraine and the target is outside the country and located in Russia or Europe (UA→RU, UA→Europe). In this study, Europe includes all countries of the European continent with the exception of Russia and Ukraine. Fig. 10 shows the ICMP-based latency for the three considered possible positions of the targets. In all cases, the latency increases significantly after the start of the war, identified by the first dashed line on the plots. The average latency after 24 Feb, is higher than the ones observed in the 10 days before the start of the conflict. The increase is +13%, +35.5%, and +7.8% for the UA→UA, UA→RU, UA→Europe scenarios, respectively. The periodic peaks that are visible throughout the monitored period are related to the different loads imposed on the network by human-driven activities, higher during the day and lower during night-time. Peaks become more evident during the conflict, compared to the baseline period. The standard deviation of latency during the war is approximately 3.4 times the one observed before the conflict for the UA→UA scenario. The increase is even larger for the other two scenarios: 15.4 for UA→RU and 6.7 times for UA→Europe. It is interesting to notice that the degradation of performance for the UA→RU scenario is worse than the UA→UA one. The plots also report a second dashed line, corresponding to a second phase of the conflict (7 Apr) when battles started concentrating in the southeast part of Ukraine.

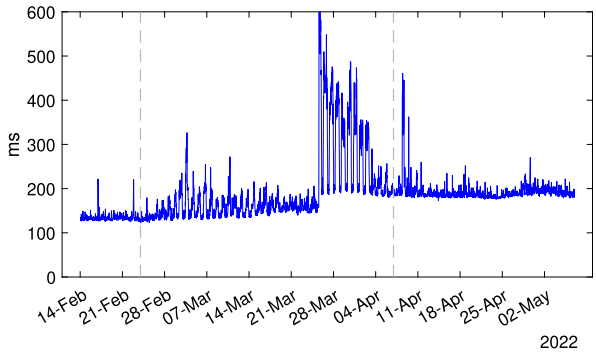


Fig. 11. UA→RU average latency, HTTP, 30 min bins.

We also estimated the packet loss by counting the number of missing echo replies, again using 30 min bins. The packet loss increases significantly after the start of the war: +249% for the UA→UA scenario, compared to the baseline period.

Finally, we studied the latency at the HTTP level, by relying on part of AMs carried out using such a protocol. Results are shown in Fig. 11 for the UA→RU scenario. Similarly to the other observed latency metrics, the HTTP-level latency becomes much higher and variable during the conflict (+44.2% and +593%, in terms of average and standard deviation). The bump in terms of BGP updates starting at the end of March and discussed in the previous sections is significantly overlapped with the period characterized by the largest fluctuations in HTTP latency.

Besides increased variability, Fig. 10(b) shows a step-like trend when considering the minimum values of latency. The same step-like trend is visible in Fig. 11, where again sources are located in UA and targets in RU. To understand the causes of such an increase in the minimum latency, we analyzed the first 10 weeks of data as follows. First, we selected all the source–target pairs that include a step-like trend and then analyzed their paths at the AS level. In particular, we retrieved a set of traceroute measurements involving the selected source–target pairs and obtained the AS number for each IP address found in the path using RIPEstat. We also checked whether the IP addresses belonged to

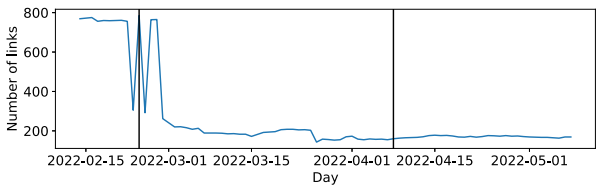


Fig. 12. Number of links in the Ukrainian AS-level topology that directly connect Ukrainian ASes to Russian ASes.

