Tracking Internet Disruptions in Ukraine: Insights from Three Years of Active Full Block Scans

Florian Holzbauer
Faculty of Computer Science
Doctoral School Computer Science
University of Vienna
Vienna, Austria
florian.holzbauer@univie.ac.at

Sebastian Strobl
SBA Research
Vienna, Austria
sstrobl@sba-research.org

Johanna Ullrich
University of Vienna
Vienna, Austria
johanna.ullrich@univie.ac.at

Abstract

Numerous disruptions to Internet access have been reported during the war in Ukraine, including large-scale outages, damage to network infrastructure, surveillance, and censorship measures. However, most observations rely on local reports or monitoring systems within Ukraine. In this paper, we investigate whether the conflict's impact on Internet connectivity can be observed externally, from a vantage point outside Ukraine. Focusing on the Kherson region, which has remained on the frontline for over three years, we conduct an active measurement campaign probing the Ukrainian address space at two-hour intervals since March 2, 2022, the 7th day of the invasion, resulting in a country-wide dataset that spans the full duration of the conflict. Extending existing outage detection approaches, we infer three signals to detect Internet disruptions and refine the mapping of ASes and address blocks to specific regions. This allows us to assign disruptions to oblasts with greater confidence. Our results demonstrate that Internet disruptions caused by the war can be measured remotely by any host connected to the Internet. Our analysis provides new insights into the resilience of small regional providers and identifies periods when Ukraine's Internet infrastructure was under significant strain.

CCS Concepts

• **Networks** → **Network measurement**; **Public Internet**.

Keywords

Outage Detection; ICMP; Full Block Scans; Ukraine; Kherson

ACM Reference Format:
Florian Holzbauer, Sebastian Strobl, and Johanna Ullrich. 2025. Tracking Internet Disruptions in Ukraine: Insights from Three Years of Active Full Block Scans. In *Proceedings of the 2025 ACM Internet Measurement Conference (IMC '25), October 28–31, 2025, Madison, WI, USA.* ACM, New York, NY, USA, 19 pages. https://doi.org/10.1145/3730567.3764449

1 Introduction

The Internet is a critical infrastructure for communication, both in everyday life and during crises. It enables people to stay in touch with family, friends, and colleagues while also serving as a primary medium for accessing information, such as news and governmental advisories. Since the war in 2022, Internet connectivity in Ukraine has been repeatedly disrupted and has undergone continuous efforts of restoration.

Several analyses have examined the impact of war on Internet connectivity in Ukraine. Many of these studies [19, 26, 30, 31] require connection initiation from within Ukraine. In contrast, active measurement campaigns that send probes to IP addresses enable data collection from outside the country. However, existing outage detection platforms, such as IODA [17], rely on Trinocular [36], which uses a limited set of representative IP addresses per /24 block.

In this work, we extend existing research on full-block [3, 4] scans by conducting our own active measurements of the Ukrainian address space. Thereby, we capture the full block state directly by probing the entire address space using ICMP, rather than inferring it from the sampled Trinocular data. This approach has several advantages: we collect the full block state every two hours, and probing every IP allows us to introduce an additional outage signal based on responsive IPs to also detect partial outages.

A central challenge, also encountered in related work, is the attribution of outages to specific regions. In §4, we address this by leveraging long-term trends in IP geolocation to improve confidence in block-level location assignments. This allows us to better enumerate Internet disruptions at the regional level, allowing us to distinguish between outages in frontline and non-frontline areas. Together, our methodology and dataset offer improved insights into Internet disruptions, particularly in countries with high address churn, such as Ukraine. In summary, we make the following contributions:

Unique Full Block Dataset (§2,§3). We collected responsiveness and round-trip-time data for the entire Ukrainian address space. While the advantage of probing all addresses over sampling for Internet outage detection has been demonstrated in small-scale case studies before, it is the first time that it is applied to a country at war over a period of three years, showcasing its relevance. Access to the dataset can be requested at `https://countrymonitor.github.io`; it is provided for research purposes only.

IP Address Churn (§4). We discover churn of IP addresses across the different regions in Ukraine. Particularly, IP addresses leave frontline regions at a faster pace than other regions. This motivates the improvement of selection strategies to identify IP addresses that are representative of individual ASes or regions.

Regional Evaluation (§4). We refine the assignment of ASes and address blocks from the national to the regional level, enabling

IMC '25, Madison, WI, USA
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1860-1/2025/10
https://doi.org/10.1145/3730567.3764449

more localized analysis of measurement data, as demonstrated for Kherson Oblast. Among 118 ASes with IPs in the region, 34 operate regional blocks, making their outages more representative. We validate this classification against IPInfo's geolocation confidence metric, finding that regional blocks generally exhibit higher geolocation precision.

Internet Disruptions (§5). Based on three outage signals inferred from our collected data, we derive periods where Internet access was disrupted in Ukraine and specifically Kherson Oblast. Our approach is able to detect Internet outages across a larger set of providers than previous work, particularly small providers. We find that during Winter 2022/23 and 2024/25, Internet disruptions were widespread across Ukraine. During the remaining time periods, outages are specific to frontline regions.

Verification of Results (§5). We verified our results on Internet outages with regard to multiple aspects. For large ASes, our results correlate with those of Trinocular. Beyond that, we were able to verify our list of regional ASes in Kherson Oblast with a regional administrator, and we were also able to relate their outages to reported events such as cable cuts, the destruction of a dam or the seizure of infrastructure. Finally, we show that outages in non-frontline regions strongly correlate with power outages.

2 Background and Related Work

In this section, we provide background on Ukraine and reported Internet disruptions caused by the full-scale invasion. Then, we compare previous Internet measurement studies on Ukraine during wartime.

