The Ukrainian Internet Under Attack: an NDT Perspective

Akshath Jain*
Carnegie Mellon University
Pittsburgh, PA, USA

Deepayan Patra*
Carnegie Mellon University
Pittsburgh, PA, USA

Peijing Xu*
Carnegie Mellon University
Pittsburgh, PA, USA

Justine Sherry
Carnegie Mellon University
Pittsburgh, PA, USA

Phillipa Gill
Google
New York, NY, USA

Abstract

On February 24, 2022, Russia began a large-scale invasion of Ukraine, the first widespread conflict in a country with high levels of network penetration. Because the Internet was designed with resilience under warfare in mind, the war in Ukraine offers the networking community a unique opportunity to evaluate whether and to what extent this design goal has been realized. We provide an early glimpse at Ukrainian network resilience over 54 days of war using data from Measurement Lab's Network Diagnostic Tool (NDT). We find that NDT users' network performance did indeed degrade – *e.g.* with average packet loss rates increasing by as much as 500% relative to pre-wartime baselines in some regions – and that the intensity of the degradation correlated with the presence of Russian troops in the region. Performance degradation also correlated with changes in traceroute paths; we observed an increase in path diversity and significant changes to routing decisions at Ukrainian border Autonomous Systems (ASes) post-invasion. Overall, the use of diverse and changing paths speaks to the resilience of the Internet's underlying routing algorithms, while the correlated degradation in performance highlights a need for continued efforts to ensure usability and stability during war.

CCS Concepts

• **Networks** → **Network measurement**.

ACM Reference Format:
Akshath Jain, Deepayan Patra, Peijing Xu, Justine Sherry, and Phillipa Gill. 2022. The Ukrainian Internet Under Attack: an NDT Perspective. In *ACM Internet Measurement Conference (IMC '22), October 25–27, 2022, Nice, France.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3517745.3561449

1 Introduction

The Internet was designed from first principles to be resilient. Early research emphasized redundancy and reliability in the face of war: partially damaging Internet infrastructure should not take down the entire system [4, 11]. Decades later, the Internet has become an essential, worldwide network of communication, information, and content, making Internet resilience all the more critical.

The present Russian invasion of Ukraine offers an unprecedented case study of Internet resilience. Ukraine is an emerging Internet economy [47]: from 2007 to 2019, Ukrainian's Internet penetration grew at a staggering rate, skyrocketing from 6.5% to over 70% [45]. With heavy destruction in cities across the country, millions fleeing their homes for safety [1], and cyberattacks on national infrastructure [17, 29, 36, 44], the country's Internet infrastructure has been heavily tested. Studying such changes to Internet usability and infrastructure over time and across regions enables us to characterize the network's resilience in disaster scenarios. To this end, we present an analysis of the state of the Internet in Ukraine by evaluating core connection quality metrics and link these observations to Internet routing changes.

The main source of data for our analysis comes from Measurement Lab (M-Lab), an open-source project providing open access to measurements of global network performance [33]. Namely, we use data from the Network Diagnostic Tool (NDT), which provides statistics on throughput, latency, and loss for a connection's "bulk transport capacity" [31]. Using the NDT data, we detect degradation of three key metrics: decreased throughput, increased latency, and increased packet loss – especially in regions that have encountered the most conflict. To the best of our knowledge, this work is the first study of user-perceived performance during the Ukrainian war.

We also use `traceroute` data from M-Lab's to characterize routing pre- and post- invasion [32]. We find that routing between clients and M-Lab servers take previously unused routes, and that clients with more new routes observed were also more likely to experience performance degradation. We also aggregated hops in the `traceroutes` by the AS to which they belong, and observed some major shifts in routing – with a notable shift for traffic entering Ukraine towards paths through Hurricane Electric over previously utilized ASes.

Our analysis of the `traceroute` data shows only a mild correlation of route updates with performance degradation. Hence, based on this analysis, we hypothesize that most of the performance instability occurs due to damage at the edge of the network, *e.g.* cell towers and consumer-facing networks. However, network data from this conflict still remains early and sparse, and this hypothesis remains to be validated.

The rest of the paper is organized as follows: in Section 2, we present background for the events in the war; in Section 3, we provide details on our chosen data sources; in Sections 4 and 5, we

*These authors contributed equally to this work.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
IMC '22, October 25–27, 2022, Nice, France
© 2022 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9259-4/22/10.
https://doi.org/10.1145/3517745.3561449

DRAFT

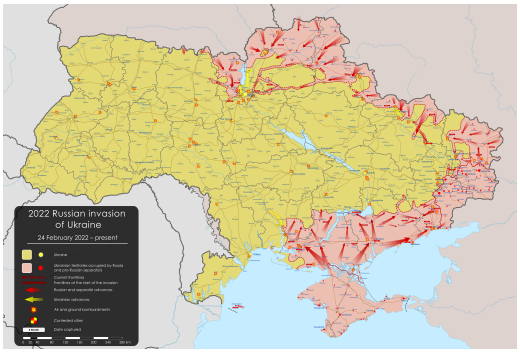


Figure 1: Areas of military activity as of March 20, 2022 (approximate date of maximum Russian occupied territory in Ukraine within the window of analysis) [13]. Shaded regions to the North, South, and East are controlled by Russian forces.

present our studies on Ukraine's network statistics and Internet infrastructure; in Section 6, we present prior work in large-scale Internet studies; finally, we conclude our study.

2 Motivation and Related Work

We focus our study on the first 54 days after the Russian invasion of Ukraine. The invasion began on February 24, 2022 [12]; military scholars identify a few key milestones in the conflict in April with Ukrainian forces winning the battle of Kyiv and forcing Russian withdrawal from the capitol (April 3 [12]). Our data analysis stops on April 18th, 2022; as reported by the Institute for the Study of War, the Northern, Eastern, and Southern fronts of Ukraine are areas which underwent direct assault during this period of the invasion [12]. Regions in the Southeast are controlled by Russian forces. The Northern region around Kyiv has been regained by Ukraine but still experiences substantial military action. The Western regions, including the city of Lviv, have largely been spared from fighting during the first months of the war. Our data analysis stops on April 18th, 2022; the contemporary state of military action is shown in Figure 1. In particular, the Northern, Eastern, and Southern fronts of Ukraine are under direct assault. Shaded regions in the Southeast are controlled by Russian forces, the Northern region around Kyiv has been regained by Ukraine but still experiences substantial military action. As we will show later in Section 4.2, performance degradation during the period of study is highest in these militarily active regions.

Characterizing Internet Degradation during the War: Communication networks constitute critical infrastructure and historically have been targeted during wartime [40]. Modern network measurement technologies present a unique opportunity for researchers to independently observe the impacts of the Ukrainian conflict on the Internet infrastructure. These observations can shed light on the impacts of the conflict in near real time and inform our understanding of the Internet's resilience during conflict.