an IXP, using data extracted from PeeringDB [31], or to a Tier 1 AS,[2] using to this purpose the list provided in [32]. Then, we compared the first week of measurements with the last one, looking for ASes that disappeared from the paths or that started being involved. The AS that was abandoned more frequently was Megafon (RU, AS31133), followed by Dataline (UA, AS35297). We also observed that during the last week of measurements, some IXPs were not included anymore in the paths of the selected source–target pairs. The IXPs that were not present anymore are MSK-IX (RU), DE-CIX (DE), and DTEL-IX (UA), in order of decreasing frequency. At the same time, some IXPs started being used, in particular NL-IX (NL). The overall decreasing number of paths involving an IXP was accompanied by a larger adoption of Tier-1s, in particular Lumen (AS3356), Cogent (AS174), Arelion (AS1299). In many cases, the paths that showed the step-like trend in the end-to-end latency appear to have as a common factor a partial shift from peering to transit, thus involving companies located higher in the Internet hierarchy. This can be due in some cases to the mutated relationship between the two countries and in other cases to the unavailability of infrastructure. To further confirm this analysis of the phenomenon, we computed the average rank and the average customer cone of all the ASes found in the paths using the data provided by ASRank [33]. In ASRank, the AS with the largest customer cone is given rank 1. The customer cone of an AS is the set of ASes that can be reached from such AS when following only provider-to-customer links in the AS graph. The average rank during the first week of measurements (before the start of the conflict) was 400, whereas the average size of the customer cone was 1272. During the last week of measurements, the two values were 256 and 8461, respectively.

We extended this analysis by computing the Internet topology as seen from the Ukrainian perspective during the whole observation period ($\sim$ 12 weeks). To do so, we used the software in [32]. For each Ukrainian AS, the software collects all its neighbors from RIPEstat, which in turn extracts this information from BGP data collected by RIPE RIS. The Ukrainian topology was collected in daily snapshots, and, for each day, we computed the number of direct links between Ukrainian and Russian ASes. The results are depicted in Fig. 12. As can be noticed, the number of links connecting Ukrainian and Russian ASes experiences a sudden drop, from almost 800 to approximately 200, after some days of instability, right after the start of the war. We then compared the first week of measurements with the last one. We collected all the direct links between Ukrainian and Russian ASes in the first week and in the last week. From these links, we extracted the ASes involved, divided by country, Russia and Ukraine. For each AS, we then computed how many links it establishes. The number of Ukrainian ASes establishing links with Russian ASes is 30 in the first week and 19 in the last week, which means that approximately 30% of Ukrainian ASes interrupted their direct connections with Russian ASes. The number of Russian ASes is instead 523 in the first week and 22 in the last week, thus just 4% of ASes are still directly connecting with Ukrainian ASes. For these two sets of ASes, we then computed the average customer cone size, for the first and the last week of measurements. In the first week, the average customer cone size for Ukrainian ASes directly connected to Russian ASes is 105, while in the last week it is 160. For Russian ASes, the average customer cone size is 51 in the first week, and 912 in the last week. This means that just the biggest ASes, in terms of customer cone size, are still maintaining a direct connection with ASes of the other country. This is particularly evident for Russian ASes. It must be noticed that a single Ukrainian AS was establishing most of the links with Russian ASes, i.e. 481 links. In the last week, none of these links is still active.

[2] A Tier 1 AS is an AS that contributes to international connectivity. The distinctive trait of Tier 1 ASes is that they are at the top of the hierarchy of the Internet AS-level graph. Tier 1 ASes, in other words, do not have any providers.

5. Conclusion

The Ukraine–Russia conflict is one of the major catastrophic events occurring to a large country since when the Internet started playing a fundamental role in our society. The Internet is not only the cornerstone of the business and communications sectors, but also a key medium for individuals who need to access news in difficult times. According to ITU data, 75% of the Ukraine population has access to the Internet, compared to 63% of the world population [34]. For Russia, the same indicator has a value of 83%. This shows how important is the Internet in such societies and economies.

Our analysis provides a quantitative estimation of the impact of the conflict on the Ukrainian Internet. Data shows an intense rise of activity from the inter-domain routing standpoint, together with some suspicious activity that could be ascribed to cyberattacks. Some Ukrainian ASes got disconnected from the Internet as the Russian invasion proceeded, but in the last period of the observation they seem to start getting back online. The war activities impacted also other Internet-related aspects, with increased latency and an AS-level topology reconfiguration which saw Russian and Ukrainian ASes cease their direct connections. Despite the intense rise in BGP activity and the increased latency, the Ukrainian Internet proved to be quite resilient: considering the probes that were connected during the first week of the monitored period, approximately 83% of them were connected also during the last week.