2.1 Ukraine and Verified Internet Outages

Ukraine is a country in Eastern Europe and is divided into 24 oblasts, two cities with special status, and an autonomous region. We refer to all these entities as regions or oblasts, irrespective of the detailed administrative differences, and use them interchangeably. The country's capital, Kyiv, is a city with special status and surrounded by an oblast of the same name, which we consider to be a single region for the purpose of our work, resulting in a total of 26 regions in our analysis. On February 24th, 2022, neighboring Russia started a full-scale invasion of the country. The initial military advance on the capital failed in April 2022, and Kherson Oblast was partly liberated again in November 2022. Since then, the frontline is practically stable.

Frontline and Non-Frontline Regions. We consequently differentiate between frontline regions, i.e., oblasts marking the border between Ukrainian and Russian troops and experiencing continuous war actions since 2022, and non-frontline regions. Frontline regions are the oblasts of Chernihiv, Donetsk, Kharkiv, Kherson, Luhansk, Sumy, and Zaporizhzhia. All other oblasts are considered to be non-frontline regions. The latter also includes Kyiv and Mykolaiv, which experienced active combat only during the initial advance at the full-scale invasion's beginning.

Kherson Oblast as an Example Region. We investigate Internet outages at the regional level, and Kherson Oblast, connecting Crimea with the Ukrainian mainland, serves as the example region for our work. We chose it as it was fully occupied by Russia in 2022 and partially liberated again in the same year. Since then, the Dnipro River marks the frontline – the right bank is controlled by Ukraine, the left bank by Russia. Its administrative center, Kherson city – a port city with 280,000 inhabitants before the war – resides on the liberated right bank. As of early 2025, only 70,000 are estimated to live in the city [16, 44].

Internet Disruptions affecting Kherson Oblast. According to reports, the region's Internet connection was disrupted and reconstructed multiple times as a consequence of kinetic warfare. The following timeline provides an overview of the events. In this work, we are able to verify these reported events based on our detected outages (indicated with ☑), see Section 5 for our detailed results. For some of the events, we also provide additional insights beyond the reports (indicated with ⚙).

- ⚙ **March–May 2022**: Russian troops searched ISP offices in Kherson and seized infrastructure [8]. In collaboration with a local ISP (Status), we verified an Internet outage caused by the seizure.
- ☑ **April 30, 2022**: An oblast-wide outage occurred due to damage to the last functioning backbone cable [20, 33]. Our dataset allowed us to pinpoint 24 active ASes that were affected by this incident.
- ☑ **May–November 2022**: Internet from Kherson was routed over Russian upstream, leading to higher RTTs [27, 41]. We confirm these RTT increases for regional ASes, and additionally observe several disconnections of non-regional ASes for addresses regional to Kherson Oblast.
- ☑ **November 11, 2022**: Ukrainian forces liberated Kherson city and its surroundings [23]. Based on our contact with the regional ISP Status, we track this event at the granularity of address blocks, revealing a ten-day outage followed by gradual service restoration for their address blocks in Kherson.
- ⚙ **June 6, 2023**: The Kakhovka dam was destroyed [24]. While only the outage of a single AS is documented [35], we show that the resulting flooding had a broader impact, with a timely disruption visible for Viner Telecom, Digicom, and TLC-K.
- ⚙ **June/July 2024 and Winter 2024/25**: Airstrikes on energy infrastructure caused electricity outages [11]. We find a strong correlation between Internet outages and power outages in non-frontline regions, suggesting that they primarily arise from a lack of electricity in these regions.

2.2 Existing Measurements Ukraine

Several Internet measurement studies attempted to gain insight into Ukraine and the consequences of warfare on the country.

Passive Measurements. Cloudflare monitored HTTP request volumes in its data centers and detected rolling power outages after targeted strikes against Ukrainian power infrastructure [2, 6]. Other studies analyzed (a) BGP data from route collectors to identify periods of unreachability of Ukrainian networks [26] as well as to quantify Crimea's dependency on certain, predominantly state-operated Russian ASes [14], (b) results from Measurement Lab's Network Diagnostic Tool (NDT), initiated by Ukrainian users, to detect the war's impact on Internet performance [19], and (c) web

Dataset	Singla et al. [42]	Klick et al. [22]	IODA/Trinocular [17]	This Work	Cloudflare [2]
Measurement Type	active	active	active	active	passive
IP/Block-based	IP	IP	/24	/24	IP
Protocols	DNP3, Modbus	60+	ICMP	ICMP	HTTP, DNS
Vantage Points	1	>1	approx. 20	1	330 cities [5]
Measurement Interval	24 hours	4 hours	10 min	2 hours	<1 min
Probes per /24 Block	256	up to 256	up to 15	256	-
Block Eligibility	-	-	$E(b) \geq 15$ & $A \geq 0.1$	$E(b) \geq 3$	-
Geolocation Confidence	Low	High	Low	High	Moderate
Target Set	UA delegated	400K static IPs	IPv4-wide	UA delegated	UA clients
Avg. Responsive IPs	435K	-	-	1.5M	-
War Period Coverage	6 Months in 2022	Until March 2023	Since 2022	Since 2022	Since 2022

$E(b)$ refers to the number of ever-active addresses in a /24 address block b, $A(E(b))$ to the long-term probability that the ever-active addresses reply.

Table 1: Comparison of methods used for Internet outage detection, with a focus on Ukraine. We compare four active measurement approaches, including this work, and one passive method (Cloudflare).

analytics data such as those provided by Google and Cloudflare, again to assess Internet performance as well as to trace the flow of refugees to Ukraine's neighboring countries [30, 31]. Passive measurements analyze already available Internet traffic instead of generating additional data transmission, but require a privileged position, e.g., in a content delivery network or at a BGP collector, to observe sufficient amounts of traffic in the first place.

Active Measurements. As an alternative, active measurements might be run from vantage points in the affected regions. Ukrainian nodes that are part of the RIPE Atlas platform are an option, e.g., to assess round-trip times between Ukraine and Russia [26]. These measurements, however, require the setup of vantage points in the region of interest and notably limit scalability. RIPE Atlas operates about 200 nodes in Ukraine [31], covering a limited number of geographic locations. In contrast, it is more flexible and scalable to send requests from a vantage point, whether inside or outside of Ukraine, to the Ukrainian address space. IODA [7, 17, 36], Singla et al. [42], and our work follow this principle, see Table 1 for a comparison of active approaches with Cloudfare's passive one.