Engineers and researchers have already published blog posts on the effects of the war on Ukraine's network structure, noting decreases in reachability for addresses based in the most heavily shelled cities [20], momentary disruptions to ISPs with the goal of subversion [2], and studies in network concentration and ISP resilience [3]. News sources have reported on the bravery and heroism of network engineers fixing damaged infrastructure in the country who have been able to preserve many services for Ukrainian citizens [8, 42] and some speculation on a lower volume of attacks on network infrastructure than expected [17]. Some prominent Internet researchers and contributors have also shared information on and analysis of Internet events in these countries on Twitter threads [15, 44].

Insights from NDT: Information about the state of network connectivity in Ukraine remains early and sparse. To the best of our knowledge, no widespread studies yet exist looking into user-experienced performance in the Ukrainian war. Hence, to complement the existing data and open new lines of inquiry regarding network performance under war, we investigate crowd-sourced data from Measurement Lab's Network Diagnostic Tool (NDT). Relative to existing data, NDT offers new insights into Ukrainian network degradation by providing data about user-perceived *performance* – *e.g.* throughput, latency, and loss rate. Using the NDT data, our goal is to understand: (1) whether and to what extent NDT users have experienced performance degradation during the war; (2) whether or not any statistically significant performance degradation is correlated with military activity; and (3) whether or not we observe shifts in core routing that are also correlated with degraded performance.

3 Methodology

We use data from Measurement Lab (M-Lab), an open-source project focusing on global measurement of network performance. M-Lab hosts a range of measurement services on a distributed platform of 210 sites in 47 countries around the world. Each site is connected to a distinct transit provider and a load balancing service directs each client to a measurement site that is geographically nearest to them. A suite of "sidecar" services run alongside each measurement service to collect packet captures and perform a traceroute (using `scamper`) towards the client [32].

The NDT dataset: This paper uses data from the Measurement Lab's (M-Lab) Network Diagnostic Tool (NDT) [33]. The NDT client is integrated into a variety of platforms with ~90% of NDT's data collected via its integration with Google search [21, 23]. On average there are over 4 million NDT tests performed each day from clients in over 200 countries and territories as of May 2022 [31].

NDT tests the client's network connectivity by downloading / uploading an object via a WebSocket over TLS. It aims to capture how fast the client's device can send/receive data using a single TCP connection. Earlier versions of NDT (*e.g.* NDT5) used TCP Reno or Cubic with the current version (NDT7) using BBR if available. In both cases, statistics about the connection are collected from the TCP_INFO structure. We use the mean throughput, minimum RTT, and loss rate statistics in our analysis.

We analyze download measurements made by NDT clients in the 108-day time range spanning from January 1, 2022 to April 18, 2022. This includes the 54 days preceding the invasion on February 24 and the first 54 days following it. We refer to these two periods as **prewar** and **wartime**, respectively. We chose a time period spanning several weeks, on either end, to ensure that we were analyzing trends within the data – and not daily / weekly fluctuations. Though the exact number of days is not important, this time range provided sufficient data to compare the Ukrainian Internet between the two periods. We use the client's geolocation, determined by MaxMind [38], and

DRAFT

published with the NDT data to identify tests from clients in Ukraine. We note that there are no NDT servers in Russia for tests originating in Ukraine, so we do not expect changes and influences on Russia's Internet infrastructure to affect the data collected.

To validate that our observed changes are linked to the invasion and are not spurious, we established baseline measurements over the same periods in 2021 (January 1 to April 18). We refer to the first 54 days of the period in 2021 as **baseline Jan-Feb, 2021** and the latter 54 days as **baseline Feb-Apr, 2021**. We expect that traffic in early 2021 reflects relative normalcy in the country (therefore matching the prewar measurements), and was not affected by the initial spike in traffic in at the start of the pandemic in early 2020 [7, 19, 35].

We find it important to note that while NDT's testing protocols and algorithms have changed over time, the congestion control algorithm was stable in the period from 2021-2022 we studied [30, 31].

Limitations: We acknowledge that data collected using the NDT tool is subject to some known limitations. The first is sampling bias – Internet speed tests are typically performed when users already experience degradation on their Internet service.

Second, our data only shows performance degradation for Internet connections that are currently functional and will not show portions of the network where access is cut off completely.

Third, is another form of sampling bias: taking Internet speed tests during wartime is a low priority activity. As a result, we would expect a drop in the number of count of Internet tests, resulting in fewer data points. However, as shown in Figures 2a and 3a, test counts are relatively stable, and we see at most a 2% decrease in tests from prewar to wartime, indicating that this form of bias is limited.

Finally, the geolocation data used for more precise analysis is not perfectly accurate. However, MaxMind's self-reported accuracy for **labeled** geolocation data is > 68% at a resolution of 25 km [37]. While it is possible that incorrectly labeled data causes biases in our dataset, we expect incorrect labels would skew results to be less significant, strengthening our results. We focus largely on cities expecting heavy damage from war; should datapoints from less damaged areas be mislabeled to these cities, we suspect performance would improve rather than worsen. The relatively high rate of city-level accuracy the MaxMind geolocation dataset provides and nature of the biases give us confidence on the measures conducted. Of the tests considered, only 9,200 of the 78,539 NDT tests (11.7%) during the 108-day period do not have geospatial data associated with the client, and these tests are not considered in our location-based analyses.

We stress that the absolute values of the metrics reported should not be taken as a complete reflection of overall network quality in Ukraine. Their utility lies with providing a standard set of metrics to compare over time and across different regions, *i.e.* the relative changes and differences are the focuses of this paper.

4 Internet Service Quality

In this section, we seek to answer whether military operations in Ukraine led to the degradation in the user-perceived quality of Internet connections. We begin by viewing the metrics in aggregate across the entire nation, and proceed to describe their behavior in increasing levels of geographic granularity. We identified key cities and compared their NDT metrics before and after the start of the invasion. These cities are Kyiv - the nation's capital and most populous city, Kharkiv and Mariupol - two cities that have been under siege since early in the invasion [28, 34], and Lviv - the de facto "western capital" that has seen over 200,000 refugees arrive from other parts of the country [25, 43]. These cities were also chosen due to their extensive media coverage, which enables us to correlate our findings with geopolitical events in the region. We investigate potential causal events corresponding to dates where we observe significant metric changes, but largely leave date-level analysis to future work.

4.1 Nation-Level Metrics

At the national level, these effects are clearly observable in the NDT data as shown in Figure 2. After the invasion began on February 24, there is a sharp increase in the average connection loss rate (2d) as well as minimum RTT (2b). The degradation becomes apparent in just a few days. Not only is there higher loss, higher RTT, and lower throughput, these metrics also fluctuate more day-to-day, which indicates more instability and unreliability. We do see that after an initial significant change in throughput and loss rate, these metrics began reverting towards pre-invasion levels. Mean download speed (2c) sees a 50% decrease with a corresponding spike in test counts (2a) near March 10, suggesting a large-scale outage, corroborated by other Internet analysts [36]. We also show that these significant changes in the metrics do not appear in the baseline from 2021, as evident in Figure 2.