CRediT authorship contribution statement

Valerio Luconi: Conceptualization, Methodology, Software, Investigation, Formal analysis, Data curation, Validation, Visualization, Writing – original draft, Writing – review & editing. **Alessio Vecchio:** Methodology, Software, Investigation, Formal analysis, Data curation, Validation, Visualization, Writing – original draft, Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This work is partially funded by the Italian Ministry of University and Research (MUR) in the framework of the CrossLab project (Departments of Excellence). We thank Massimo Candela, Ph.D. for the precious comments and suggestions. The views expressed are solely those of the authors.

References

[1] R. Fontugne, K. Ermoshina, E. Aben, The internet in crimea: a case study on routing interregnum, in: 2020 IFIP Networking Conference (Networking), 2020, pp. 809–814.

[2] K. Limonier, F. Douzet, L. Pétiniaud, L. Salamatian, K. Salamatian, Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine, First Monday 26 (5) (2021).

[3] J. Graham-Cumming, Internet traffic patterns in Ukraine since February 21, 2022, 2022, https://blog.cloudflare.com/internet-traffic-patterns-in-ukraine-since-february-21-2022/. (Accessed: 2022-08-11),

[4] M. Prince, Steps we've taken around Cloudflare's services in Ukraine, Belarus, and Russia, 2022, https://blog.cloudflare.com/steps-taken-around-cloudflares-services-in-ukraine-belarus-and-russia/. (Accessed: 2022-08-11),

[5] A. Siddiqui, Did Ukraine suffer a BGP hijack and how can networks protect themselves? 2022, https://www.manrs.org/2022/03/did-ukraine-suffer-a-bgp-hijack-and-how-can-networks-protect-themselves. (Accessed: 2022-08-11),

[6] E. Aben, The resilience of the internet in Ukraine, https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine/.

[7] A. Jain, D. Patra, P. Xu, J. Sherry, P. Gill, The ukrainian internet under attack: An NDT perspective, in: Proceedings of the 22nd ACM Internet Measurement Conference, IMC '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 166–178, http://dx.doi.org/10.1145/3517745.3561449.

[8] M. Jonker, G. Akiwate, A. Affinito, k. Claffy, A. Botta, G.M. Voelker, R. van Rijswijk-Deij, S. Savage, Where .ru? Assessing the impact of conflict on Russian domain infrastructure, in: Proceedings of the 22nd ACM Internet Measurement Conference, IMC '22, Association for Computing Machinery, New York, NY, USA, 2022, pp. 159–165, http://dx.doi.org/10.1145/3517745.3561423.

[9] K. Cho, C. Pelsser, R. Bush, Y. Won, The Japan Earthquake: The Impact on Traffic and Routing Observed by a Local ISP, in: Proceedings of the Special Workshop on Internet and Disasters, SWID '11, Association for Computing Machinery, 2011.

[10] J. Heidemann, L. Quan, Y. Pradkin, A Preliminary Analysis of Network Outages During Hurricane Sandy, Tech. Rep., (ISI-TR-2008-685b) USC/Information Sciences Institute, 2012.

[11] T. Favale, F. Soro, M. Trevisan, I. Drago, M. Mellia, Campus traffic and e-Learning during COVID-19 pandemic, Comput. Netw. 176 (2020) 107290.

[12] M. Candela, V. Luconi, A. Vecchio, Impact of the COVID-19 pandemic on the Internet latency: A large-scale study, Comput. Netw. 182 (2020) 107495.

[13] A. Feldmann, O. Gasser, F. Lichtblau, E. Pujol, I. Poese, C. Dietzel, D. Wagner, M. Wichtlhuber, J. Tapiador, N. Vallina-Rodriguez, O. Hohlfeld, G. Smaragdakis, The lockdown effect: Implications of the COVID-19 pandemic on internet traffic, in: Proceedings of the ACM Internet Measurement Conference, IMC '20, Association for Computing Machinery, New York, NY, USA, 2020, pp. 1–18, http://dx.doi.org/10.1145/3419394.3423658.

[14] X. Zhuo, B. Wellman, J. Yu, Egypt: The first internet revolt? Peace Mag. 27 (3) (2011) 6–10.