Detecting Internet Disruptions in Ukraine. Table 1 compares existing approaches for measuring Internet disruptions in Ukraine. Singla et al. [42] probed the entire Ukrainian address space using industrial protocols (Modbus, DNP3), but only once every 24 hours and for six months in 2022. Klick et al. [22] focused on a set of 400k static IPs probed at an interval of four hours. By targeting static IP addresses, this approach reduced noise from dynamic address changes and increased confidence in assigning outages to regions. Similarly, we improve geolocation precision. Instead of probing only static, we evaluate long-term geolocation trends to assign blocks to regions with high confidence (§4).

The IODA platform applies the Trinocular method, probing up to 15 IPs per /24 block. By trading comprehensive probing for fewer addresses, it achieves the highest probing frequency among active approaches, with measurements every ten minutes [17, 36]. While block-based probing increases outage confidence over single-IP approaches [40], its reliance on few IPs can yield unstable results. Full-block scanning (FBS) addresses this by aggregating responses across rounds, reducing the eligibility threshold to three ever-active IPs ($E(b) \geq 3$), though it has only been evaluated in case studies and is not actively used by IODA [3, 4].

Cloudflare instead monitors traffic volumes passively [2], benefiting from wide vantage coverage and high temporal resolution, but relying on proprietary data. Our dataset complements these methods by actively probing 10.5M Ukrainian IPs, with about 1.5M responding per round, every two hours (§3). This is the first long-term study to apply FBS in practice, extending coverage and stability beyond other active approaches. Unlike passive measurements, this data can be collected by any host connected to the Internet.

3 Methodology

Only seven days after the beginning of the full-scale invasion of Ukraine, we began probing the entire Ukrainian IPv4 address space. We tried to minimize the impact on Ukrainian networks and state ethical considerations in Appendix A. By combining this active measurement data with external sources, we generate three distinct outage signals. We first describe our measurement setup and signal generation (§ 3.1). Since IP responsiveness alone is insufficient to reliably infer outages and assign them to regions, we then discuss the external datasets integrated into our analysis (§ 3.2).

3.1 Setup and Signals

Data Collection. We probe all Ukrainian IPv4 addresses at a two-hour interval using ZMap [13] from our vantage point located in a European data center, approximately 1000km from Ukraine's capital Kyiv. The ICMP-based measurements started on March 2nd 2022, at 10 p.m., i.e., the 7th day of the full-scale invasion, and have been running since. For the work at hand, we analyze data from the beginning of our measurements to February 24th, 2025, the invasion's third anniversary.

Internet Availability Signals. We combine our collected data with external datasets to generate three Internet availability signals, aggregated at the AS or regional level. The first two signals align with those of IODA [17], though the second signal *FBS* is generated from our results by comprehensively measuring the address space

Level	BGP ★	FBS 🟩	IPS ▲
AS	< 95%	< 80% (if IPS < 95%)	< 80%
Regional	< 95%	< 95% (if IPS < 95%)	< 90%

Table 2: Static Internet disruption detection thresholds relative to a seven-day moving average.

instead of sampling. We extend these signals by a third signal that is only feasible due to comprehensively probing the Ukrainian IP address space.

1. *BGP* ★ provides the number of routed /24 address blocks per AS. As we also develop a method to assign ASes to a region, we are also able to generate this signal per region.
2. *FBS* 🟩 provides the number of active /24 address blocks, again either grouped per AS or region, and is equivalent to the number of address blocks meeting the eligibility criteria of at least three ever-active addresses per month.
3. *IPS* ▲ provides the number of responsive IP addresses per AS or region and enables us to also capture partial outages, i.e., decreases in IP activity while block reachability remains stable. We limit this signal to months where the average number of responsive IP addresses exceeds 10.

Signal Properties. *FBS* 🟩 and *IPS* ▲ are based on the regional share of IPs in blocks classified as regional. To detect outages, we compare current values with the moving average of the previous week. Based on the level of aggregation, i.e., AS or region, we defined different thresholds for outages, see Table 2. The rationale is that more granular aggregations (e.g., ASes in comparison to regions) involve fewer entities (IPs, blocks). Consequently, they are assigned more relaxed thresholds to avoid false positives. Due to the sliding window, the moving average adapts to the new baseline after an outage, causing the outage criteria to no longer be met. To still capture such long-lasting outages, we add a flag to the *BGP* ★ signal – if no routed /24 is visible for the ASN or region, the outage period is considered ongoing, even after the moving average stabilizes. Finally, we also employ ISP availability sensing as proposed by Baltra et al. [3] to avoid false positives in the *FBS* 🟩 signal. This way, we filter out false positives caused by dynamic IP reallocations, rather than mistaking them for outages.

Limitation - Single Vantage Point. All measurements were conducted from a single vantage point located outside Ukraine. This design reflects both the urgency of setting up the monitoring infrastructure during the early stages of the war and the storage constraints of processing a more comprehensive *FBS* 🟩 signal than previous Trinocular signals. Previous campaigns did not reveal systematic limitations associated with this vantage point. However, as with any single-source measurement system, data is unavailable when the vantage point is offline. These outages occurred on the following dates and are indicated in the figures (March 6th-7th, 2022, March 14th-28th, 2022, October 12th-19th, 2022, March 5th - April 2nd, 2024, July 13th, 2024, August 7th-19th, 2024, and September 16th, 2024).

Limitation - Bi-Hourly Probing Interval. To minimize measurement load on the Ukrainian Internet, we adopted a probing interval of two hours. This choice reduces potential network strain but limits our temporal resolution. Specifically, outages that begin and resolve between two consecutive probing windows may go undetected. Each probing session spans approximately 20 minutes, so the maximum undetected outage duration is bounded by the remaining 100 minutes between sessions. Other approaches, like Trinocular, measure at shorter intervals, e.g., 10 minutes, promising higher resolution. We quantify the limitation in Section 5.4 by enumerating outages between our probing intervals. However, they only probe a fraction of the addresses in each round and do not report outages for small regional providers that our exhaustive measurements are able to detect.