4.2 Region-Level Metrics

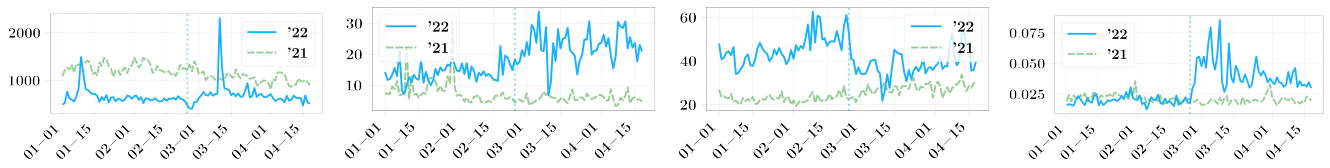
Key metrics also correlated with active war-zones at a regional level. In Ukraine, an administrative region is known as an oblast. As shown in Figure 3, we have considerable changes in each of the four primary metrics: decrease in test counts (3a), increase in MinRTT (3b), decrease in mean download speed (3c), and increase in loss rate (3d). Curiously, the change in Figure 3a is far less than its counterparts (3b, 3c, 3d). This indicates that test counts remained fairly stable from prewar to wartime and helps ensure that wartime test counts were relatively unbiased compared to prewar test counts. In particular, we see that oblasts in the North and Southeast are directly correlated with worsening metrics – the same regions with active conflict.

4.3 City-Level Metrics

Our analysis of the NDT metrics at the city level further links poor connection quality to contested regions with active conflict. In Kyiv, Kharkiv, and Mariupol, there is a statistically significant decrease in quality across metrics. Table 1 shows the means of the metrics pre- and post-invasion. We note that such changes are not seen in the 2021 baseline and attributable to the disruption of Internet infrastructure in the contested regions. Lviv, however, does not encounter any statistically significant changes in the measured periods. As of April 21, Lviv has seen some attacks, including a missile bombardment on April 18 [26]. Though the situation in Lviv is rapidly changing, it appears that degradation in the Internet quality of some regions does not have an immediate cascading effect on the entire country.

We also present the NDT test counts from the cities of Kharkiv and Mariupol. Both cities have been the target of concentrated besieging. Generally, a sudden increase in NDT test counts is likely a signal of Internet issues, but a sudden decrease does not necessarily mean an improvement in Internet quality. Figure 4 shows NDT test

DRAFT

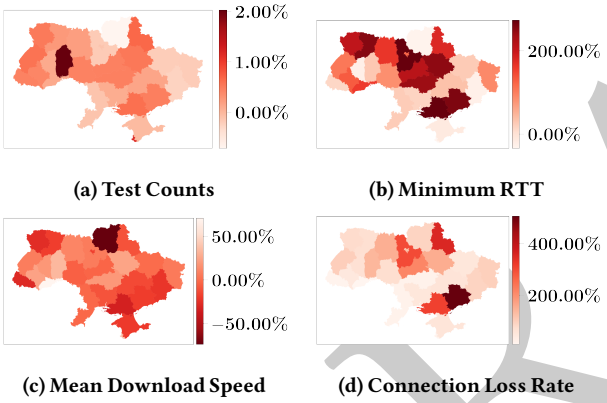


(a) Test Counts (b) Minimum RTT (ms) (c) Mean Goodput (Mbps) (d) Connection Loss Rate

Figure 2: For each metric, the figures show the daily mean of all NDT download tests originating from Ukraine. The dotted, vertical line indicates February 24, 2022, the start of the invasion.

Table 1: City level metrics compared before and after the invasion in 2022. Welch's t-test is used for statistical significance ($p < 0.05$). A "*" indicates a statistically significant change.

	# Tests		MinRTT (ms)			MeanTput (Mbps)			LossRate (%)		
	Prewar	Wartime	Prewar	Wartime	p-value	Prewar	Wartime	p-value	Prewar	Wartime	p-value
Kyiv	10023	8513	11.340	26.613	***2.6E-60**	64.02	50.86	***4.1E-43**	1.37	3.14	***1.3E-122**
Kharkiv	1839	1215	23.099	31.669	***3.7E-10**	45.45	52.70	***2.0E-06**	2.34	3.32	***1.8E-08**
Mariupol	296	26	17.668	17.103	9.2E-01	32.88	18.80	***2.1E-02**	2.79	6.84	***1.0E-04**
Lviv	1315	1857	5.563	11.942	***1.3E-18**	39.37	41.85	1.9E-01	1.73	3.29	***7.6E-17**
National	35488	37815	13.807	21.734	***9.3E-57**	45.06	37.34	***1.4E-86**	1.97	4.14	***0.0**



(a) Test Counts (b) Minimum RTT

(c) Mean Download Speed (d) Connection Loss Rate

Figure 3: The graphs show percentage changes of metrics on a per-oblast basis comparing wartime numbers to prewar numbers.

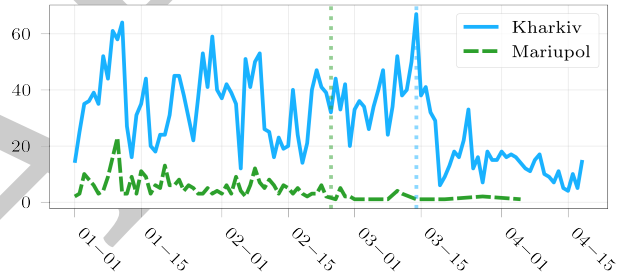


Figure 4: NDT download test counts from Kharkiv and Mariupol. The dashed lines mark the start of the invasion as well as a major shelling attack on Kharkiv on March 14.

counts from Mariupol all but disappear after March. This coincides with Russian forces surrounding the city on March 1 [34]. Similarly, we see a large drop in Kharkiv following March 14, after officials report over 600 residential buildings destroyed [28]. The disruption of civilian life by the conflict as people flee their homes explains the decrease in test counts as well as highlight the bias in the NDT data – if a person is fleeing for their safety, it is unlikely they will perform a speed test out of concern for the Internet service quality.

The trends we see in the test data are not unexpected. As people flee from active war zones, fewer users will be on the Internet in the region. As fighting leads to damaged networking infrastructure, the quality of service will decrease.

5 Routing and Resilience

We now focus our investigation to determine the root causes of the observed user connection degradation by analyzing architectural changes to the network. In this section, we present that the effects of the conflict demonstrate damage to routing infrastructure. We use M-Lab's `scamper` data set of `traceroute` data to investigate how routing in Ukraine has been impacted by the loss of routing infrastructure and whether specific ASes are disproportionately affected. We find significant changes in Ukraine's path and node-level infrastructure to correlate with the timeline of the invasion and provide evidence that these changes are connected to deteriorating connection quality during wartime. We additionally find evidence that Ukraine's network is responsive to performance changes and exhibits resilience in the face of network damage.

5.1 Routing Paths

In this section we study changes to routing decisions at a per-connection level. We consider a connection to be a (source, destination) pair of IP addresses and a path to be the `traceroute` IP address sequence used to satisfy a connection. We measure the use of new backup paths as a proxy for routing failures, hypothesizing that wartime events, perhaps outages or damaged infrastructure, cause disruptions that force the usage of alternative routes. Our hypothesis is grounded with an observed correlation between a diversification of path usage and degradation in connection quality in Ukraine, demonstrated in Appendix D.