[15] J. Groshek, Forecasting and observing: A cross-methodological consideration of Internet and mobile phone diffusion in the Egyptian revolt, Int. Commun. Gazette 74 (8) (2012) 750–768.

[16] S.A. Jyothi, Solar superstorms: Planning for an internet apocalypse, in: Proceedings of the 2021 ACM SIGCOMM 2021 Conference, Association for Computing Machinery, 2021, pp. 692–704.

[17] E.K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, J.P.G. Sterbenz, Modelling communication network challenges for Future Internet resilience, survivability, and disruption tolerance: a simulation-based approach, Telecommun. Syst. 52 (2) (2013) 751–766.

[18] RIPE Network Coordination Center. https://www.ripe.net/. (Accessed: 2022-08-11).

[19] RIPE NCC Routing Information Base. https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris. (Accessed: 2022-07-20).

[20] Y. Rekhter, S. Hares, T. Li, A Border Gateway Protocol 4 (BGP-4), 2006, RFC 4271.

[21] L. Blunk, C. Labovitz, M. Karir, Multi-Threaded Routing Toolkit (MRT) Routing Information Export Format, RFC, (6396) 2011, http://dx.doi.org/10.17487/RFC6396, URL https://www.rfc-editor.org/info/rfc6396.

[22] BGPStream. https://bgpstream.caida.org/. (Accessed: 2022-07-20).

[23] RIPEstat, https://stat.ripe.net/. (Accessed: 2022-07-20).

[24] RIPE NCC Staff, Ripe atlas: A global internet measurement network, Internet Protoc. J. 18 (3) (2015).

[25] Timeline of the 2022 Russian invasion of Ukraine, https://en.wikipedia.org/wiki/Timeline_of_the_2022_Russian_invasion_of_Ukraine. (Accessed: 2022-07-20).

[26] K.Z. Sediqi, L. Prehn, O. Gasser, Hyper-specific prefixes: Gotta enjoy the little things in interdomain routing, SIGCOMM Comput. Commun. Rev. 52 (2) (2022) 20–34.

[27] B. Al-Musawi, P. Branch, G. Armitage, BGP Anomaly Detection Techniques: A Survey, IEEE Commun. Surv. Tutor. 19 (1) (2017) 377–396.

[28] C. Amin, M. Candela, D. Karrenberg, R. Kisteleki, A. Strikos, Visualization and Monitoring for the Identification and Analysis of DNS Issues, in: Proceedings of the Tenth International Conference on Internet Monitoring and Protection, 2015.

[29] M. Candela, V. Luconi, A. Vecchio, A worldwide study on the geographic locality of Internet routes, Comput. Netw. 201 (2021) 108555, http://dx.doi.org/10.1016/j.comnet.2021.108555, URL https://www.sciencedirect.com/science/article/pii/S1389128621004734.

[30] M. Candela, E. Gregori, V. Luconi, A. Vecchio, Dissecting the speed-of-internet of middle east, in: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2019, pp. 720–725, http://dx.doi.org/10.1109/INFCOMW.2019.8845104.

[31] PeeringDB, https://www.peeringdb.com/. (Accessed: 2022-08-10).

[32] Visualising AS Hegemony per country, https://github.com/InternetHealthReport/country-as-hegemony-viz. (Accessed: 2022-08-11).

[33] CAIDA AS Rank, http://as-rank.caida.org. (Accessed: 2022-07-20).

[34] ITU DataHub, https://datahub.itu.int/. (Accessed: 2022-08-10).

Valerio Luconi received the master's and Ph.D. degrees in computer engineering from the University of Pisa, in 2012 and 2016, respectively. He is currently a Researcher with IIT-CNR, Pisa. His research interests include Internet measurements, the Internet topology, IP geolocation, network neutrality, and network monitoring.

Alessio Vecchio is an associate professor at the University of Pisa, Italy. He has been involved in several national and EU-funded projects (CONGAS, NeutMon, MECPerf). He is currently serving as associate editor of Pervasive and Mobile Computing and IEEE Access. He co-launched and co-organized five editions of the PerMoby workshop (an IEEE PerCom workshop focusing on human mobility). He has been TPC chair of the Seventh IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing (IEEE PerCom PerSeNS) and in the technical committee of many other international events.