3.2 External Datasets

For our measurement study, we extend our probing data with external datasets. As an input for our ZMAP measurements, we relied on **RIPE Delegations** [38], which contain allocated and assigned IP address ranges, among others, for European countries. In the delegations files from December 14th, 2021 the most recent at the start of the invasion, we found address ranges with a total of addresses with Ukraine's country code UA. We also rely on **RouteViews BGP dumps** [45], which, like our measurement data, are available in two-hour intervals. These are used to create the Internet availability signal *BGP*★ based on the number of routed /24 blocks. Additionally, this data enables the aggregation of IP addresses per AS. For geolocation, we use the commercial service **IPInfo** [18] to assign IP addresses to geographic locations both on the regional and country level. We obtained access to the full database on the first day of each month. While an IP might be located in different geolocations over a given month, we focus on long-term trends by detecting providers that remain in the same region across multiple months. This approach reduces geolocation noise in the detection of outages.

To validate our findings, we use **IODA** [17], which detects and reports Internet outages in the IPv4 Internet. Unlike other platforms such as Netblocks [34] or Kentik [21], IODA provides access to raw signal and outage data [25]. We rely on their API to compare and validate outages detected for Ukraine. Finally, we compare outages with **Energy Map** data provided by the national power company Ukrenergo [32], which includes information on power grid outages affecting more than 50% of Ukraine's Oblasts between January 1st, 2023 and January 20th, 2025.

Limitation - Leased Prefixes and Churn. Our measurements relied on a static snapshot of RIPE delegations from December 14th, 2021, which we used unaltered throughout the three-year period. However, RIPE notes that delegation data may not always reflect actual usage, particularly due to leased prefixes—i.e., address blocks registered in one country but used in another. At the start of our measurements, 350K addresses (3.3%) delegated to Ukraine were geolocated outside the country. To assess the reverse case, we relied on IP geolocation to reveal 773K addresses (7.4%) used in Ukraine but delegated to other countries. Assessing churn in delegated prefixes, 348 Ukrainian prefixes (12%) changed their registered country code, with one-third reallocated to Russia and the rest to various

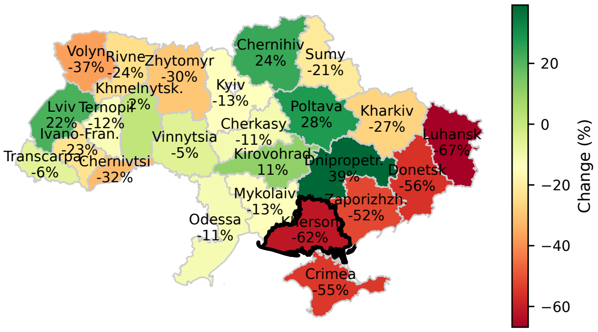

Figure 1: Relative change in IPv4 address counts per oblast (February 1, 2022 – February 1, 2025). IP addresses shift away from frontline regions to other parts of Ukraine or to foreign countries.

European countries and the U.S. We also observed a net decline in prefix allocations to Ukraine: only 198 new prefixes (7%) were assigned over three years (see Figure 18 in Appendix B). Based on these dynamics, we estimate RIPE delegations to consistently cover at least 93% of Ukraine's active address space during our measurements, making them a reliable baseline for IP-level monitoring.

4 Regional Classification

We refine the assignment of ASes and /24 address blocks from the national to the regional level using Ukraine's administrative divisions (oblasts). However, direct application of geolocation services reveals significant address churn, with IPs shifting between regions or countries (see §4.1). To avoid misclassifying regional outages, we introduce a stricter definition of regionality based on sustained address presence over time (§4.2). We then verify this classification (§4.3) and assess its impact on our dataset by analyzing address responsiveness (§4.4).

4.1 Regional Address Churn

We geolocated all probed IP addresses using IPinfo and compared their regional assignment from before the war (February 1, 2022) to three years later (February 1, 2025). Our results reveal substantial address churn, with many IPs moving between regions or leaving Ukraine entirely. This motivates a stricter definition of regionality for both ASes and address blocks.

Churn across Ukraine. Figure 1 shows the relative change in IPv4 address counts per oblast. Nineteen of 26 regions saw declines, with the sharpest losses in frontline areas: Luhansk (-67%), Kherson (-62%), Donetsk (-56%), Zaporizhzhia (-52%), Kharkiv (-27%), and Sumy (-21%). Only Chernihiv recorded a net increase (+24%). Churn also occurred in non-frontline oblasts such as Volyn (-37%), Zhytomyr (-30%), and Rivne (-24%). Appendix C, Figure 20 shows increasing IPv6 adoption, which may help extend outage detection in sparse regions once suitable methods exist. Geolocation confidence, measured by IPInfo's radius metric (5 to 5,000 km, with increasing step widths), also declined—its median for Ukrainian IPs rose from 100 km in 2022 to 500 km thereafter. Of 3.73M IPs that changed location, 2.24M moved between Ukrainian regions, primarily driven by national ISPs like Ukrtelecom (697K), Kyivstar (341K), Vodafone (243K), and Vega (67K), reflecting dynamic address assignment. Another 1.5M addresses were geolocated abroad, mostly to the US (926K), Russia (110K), and Germany (60K). Notably, AS16509 (Amazon) now announces 519K of these, about one-third of the externally reassigned IPs.

Churn in the Kherson Region. We also found this trend in Kherson. Of the 141K IP addresses initially geolocated to Kherson, only 36K (26%) remained there after three years. 63K (45%) moved to another Ukrainian oblast, and 41K (29%) were geolocated abroad. This includes 33K IPs previously held by Volia (AS25229), now announced by Amazon.