DRAFT

Table 2: Average path and test counts for the top-1000 connections in 2021 and 2022.

	# Paths/Conn.	# Tests/Conn.
Baseline Jan-Feb, 2021	2.175	83.579
Baseline Feb-Apr, 2021	2.172	63.019
Prewar, 2022	3.281	210.910
Wartime, 2022	4.284	192.058

With these signals in mind, we consider the changes in routing for tests at large. We see a significant increase in the number of paths used per connection: as depicted in Table 2, the level of path diversity greatly increased after the start of the war, while during our baseline period in 2021, there was no corresponding change. In each of the periods under consideration, we take the 1000 connections with the greatest number of tests, and determine the average number of unique paths utilized during the period of study to serve these connections. On average, an arbitrary connection in this set used one more path after the start of the war, even with less traffic through the pair of endpoints.

We consider our results in this section a signal that preventative issues in network infrastructure modified routing behaviors, exhibiting some performance degradation as a result. That said, our observations also indicate the resiliency of the country's Internet infrastructure in adapting to changing network availability and stability. The use of alternative routes suggests readily available backup infrastructure able to cope with networking failures and provide more reliable service. We believe there is scope for future work to strengthen understanding of networking failures and their effects on key metrics. Our proxy metric considering unique paths as a measure of failure is imperfect, as it does not capture failures at the lowest level. A more tailored dataset correlating metrics to identified outages from infrastructure or human error would eliminate the need to use a proxy variable. Additional work on router alias resolution may also prove to be more precise than IP-level measurement [27].

5.2 Autonomous Systems

To understand the role of ASes in achieving high availability and resiliency in Ukraine, we investigate how they participate in routing and how participation changes after the invasion. For each `traceroute` that was carried out as a result of an NDT test originating from Ukraine, we made note of which AS each hop belonged to. We focus now on the top 10 most frequently occurring ASes, each of which appeared in over 10k tests, and the NDT traffic routed through them.

To varying degrees, even the 10 most frequently occurring ASes experienced significant degradation in latency, throughput, and loss that cannot be explained by natural fluctuations. As shown in Table 3, half of the top 10 ASes experienced over a 100% increase in RTT following February 24, and the average loss rate more than doubled for another set of 5 ASes. Over half of the ASes experienced statistically significant increases in RTT and loss. We performed the same analysis against the top 10 ASes from the same period in 2021 as a baseline. Even if we assume the worst degradation for each metric seen in the baseline is "natural," most of the top 10 ASes experience even greater increases in RTT or loss after the invasion.

However, different ASes – even those serving the same city – are impacted by the war in isolated and independent ways. For example,

Table 3: Changes in metrics that exceed the baseline (2021) fluctuations are underlined, while a * indicate statistical significance ($p < 0.05$) using Welch's T-test.

ASN	Name	Δ Counts	Δ TPut	Δ RTT	Δ Loss
15895	Kyivstar	+16.45%	**-36.62%***	+10.20%	1.58×*
3255	UARNet	+37.59%	-5.99%	**+134.0%***	1.59×*
25229	Kyiv Telecom	+31.18%	-4.93%	**+176.4%***	**2.20×***
35297	Dataline	+71.94%	**-34.43%***	+86.01%*	**2.81×***
21488	Emplot LTd.	**-86.73%**	+0.31%	**+554.6%***	**3.73×***
21497	Vodafone UKr	+15.82%	-19.67%*	**+202.8%***	0.98×
6876	TeNeT	-34.72%	+5.55%	-7.00%	0.60×*
50581	Ukr Telecom	+282.8%	-22.41%*	**+116.7%***	**4.92×***
39608	Lanet	**-44.41%**	-21.93%*	**+118.7%***	**2.80×***
13307	SKIF ISP Ltd.	-13.18%	+9.75%*	-46.89%	0.82×
Baseline Fluctuations		-36.85%	-25.06%	+109.71%	1.72×

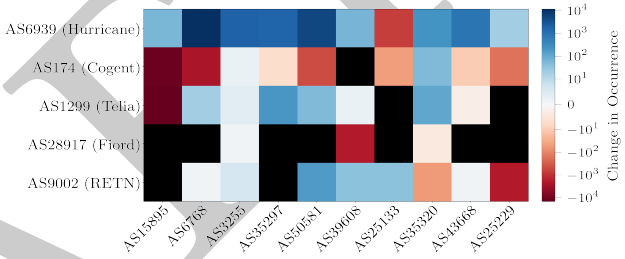


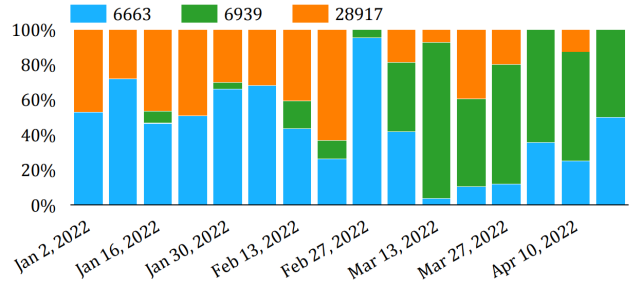
Figure 5: The heat map shows how connectivity from "Border ASes" outside of Ukraine (vertical axis) to Ukrainian ASes (horizontal axis) change after the invasion. Black squares indicate no routes are seen between the two ASes. The change in occurrence is the difference in the number of tests traversing the AS pair between the wartime period and prewar period (wartime - prewar).

traffic through Kyivstar experiences increased latency and decreased throughput, while traffic through SKIF ISP experiences no degradation above baseline; both ASes serve Kyiv and the surrounding area. Also notable is TeNeT, an Odessa ISP that did not see degradation above baseline levels. AS-level data suggests that severe damage is localized to few ASes while the rest continue to participate in routing at or near baseline levels. Furthermore, the top 10 ASes shown in Table 3 are only responsible for routing 25.6% of the 852,738 NDT tests considered. Combined with the fact that users IPs are not concentrated within one or few ASes [3], this supports findings from the preceding section that the routing infrastructure as a whole remains functional despite certain ASes going dark.

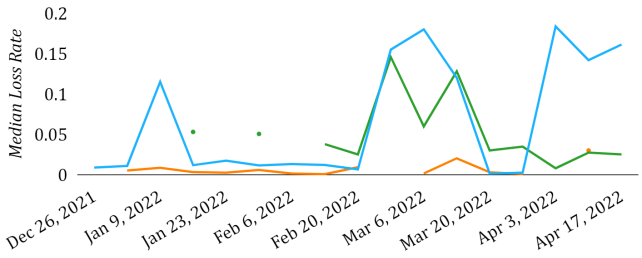
So far we have only considered ASes local to Ukraine, but because NDT servers are not located in Ukraine, we can see from the `traceroute` data how Ukraine receives international traffic. To investigate the connectivity, we look at the hops in the `traceroutes` where one endpoint is a non-Ukrainian "border AS" and the other is Ukrainian.