Key Takeaways

(1) Between 2022 and 2025, 3.7M IP addresses changed location, indicating substantial churn.
(2) Of these, 2.2M moved within Ukraine (mainly due to national ISPs), while 1.5M were reassigned abroad, primarily to Amazon, the US, or Russia.
(3) Frontline regions lost more IPs than non-frontline regions; in Kherson, only 26% of IPs remained.

4.2 Definition of Regionality

Address churn motivates a stricter definition of regionality in favor of reducing the distortion of our results. Therefore, we aggregate IP addresses to AS or /24 address blocks, respectively, and decide on their regionality depending on their share of addresses in a region over time. Based on our definition, we define them as regional, i.e., primarily operating in a single region, or non-regional, i.e., operating in multiple regions.

Formal Definition. Let E_{total} denote the set of entities, either ASes or /24 address blocks, with at least one geolocated IP address in the investigated region over the observed period T. For each entity $e \in E_{\text{total}}$ at time t, we define the share $s_t(e) = \frac{n_t(e)}{N(e)}$, where $n_t(e)$ is the number of geolocated IPs in the region and $N(e)$ is its maximum possible number of addresses (for ASes their addresses in Ukraine; for /24 blocks $N(e) = 256$). We classify entity e as regional for a region if its share meets the threshold M in at least T_{perc} of routed months T_{routed}. As an example, Figure 2 shows a /24 block classified as regional.

$$E_{\text{reg}} = \left\{ e \in E_{\text{total}} \;\middle|\; \sum_{t=1}^{T_{\text{routed}}} \mathbf{1}\big(s_t(e) \geq M\big) \;\geq\; \big\lfloor T_{\text{perc}} \cdot T_{\text{routed}} \big\rfloor \right\}$$

To assess the sensitivity of our classification for different parameter choices, we vary M and T_{perc} from 0.1 to 1 in steps of 0.1, see Figures 22 and 23 in Appendix D on the resulting numbers of regional ASes and blocks. For the remainder of this work, we selected thresholds of $M = 0.7$ and $T_{\text{perc}} = 0.7$.

We illustrate the impact of our parameter choices by two ISPs in Kherson. With a strict threshold of $M = 0.9$ and $T_{\text{perc}} = 0.9$, *ISP Status* would be classified as non-regional as one of its four /24 subblocks is located in Kyiv. By contrast, relaxed thresholds

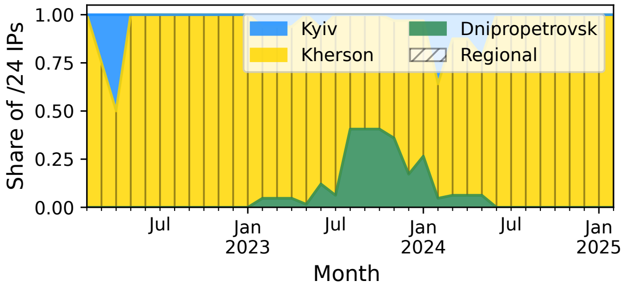

Figure 2: The exemplary /24 block 176.8.28 belonging to Kyivstar meets the regional threshold of M=0.7 in more than 70% of routed months in Kherson.

	Ukraine			Kherson		
Category	**ASes**	$\overline{\textbf{IPS}}$	$\overline{\textbf{/24s}}$	**ASes**	$\overline{\textbf{IPS}}$	$\overline{\textbf{/24s}}$
Total	2024	8.99M	35.2K	118	73.8K	512
⚑ Reg.	1428	4.17M	16.7K	13	8.3K	33
🌍 Non-Reg.	484	4.80M	19.4K	40	64.9K	465
🕘 Temporal	112	17.9K	313	65	596	15
Target Set	1773	7.15M	28.5K	34	41.7K	168

Table 3: Classification of regional, non-regional, and temporal ASes, including average monthly counts of ASes, IP addresses, and /24 blocks in Ukraine and Kherson (2022–2025). The final row highlights the target set: Regional and non-regional ASes with regional /24 blocks that are suitable for outage detection.

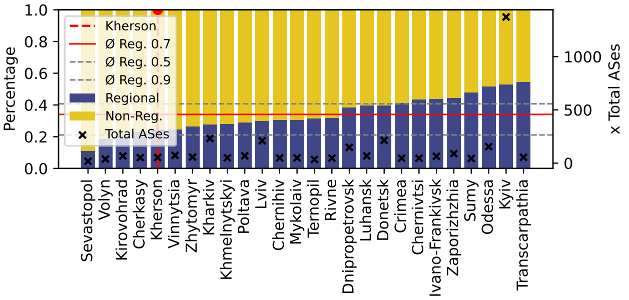

Figure 3: Regional classification helps to identify important ASes per region. Regional ASes account on average for 34% of the ASes with at least one address geolocated to a region. From 118 ASes in Kherson, we identified 40 non-regional and 13 regional ones, while 65 only show temporary presence in the region.

of 0.5 would classify providers operating across multiple oblasts, such as *Digicom*, as regional. Our chosen tradeoff of 0.7 balances these extremes: it permits a share of IPs to be operated outside the main oblast, while still capturing the regional nature of the provider. The same rationale applies at the block level. However, in contrast to ASes, /24s pointing to multiple locations and oblasts are less prominent. From the total of 35.2K /24s we find a mean of 78% pointing to a single location during a given time. This number increasees to 86% on the oblast level. Figure 21 in Appendix D shows that for multi-local /24s there is usually a dominant share that points to one region. We aim to detect temporal assignments as an additional filter on non-regional ASes, as temporal geolocation assignments (a few IPs, only one month) are likely caused by noise in geolocation and are not valuable measurement targets. We define non-regional ASes as temporal if they fail to reach a certain number of IPs in the target region (< 256, equaling one /24) or the regional share exceeds 10% for at least one month.