Figure 5 shows how connections between the most common "Border ASes" and Ukrainian ASes change as a result of the invasion. For many Ukrainian ASes (columns), we see an increase in the number tests utilizing Hurricane Electric and fewer utilizing Cogent

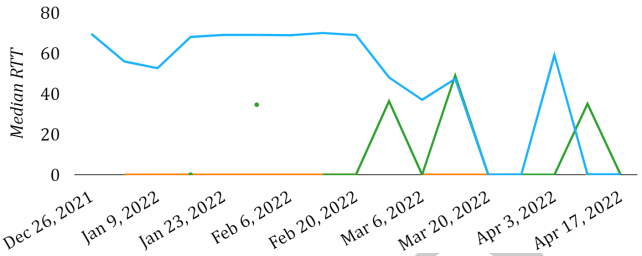
DRAFT



(a) Weekly percentage of connections through AS199995



(b) Weekly median loss rate of NDT tests



(c) Weekly median RTT of NDT tests

Figure 6: The portion of NDT tests routing through AS6663 to AS199995 decreases as the median loss rate and RTT of tests through this AS increases.

Networks. Though we did not find sources to corroborate this observation, a recent report from RIPE on the resilience of the Internet in Ukraine does also note that Hurricane Electric participates in routing for a high percentage of the population, making it "influential" [3].

We see a shift in routing preference to Hurricane Electric very clearly in Ukrainian AS 199995. We find that three main foreign "border" ASes route through AS 199995, with AS 6939 being Hurricane Electric. Shown in Figure 6, as AS 6663's loss rate increases, a much larger proportion of connections going through AS 199995 arrive from AS 6939, whose connections have far better performance. While many other Ukrainian ASes interact with Hurricane Electric, AS 199995 is the most commonly occurring AS in the data which interacts with multiple foreign ASes.

6 Related Work

Related work directly connected to the Russian invasion of Ukraine was dicussed in Section 2. In this section, we discuss other related work on characterizing Internet resilience in the face of destabilizing world events and natural disasters.

Major World Events: In the aftermath of the 9/11 attacks, Partridge et. al. led a workshop to analyze networking data in the time after the attacks to better understand the effect on telecommunications issues, with the goal of preventing communication disruptions should such events transpire again [14]. Following Arab Spring in 2011, Dainotti et al. characterized the impact of censorship on Internet connections in Egypt and Libya using BGP data, darknet traffic, and active probe measurements [16].

Natural Disasters: The effects of the recent COVID-19 pandemic on Internet trends has been well-studied under various lenses. Böttger et. al. demonstrate worldwide traffic surges and connection quality degradations correlated with events at the start of the pandemic from the vantage point of Facebook's edge network [7]. Feldmann et. al. observe lasting shifts of aggregated and application-specific traffic distributions from a set of four vantage points [19]. Lutu et. al. consider data from the perspective of a large mobile network operator in the UK and study decreases in human and network mobility patterns causing variations in traffic rates [35]. Candela et. al. conduct a case study of Internet metrics in the country of Italy from the RIPE dataset, observing increased latency and packet loss at the peak of the pandemic, and compare these changes to metrics in other European countries [9].

There is also a body of work outlining responses to other natural disasters, including the earthquake and subsequent tsunami in Japan in 2011 [10] and Hurricane Sandy on the US East Coast in 2013 [18]. Other studies focus on general weather related Internet impacts [39], power outages [5] and Internet outage analysis [6].

Measurement Lab: Data from Measurement Lab has been used in work to learn Internet path changes and metrics [46], studying latency distributions on the Internet [24], an evaluation of the Record Route option of the IPV4 protocol [22], and recently was editorialized to revisit on the decade since it was introduced to the research community [21]. The Internet Society has additionally published a dashboard on Ukrainian M-Lab data [41]. We leave analysis of other data sets as a potential avenue for future work.

7 Discussion and Conclusion

To the best of our knowledge, this work is the first study of user-perceived performance during the Ukraine war. We observe noticeable performance degradation for NDT users in regions under direct attack, and we find modest correlations between increased path diversity and decreased connection performance. However, the ability of the network to rapidly adapt and diversify paths provides evidence of infrastructure resilience. Numerous open questions remain about the Ukrainian Internet experience in wartime. Are there other sources of degradation which explain the drastic effects on network performance? What applications and services suffered the most, and which performed the best? We look forward to future work in this area in order to guide the networking community to design an Internet that meets the needs of the world's most vulnerable users.

DRAFT

References

[1] (2022-07-04). *How many Ukrainian refugees are there and where have they gone?* https://www.bbc.com/news/world-60555472

[2] Emile Aben. (2022-02-28). *The Ukrainian Internet.* https://labs.ripe.net/author/emileaben/the-ukrainian-internet/

[3] Emile Aben. (2022-03-10). *The Resilience of the Internet in Ukraine.* https://labs.ripe.net/author/emileaben/the-resilience-of-the-internet-in-ukraine/

[4] P. Baran. 1964. On Distributed Communications Networks. *IEEE Transactions on Communications Systems* 12, 1 (1964), 1–9. https://doi.org/10.1109/TCOM.1964.1088883

[5] Niloofar Bayat, Kunal Mahajan, Sam Denton, Vishal Misra, and Dan Rubenstein. 2021. Down for Failure: Active Power Status Monitoring. *Future Gener. Comput. Syst.* 125, C (dec 2021), 629–640. https://doi.org/10.1016/j.future.2021.06.055

[6] R. Bogutz, Y. Pradkin, and J. Heidemann. 2019. Identifying Important Internet Outages. In *2019 IEEE International Conference on Big Data (Big Data).* IEEE Computer Society, Los Alamitos, CA, USA, 3002–3007. https://doi.org/10.1109/BigData47090.2019.9006537

[7] Timm Böttger, Ghida Ibrahim, and Ben Vallis. 2020. How the Internet Reacted to Covid-19: A Perspective from Facebook's Edge Network. In *Proceedings of the ACM Internet Measurement Conference* (Virtual Event, USA) *(IMC '20).* Association for Computing Machinery, New York, NY, USA, 34–41. https://doi.org/10.1145/3419394.3423621

[8] Thomas Brewster. (2022-03-22). *Ukraine's Engineers Battle To Keep The Internet Running While Russian Bombs Fall Around Them.* https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/?sh=1d168a015a4c

[9] Massimo Candela, Valerio Luconi, and Alessio Vecchio. 2020. *Computer Networks* 182 (2020), 107495. https://doi.org/10.1016/j.comnet.2020.107495

[10] Kenjiro Cho, Cristel Pelsser, Randy Bush, and Youngjoon Won. 2011. The Japan Earthquake: The Impact on Traffic and Routing Observed by a Local ISP. In *Proceedings of the Special Workshop on Internet and Disasters* (Tokyo, Japan) *(SWID '11).* Association for Computing Machinery, New York, NY, USA, Article 2, 8 pages. https://doi.org/10.1145/2079360.2079362

[11] D. Clark. 1988. The Design Philosophy of the DARPA Internet Protocols. In *Symposium Proceedings on Communications Architectures and Protocols* (Stanford, California, USA) *(SIGCOMM '88).* Association for Computing Machinery, New York, NY, USA, 106–114. https://doi.org/10.1145/52324.52336