Separate Classification of ASes and Blocks. ASes, both regional and non-regional, might encompass regional and non-regional address blocks. The blocks' classification has two advantages. First, regional ASes might predominantly serve one region, but often also other (neighboring) regions to a certain extent. Exclusion of the non-regional blocks improves the result's significance for the region of interest. For example, AS25482 (Status) is regional in Kherson. Three of its four/24 blocks meet the regionality criteria; the fourth is regional in Kyiv and would distort our results for Kherson. Second, non-regional ASes like national ISPs might contain regional blocks, providing insight into a region. From AS15895 (Kyivstar) 299 /24s located once in the Kherson region, of which only 52 are regional.

Mitigated Noise to Outage Attribution. There is inherent noise in geolocation due to the mobility of IP addresses and the dynamic usage of address blocks. Introducing regional classification to outage attribution, we mitigate these common scenarios. While this approach still relies on IP geolocation, it does so only on the regional level and not on the more granular city level. By identifying and excluding dynamic blocks, regional dependency is limited to long-term stable blocks. Summarizing, we mitigate the following scenarios: *(II) IP drift:* If one or more IP addresses of a /24 temporarily geolocate to a different region, our outage detection approach only includes the IPs belonging to the regional part of the block. *(II) Block drift:* If a /24 block geolocates to another subdivision for a limited period, we do not attribute outages to this block. *(III) Regional churn:* If multiple IP addresses and blocks leave a region and are somewhere else, the block is entirely classified as non-regional and excluded from outage detection. If it still passes the threshold, it is evaluated only during the months in which it is considered to be regional. Finally, our approach cannot prevent *systematic misattribution*, i.e., IPInfo assigning the block to an incorrect region for ≥ 70% of months across the 3-year window.

Key Takeaways

(1) We classify ASes and /24 blocks as *regional* or *non-regional* depending on long-term trends in geolocation.
(2) Regional classification mitigates noise from IP and block shifts, reducing misattribution in outage detection.
(3) Separating AS and block classification improves precision: regional ASes may still contain some non-regional blocks, and non-regional ASes may include regional blocks.

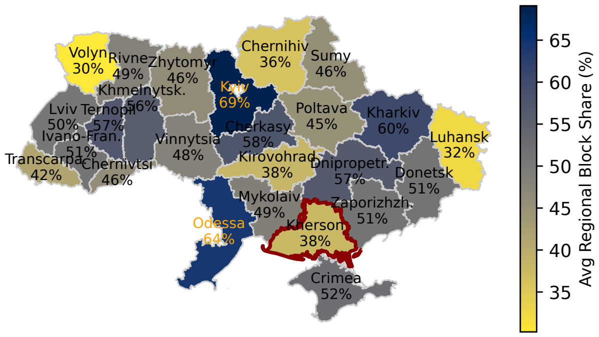

Figure 4: Share of regional /24 address blocks. On average, 50% of the blocks with at least one address geolocated to the region are classified as regional.

4.3 Evaluation

According to our definition, we classified ASes and /24 address blocks into regional and non-regional.

Regional Classification Ukraine. Table 3 shows that 1428 ASes (serving 16.7K /24 blocks) are regional for at least one of the 26 oblasts, while 484 are non-regional and 112 are temporal. Comparing IPInfos' confidence metric reveals a notable geolocation gap: IPs from non-regional /24s show a stable median radius of 500km across years, whereas regional /24s show higher precision, 50km in 2022, increasing to 200km by 2025. This reflects more accurate geolocation of regional networks, often tied to fixed sites like data centers or government offices, unlike mobile or carrier IPs [1]. Prior work supports the high prevalence of regional networks, noting Ukraine's unusually fragmented Internet infrastructure [12]. Figure 3 shows the number of regional ASes per oblast: 46% of ASes with at least one geolocated address are eventually classified as regional. However, some ASes are regional in one oblast and non-regional in others, leading to lower regional shares than the totals in Table 3. Figure 4 displays the share of regional blocks. This share ranges from 69% in Kyiv to 30% in Volyn. In total, we classify 28.5K /24 blocks, covering 7.15M IPs and 1773 ASes, as regional (Table 3), making them valuable for detecting regional outages. Temporal ASes account for 112 (5.5%) nationally, but this rises sharply in Kherson, where 118 ASes have at least one IP, and 65 (55%) appear only temporarily.

Regional Classification: Kherson. We identified 34 ASes with regional blocks in Kherson, as summarized in Table 3. Figure 5 presents these ASes ordered by their regional share of IP addresses, with higher shares indicating stronger association with Kherson. The figure shows a clear visual distinction between regional and non-regional ASes: regional providers appear at the top, while non-regional ones are concentrated at the bottom. It also highlights ASes that were active during only part of the measurement period. These are accurately captured by our method and appear with white gaps, indicating that the AS was no longer BGP-routed at those times. In total, seven ASes show discontinued service: 15458, 25256, 56359, 34720, 47598, 42469, and 44737.

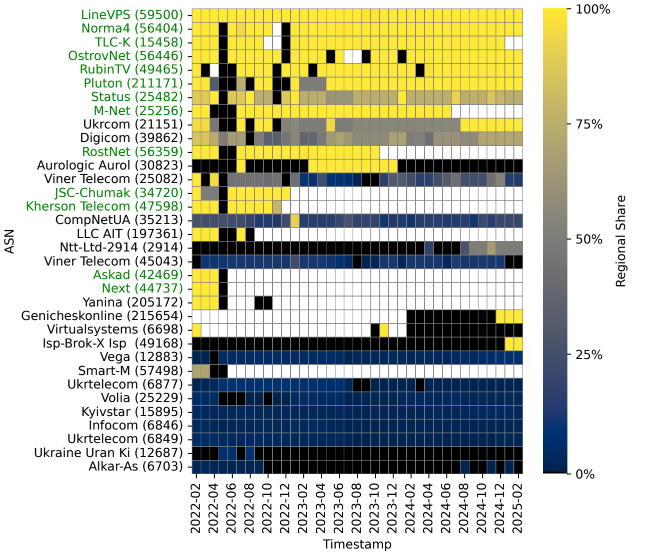

Figure 5: ASes with regional /24 address blocks in Kherson. Periods without BGP visibility are indicated in white.

Verification in Kherson. We contacted a local ISP and one of their administrators named the active regional providers in Kherson city and its surroundings, i.e., the liberated area on the right bank. This way, we verified that the ASes classified by our approach are indeed regional for Kherson oblast. We missed two providers in Kherson city, namely AS42782 (Stream Kherson), and AS39667 (Online Net). Their addresses are leased from AlfaTelecom, thus attributed to the Czech Republic in the RIPE delegations files, and eventually not considered by our input data set, see limitations.

Key Takeaways

(1) In Ukraine, we identify 1,428 regional ASes and 28.5K regional /24 blocks (7.15M IPs).
(2) Regional blocks show higher geolocation precision (median radius 50 km in 2022, 200 km in 2025) than non-regional ones (stable at 500 km).
(3) In Kherson, classification distinguishes 13 regional and 40 non-regional ASes, validated with a local ISP.

4.4 Regional Responsiveness

Outage detection on the regional level requires limitation to regional IP addresses as defined in the previous subsections, but also reduces the number of responses from our dataset, collected in the Internet measurements, for analysis. Consequently, we examine the responsiveness of regional blocks in Ukraine.

Responsiveness of Regional IPs. Probing 10.5M Ukrainian IP addresses, we received on average 1.47M replies in 2022. By 2025, this number dropped to 1.21 million replies, a reduction by −18%. Regional IPs accounted for 1.31M in 2022 (89% of all responses) and 1M in 2025 (83% of all responses), i.e., regional addresses return more responses than non-regional ones. Figure 6 provides absolute and relative numbers of responsive IPs within regional blocks per region.

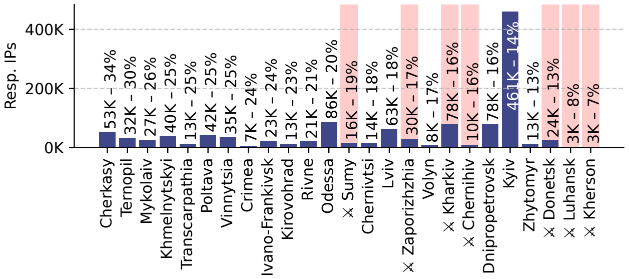

Figure 6: Share of responsive IP addresses per oblast. Labels indicate the average number and percentage of responsive IPs among all regional IPs in each oblast. Frontline regions are marked in red.

Frontline oblasts show lower responsiveness with the lowest share in Kherson oblast – from 41.7K IP addresses in regional blocks, 4.5K (10.7%) were responsive in 2022 and 1.4K (3.4%) in 2025, impacting the eligibility of blocks for outage detection.

Filtering Measurable Blocks. We build on the established method of full block scans [4] for outage analysis that requires at least three ever-active IPs per block and month ($E(b) \geq 3$) as eligibility criteria. From the 21.4K responsive /24 address blocks in our measurement data set, 20.4K, on average, meet this criterion. Figure 7 shows the distribution of measurable blocks across the different regions and highlights changes observed between 2022 and 2025. In frontline regions, we observe a strong correlation with recorded IP churn. Although the overall number of responsive IPs has decreased and most blocks are now concentrated in the capital, Kyiv, measurable blocks remain present in every oblast as of 2025. In Kherson, 1,400 responsive IPs are observed across 89 regional /24 blocks. These blocks form the basis for our outage detection in the region.

Comparing Block Eligibility to Trinocular. Table 4 compares the number of eligible blocks for full block scans, as done in our work, with Trinocular [36] for all regions of Ukraine. Trinocular poses stricter block eligibility criteria ($E(b) \geq 15 \wedge A \geq 0.1$). Yet, with 18.1K eligible blocks, the number of eligible blocks remains comparable. However, this number needs contextualization, considering Trinocular's known limitations: 4K blocks exhibit indeterminate belief ($A < 0.3$) [4], i.e., are more likely not to lead to a definitive belief whether the block is up or down. Additionally, Richter et al. [37] decided to exclude sparse blocks with five or more outages in three months further as they have shown fluctuating results. Consequently, many blocks might have to be filtered despite their initial eligibility (see §5.4 for a comparison).

Key Takeaways

(1) Despite an overall decline in replies (−18% from 2022 to 2025), regional IPs consistently respond more often than non-regional ones; frontline oblasts show the lowest responsiveness, with Kherson at the bottom.
(2) In 2025, all oblasts still show responsive eligible blocks.
(3) Compared to Trinocular, FBS preserves a higher number of eligible blocks and avoids indeterminate belief.

Category	Regional		Non-Regional	
All Regional Blocks	28,458	100.0%	10,650	100.0%
Responsive	21,542	76.0%	5,993	56.0%
-> Full Block Scans [4]	20,603	96.0%	5,628	94.0%
-> Trinocular [36]	18,138	84.0%	4,314	72.0%
Thereof Indetermined [36]	4,376	24.0%	2,549	59.0%

Table 4: Eligible blocks comparing regional to the filtered non-regional for outage detection.

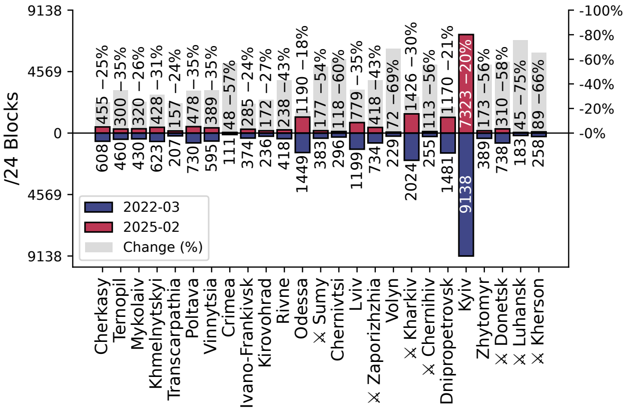

Figure 7: Comparison of responsive /24 address blocks (2022-03 vs. 2025-02).