[12] Mason Clark, George Barros, Frederick W. Kagan, Kateryna Stepanenko, and Karolina Hird. (2022-04-20). *Ukraine Conflict Updates.* https://www.understandingwar.org/backgrounder/ukraine-conflict-updates

[13] Wikimedia Commons. 2022. *2022 Russian Invasion of Ukraine.* https://commons.wikimedia.org/wiki/File:2022_Russian_invasion_of_Ukraine.svg

[14] National Research Council. 2003. *The Internet Under Crisis Conditions: Learning from September 11.* The National Academies Press, Washington, DC. https://doi.org/10.17226/10569

[15] Jim Cowie. (2022-03-04). *This is consistent with what's currently visible at the Cogent looking glass; namely, no direct adjacencies to Vimpelcom, but the much more substantial connections to Rostelecom 12389, Vkontakte 47541, and Megafon 31133 remain.* https://mobile.twitter.com/jimcowie/status/1499838091191889925

[16] Alberto Dainotti, Claudio Squarcella, Emile Aben, Kimberly C. Claffy, Marco Chiesa, Michele Russo, and Antonio Pescapé. 2014. Analysis of Country-Wide Internet Outages Caused by Censorship. *IEEE/ACM Transactions on Networking* 22, 6 (2014), 1964–1977. https://doi.org/10.1109/TNET.2013.2291244

[17] Gerrit De Vynck, Rachel Lerman, and Cat Zakrzewski. (2022-03-29). *How Ukraine's Internet still works despite Russian bombs, cyberattacks.* https://www.washingtonpost.com/technology/2022/03/29/ukraine-internet-faq/

[18] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. 2013. ZMap: Fast Internet-Wide Scanning and Its Security Applications. In *Proceedings of the 22nd USENIX Conference on Security* (Washington, D.C.) *(SEC'13).* USENIX Association, USA, 605–620.

[19] Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, Oliver Hohlfeld, and Georgios Smaragdakis. 2020. The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic. In *Proceedings of the ACM Internet Measurement Conference* (Virtual Event, USA) *(IMC '20).* Association for Computing Machinery, New York, NY, USA, 1–18. https://doi.org/10.1145/3419394.3423658

[20] Mat Ford. (2022-03-16). *Ukrainian Internet Shrinks by Over 15%.* https://pulse.internetsociety.org/blog/ukrainian-internet-shrinks-by-over-15

[21] Phillipa Gill, Christophe Diot, Lai Yi Ohlsen, Matt Mathis, and Stephen Soltesz. 2022. M-Lab: User Initiated Internet Data for the Research Community. *SIGCOMM Comput. Commun. Rev.* 52, 1 (mar 2022), 34–37. https://doi.org/10.1145/3523230.3523236

[22] Brian J Goodchild, Yi-Ching Chiu, Rob Hansen, Haonan Lua, Matt Calder, Matthew Luckie, Wyatt Lloyd, David Choffnes, and Ethan Katz-Bassett. 2017. The Record Route Option is an Option!. In *Proceedings of the 2017 Internet Measurement Conference* (London, United Kingdom) *(IMC '17).* Association for Computing Machinery, New York, NY, USA, 311–317. https://doi.org/10.1145/3131365.3131392

[23] Google. [n.d.]. *Test your internet speed.* https://support.google.com/websearch/answer/6283840

[24] Toke Høiland-Jørgensen, Bengt Ahlgren, Per Hurtig, and Anna Brunstrom. 2016. Measuring Latency Variation in the Internet. In *Proceedings of the 12th International on Conference on Emerging Networking EXperiments and Technologies* (Irvine, California, USA) *(CoNEXT '16).* Association for Computing Machinery, New York, NY, USA, 473–480. https://doi.org/10.1145/2999572.2999603

[25] Max Hunder. (2022-03-07). *Mayor of Ukraine's Lviv appeals for help with flood of displaced people.* https://www.reuters.com/world/mayor-ukraines-lviv-appeals-help-with-flood-displaced-people-2022-03-07/

[26] Yuras Karmanau. (2022-04-18). *Zelenskyy: Russian offensive in eastern Ukraine has begun.* https://apnews.com/article/russia-ukraine-war-lviv-missile-strikes-536b8f0bb48ae21a6ee30991a5535ea3

[27] K Keys. 2008. *IP Alias Resolution Techniques: Technical Report.* Technical Report. Cooperative Association for Internet Data Analysis (CAIDA).

[28] Ivana Kottasová and Yulia Kesaieva. (2022-03-15). *Kharkiv was struck 65 times on Monday and 600 residence buildings have been destroyed so far, officials say.* https://www.cnn.com/europe/live-news/ukraine-russia-putin-news-03-15-22/h_3799075fd4af25327b19f6496cbb1bc0

[29] Brian Krebs. (2022-03-11). *Report: Recent 10x Increase in Cyberattacks on Ukraine.* https://krebsonsecurity.com/2022/03/report-recent-10x-increase-in-cyberattacks-on-ukraine/

[30] Measurement Lab. (2020-08-05). *Evolution of NDT.* https://www.measurementlab.net/blog/evolution-of-ndt/

[31] Measurement Lab. (2021-01-01 – 2022-04-16). The M-Lab NDT Data Set. https://measurementlab.net/tests/ndt. Bigquery table `ndt.unified_download`.

[32] Measurement Lab. (2021-01-01 – 2022-04-16). The M-Lab Traceroute Data Set. https://measurementlab.net/tests/traceroute. Bigquery table `ndt.scamper1`.

[33] Measurement Lab. [n.d.]. *What is Measurement Lab?* https://www.measurementlab.net/about

[34] Tim Lister and Olya Voitovych. (2022-03-01). *Russian-backed separatist leader expects his forces to surround Mariupol on Tuesday.* https://www.cnn.com/europe/live-news/ukraine-russia-putin-news-03-01-22/h_0e3d20b474aa007bb1e4acc0d0fba984

[35] Andra Lutu, Diego Perino, Marcelo Bagnulo, Enrique Frias-Martinez, and Javad Khangosstar. 2020. A Characterization of the COVID-19 Pandemic Impact on a Mobile Network Operator Traffic. In *Proceedings of the ACM Internet Measurement Conference* (Virtual Event, USA) *(IMC '20).* Association for Computing Machinery, New York, NY, USA, 19–33. https://doi.org/10.1145/3419394.3423655

[36] Doug Madory. (2022-03-10). *Large outages today in #Ukraine. Ukrtelecom (AS6849) down nationally at 9:35 UTC (11:35am local) for 40min. Triolan (AS13188) has been down nationally for over 12hrs due to reported cyber attack. Still almost entirely offline. Vizes from @gatech_ioda and @kentikinc:.* https://twitter.com/DougMadory/status/1501910709734678529

[37] Inc. MaxMind. [n.d.]. *GeoIP2 City Accuracy.* https://www.maxmind.com/en/geoip2-city-accuracy-comparison?country=UA&resolution=25&cellular=all

[38] Inc. MaxMind. [n.d.]. *GeoIP® Databases Services: Industry Leading IP Intelligence.* https://www.maxmind.com/en/geoip2-services-and-databases

[39] Ramakrishna Padmanabhan, Aaron Schulman, Dave Levin, and Neil Spring. 2019. Residential Links under the Weather. In *Proceedings of the ACM Special Interest Group on Data Communication* (Beijing, China) *(SIGCOMM '19).* Association for Computing Machinery, New York, NY, USA, 145–158. https://doi.org/10.1145/3341302.3342084

[40] Jonathon Penney. 2012. Communications Disruption Censorship under International Law: History Lessons. In *USENIX Workshop on Free and Open Communication on the Internet (FOCI).*

[41] Amreesh Phokeer. (2022-04-06). *Ukraine-Russia M-Lab Dashboard.* https://pulse.internetsociety.org/blog/ukraine-russia-mlab-dashboard

[42] JJ Rosen. (2022-03-06). *Ukraine's resilience also shows in its strong technology experts.* https://www.tennessean.com/story/money/tech/2022/03/06/ukraines-resilience-also-shows-its-strong-technology-experts/9345361002/

[43] David L. Stern. (2022-02-18). *Ukraine's Lviv becomes 'western capital' as some diplomats leave Kyiv.* https://www.washingtonpost.com/world/2022/02/18/ukraine-russia-lviv-war/

[44] Suhail. (2022-02-24). *1/ Cyber attack thread of the ongoing invasion:.* https://twitter.com/suhail/status/1496876355664822272?lang=en

[45] International Telecommunication Union. (2019). *Individuals using the Internet (population) - Ukraine.* https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=UA&most_recent_value_desc=true

[46] Sarah Wassermann, Pedro Casas, Thibaut Cuvelier, and Benoit Donnet. 2017. NETPerfTrace: Predicting Internet Path Dynamics and Performance with Machine Learning. In *Proceedings of the Workshop on Big Data Analytics and Machine Learning for Data Communication Networks* (Los Angeles, CA, USA) *(Big-DAMA '17).* Association for Computing Machinery, New York, NY, USA, 31–36. https://doi.org/10.1145/3098593.3098599

[47] Tetiana Zatonatska, Oleksandr Dluhopolskyi, Iryna Chyrak, and Nataliya Kotys. 2019. The internet and e-commerce diffusion in European countries (modeling

DRAFT

at the example of Austria, Poland and Ukraine). *Innovative Marketing* 15, 1 (2019), 66–75. https://doi.org/10.21511/im.15(1).2019.06

DRAFT

A Ethics Statement

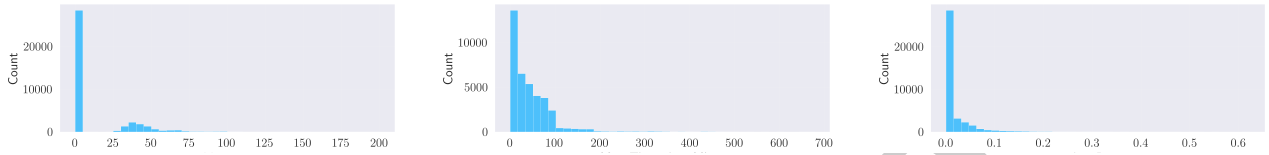
To the best of our knowledge, this research does not raise any ethical issues.

DRAFT

B Justification for Welch's t-test

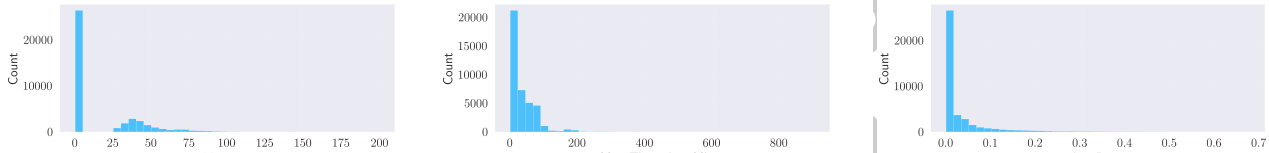
We used Welch's t-test to determine statistical significance. We chose this test specifically because it enables us to compare samples from populations that do not have equal variance. In our analysis, we found that the samples we compared had unequal variances, which could imply that the populations they were sampled from also had unequal variance.

Welch's t-test also expects that the data is sampled from normally distributed populations. Figures 7 and 8 show the sample distributions for each metric in the prewar and wartime periods, respectively. Minimum RTT appears to be normally distributed (aside for the spike near 0), but the other metrics are slightly skewed. While its impossible to know the exact population distribution, the lack of normality in the samples could be considered a limitation of the statistical tests.



(a) Minimum RTT (ms) **(b) Mean Download Speed (Mbps)** **(c) Connection Loss Rate**

Figure 7: Distributions for each key metric during the prewar period.



(a) Minimum RTT (ms) **(b) Mean Download Speed (Mbps)** **(c) Connection Loss Rate**

Figure 8: Distributions for each key metric during the wartime period.

DRAFT

C Supplementary Data on Internet Service Quality

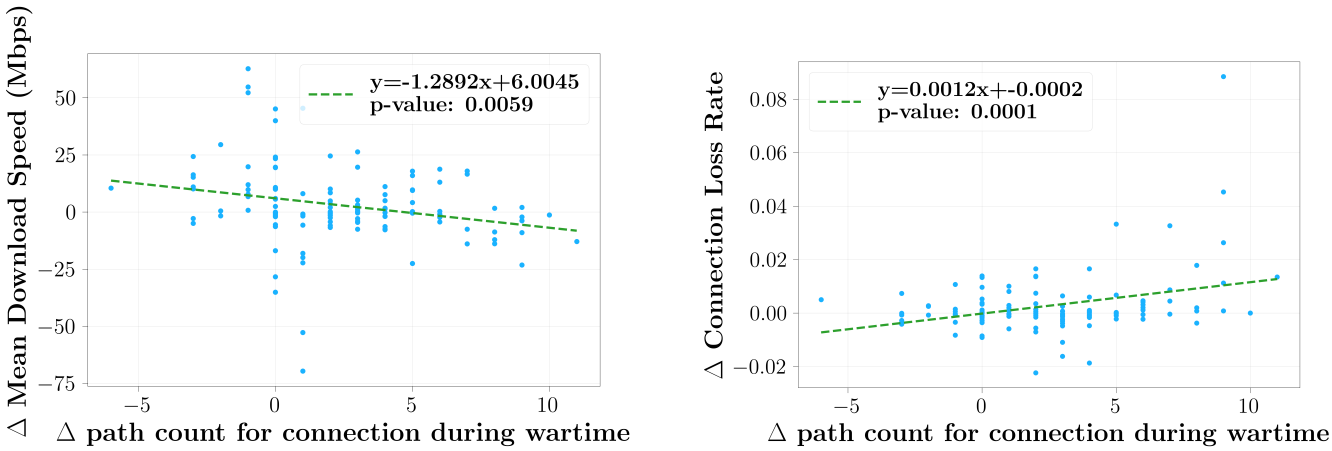
Table 4: Raw values for region/oblast-level metrics.

	Prewar				Wartime			
Region/Oblast	MeanTput (Mbps)	MinRTT (ms)	LossRate	Count	MeanTput (Mbps)	MinRTT (ms)	LossRate	Count
Kiev City	61.71	11.69	1.30%	11216	50.61	25.99	2.93%	10023
Dnipropetrovs'k	35.18	13.18	1.82%	3024	30.14	17.93	2.96%	3483
L'viv	34.70	6.53	1.62%	1881	37.16	13.44	3.27%	2964
Odessa	40.31	9.07	1.99%	2210	39.43	11.31	2.41%	1969
Kharkiv	42.72	21.42	2.22%	2102	42.51	26.93	3.41%	1692
Donets'k	26.87	22.22	2.09%	1749	20.78	16.50	4.02%	1318
Zaporizhzhya	24.71	4.16	2.00%	1046	19.87	14.94	12.09%	1552
Vinnytsya	34.56	6.73	1.39%	894	32.82	12.35	2.42%	1293
Mykolayiv	55.30	28.20	1.50%	1031	49.50	32.84	2.31%	1127
Transcarpathia	27.36	18.43	4.77%	721	19.53	20.96	5.58%	1040
Chernihiv	71.33	14.20	2.45%	1298	18.55	9.90	4.71%	366
Kiev	32.76	4.65	1.35%	887	34.92	17.40	5.38%	728
Kherson	24.59	5.08	2.07%	614	16.37	18.94	8.57%	986
Cherkasy	48.00	3.94	0.85%	570	46.33	12.37	2.68%	831
Rivne	34.81	3.30	2.14%	612	28.21	11.69	3.69%	766
Poltava	31.12	5.04	1.47%	537	38.56	17.60	3.77%	824
Ivano-Frankivs'k	22.16	6.58	2.19%	535	27.34	15.28	3.26%	758
Ternopil'	37.16	11.50	1.46%	531	43.95	8.78	2.46%	594
Kirovohrad	18.64	3.30	1.87%	437	22.19	11.22	2.28%	642
Luhans'k	13.87	10.30	2.92%	581	14.66	19.63	5.88%	470
Volyn	36.62	4.49	1.49%	414	26.84	13.80	2.67%	631
Zhytomyr	25.65	8.25	2.10%	459	28.38	21.82	5.31%	555
Chernivtsi	22.24	4.71	2.01%	462	38.00	12.16	2.22%	513
Khmel'nyts'kyy	21.67	11.15	2.06%	227	28.86	14.49	4.94%	688
Sumy	22.61	7.47	1.87%	329	20.18	20.83	8.52%	552
Crimea	43.41	65.76	2.80%	348	34.60	57.15	4.45%	338
Sevastopol'	21.52	47.53	3.48%	92	29.80	31.01	4.08%	199

DRAFT

D Supplementary Performance Analysis of Routing

As pictured in Figure 9, as the number of paths a connection uses increases, we see corresponding, statistically significant decreases in throughput and increases in loss rates. We measure the change in unique path counts for a connection, as defined in Section 5, as the difference between the number of unique paths observed when serving a connection during wartime and the number of unique paths observed when serving a connection before the war. In order to establish this correlation on a persistent set of connections, we only consider connections that had at least ten tests both prewar and during wartime, though the correlations still hold on a larger scale with less filtering.



(a) Mean Download Speed

(b) Connection Loss Rate

Figure 9: Performance changes in connection bandwidth and loss rate with respect to changes in the number of paths used per connection.

Table 5: Raw values for AS-level metrics.

ASN	Period	Mean TPut (Mbps) mean	median	std	MinRTT (ms) mean	median	std	LossRate mean	median	std	Count
15895	Prewar	37.836	36.175	30.064	22.514	0.070	79.346	0.0161	0.0053	0.0274	3367
	Wartime	23.980	9.262	33.132	24.809	0.074	185.841	0.0254	0.0029	0.0591	3921
3255	Prewar	61.664	35.516	63.927	5.257	0.035	20.839	0.0177	0.0028	0.0408	1934
	Wartime	57.971	32.944	67.471	12.300	0.038	29.250	0.0281	0.0042	0.0604	2661
25229	Prewar	52.699	42.534	43.359	7.259	0.039	17.372	0.0150	0.0034	0.0288	1549
	Wartime	50.099	32.920	54.275	20.062	0.045	35.240	0.0330	0.0074	0.0663	2032
35297	Prewar	31.969	13.243	72.602	13.151	0.047	28.112	0.0135	0.0026	0.0326	816
	Wartime	20.962	6.708	36.731	24.462	0.067	48.810	0.0379	0.0106	0.0638	1403
21488	Prewar	90.516	92.006	35.202	3.755	0.038	11.063	0.0019	0.0007	0.0057	1809
	Wartime	90.792	92.024	24.488	24.581	31.618	15.289	0.0072	0.0048	0.0117	240
21497	Prewar	18.720	14.321	20.635	6.584	0.064	22.321	0.0391	0.0032	0.0820	929
	Wartime	15.038	9.213	18.778	19.932	0.070	43.905	0.0383	0.0035	0.0886	1076
6876	Prewar	45.038	43.225	33.827	4.187	0.054	15.621	0.0121	0.0017	0.0351	1129
	Wartime	47.538	52.301	33.164	3.894	0.054	14.032	0.0073	0.0011	0.0153	737
50581	Prewar	31.827	15.366	43.035	4.670	0.040	13.145	0.0105	0.0030	0.0233	360
	Wartime	24.695	11.530	39.290	10.118	0.042	21.367	0.0518	0.0055	0.1033	1378
39608	Prewar	84.613	45.551	110.260	6.086	0.042	19.883	0.0075	0.0016	0.0198	1056
	Wartime	66.061	49.085	77.319	13.311	0.059	34.283	0.0209	0.0025	0.0568	587
13307	Prewar	115.258	153.041	67.662	0.591	0.032	6.514	0.0038	0.0005	0.0128	774
	Wartime	126.493	177.031	70.678	0.314	0.032	3.861	0.0031	0.0001	0.0157	672

DRAFT

Table 6: p-values for AS-level metrics.

ASN	Name	MeanTput	MinRTT	LossRate
15895	**Kyivstar**	2.454e-76	4.824e-1	9.508e-19
3255	**UARNet**	5.902e-2	2.452e-21	3.750e-12
25229	**Kyiv Telecom**	1.112e-1	9.592e-45	1.901e-27
35297	**Dataline**	5.720e-5	5.621e-12	1.261e-31
21488	**Emplot LTd.**	8.768e-1	7.354e-57	5.642e-11
21497	**Vodafone UKr**	3.433e-5	5.232e-18	8.193e-1
6876	**TeNeT**	1.144e-1	6.735e-1	5.407e-5
50581	**Ukrainian Telecom**	4.553e-3	2.126e-9	5.975e-40
39608	**Lanet**	7.122e-5	3.250e-6	4.102e-8
13307	**SKIF ISP Ltd.**	2.144e-3	3.185e-1	3.674e-1

DRAFT