5 Internet Disruptions

For a set of 1,773 ASes with regional address blocks (see Table 3) we analyze Internet outages across Ukraine, gradually increasing the granularity of our analysis. We start with a national view, finding that outages in non-frontline areas are largely driven by electricity outages (§ 5.1). We then focus on three key events in Kherson–the Mykolaiv cable damage, traffic rerouting during Russian occupation, and the Kakhovka dam destruction–highlighting their distinct impacts on distinct ASes in the region (§ 5.2). Through direct communication with Status AS, a local ISP, we confirmed visibility in provider-level outages (§ 5.3). Finally, we compare our findings with IODA data, showing broader outage coverage, especially for smaller ASes (§ 5.4).

5.1 Disruptions in Ukraine

Figure 8 presents the Internet outages per Ukrainian oblasts separated by the three signals – BGP reachability (*BGP* ★), active /24 blocks (*FBS* 🟩), and responsive IPs (*IPS* ▲) – each detecting different types of outages. For two periods, we observe a decline in responsive IPs affecting practically the entire Ukraine, while the number of active /24 blocks remains stable. This pattern persists even when applying thresholds as high as 99% for block activity, suggesting that blocks remained active despite lower numbers of responsive IPs. The figure further shows that most outages are not detectable through BGP alone. Instead, the majority are revealed by the FBS and IP responsiveness signals. In contrast, the IODA-based Figure 25 (replicated in Appendix G) portrays a different picture,

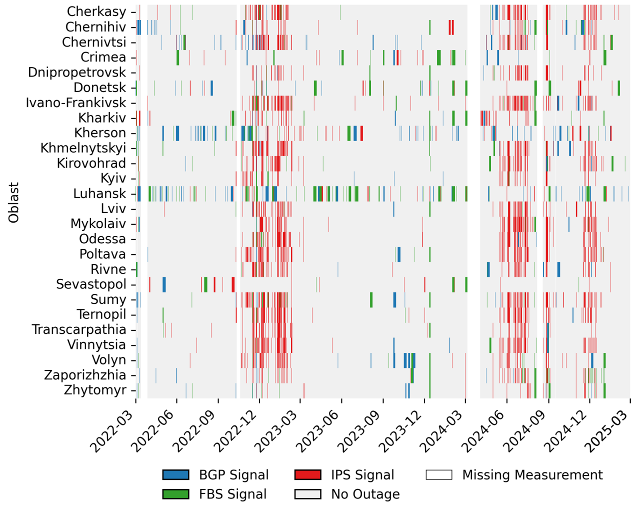

Figure 8: Internet disruptions detected by region. The three outage signals on routed /24 address blocks *BGP* ★, active blocks *FBS* ■, and responsive IPs *IPS* ▲ detect different outages.

dominated by long-term losses in BGP visibility across oblasts. We attribute this difference to the absence of regional classification in IODA's data model. Since IODA maps both regional and non-regional ASes to oblasts, BGP outages affecting large, non-regional providers can manifest as simultaneous outages across multiple regions.

Frontline vs. Non-Frontline Regions. In Figure 8, oblasts at the frontline, e.g., Kherson or Luhansk, experience recurring outages throughout the entire three-year measurement period. Non-frontline regions are primarily affected by outages during the winter months of 2022/23, and again in 2024/25. Figure 9 presents the average number of Internet outages per month separately for frontline and non-frontline regions. The figure also compares our results with those from IODA. For IODA, the non-frontline regions resemble the pattern from the frontline regions, suggesting that their ability to attribute outages to individual regions might be affected by IP churn. Beyond, IODA reports more hours of downtime. In some months, they account for 450 hours that would be equivalent to 63% downtime. IODA's higher outage hours appear to stem from long-term BGP visibility losses, which inflate the total hours of reported downtime.

Disruptions in Non-Frontline Regions. The outages detected in the winter months of 2022/23 and again in 2024/25 appear to affect all oblasts, see again Figure 8. A closer look, however, reveals that Crimea and Sevastopol, which are also on the Crimean peninsula, did not experience these outages. Both are occupied by Russia since 2014, and unlike the other Ukrainian regions connected to the Russian power grid [43].

1 ***June, July, and Winter 2024.*** In Figure 10, we consequently compare the Internet disruptions, as detected by our data, with the periods of electricity outages reported by Ukrenergo, the Ukrainian power grid operator [32]. This data is only available from 2023 onward and shows a clear increase in 2024 with 1951 hours without electricity. In the figure, we also indicate 13 dates of confirmed large-scale attacks on Ukraine's energy infrastructure as reported by Dixigroup [11]. Comparing the number of Internet and power outages, we detected on average 686 hours with Internet disruptions; the latter were typically shorter, possibly due to backup power solutions in place and power disruptions not affecting all oblasts equally. When looking at the worst case scenario, the maximum outage hours per day in which any of the oblast is affected, we detect up to 2,822 hours, including days where no power outages were reported by Ukrenergo. For instance, Kyivstar can maintain mobile services for up to four hours without electricity, and its core infrastructure even longer [10].

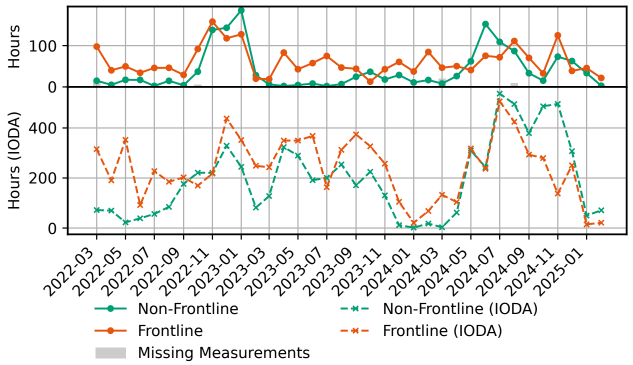

Figure 9: Monthly aggregated hours affected by Internet outages, comparing our measurements (top) with estimates based on Trinocular data from IODA (bottom).

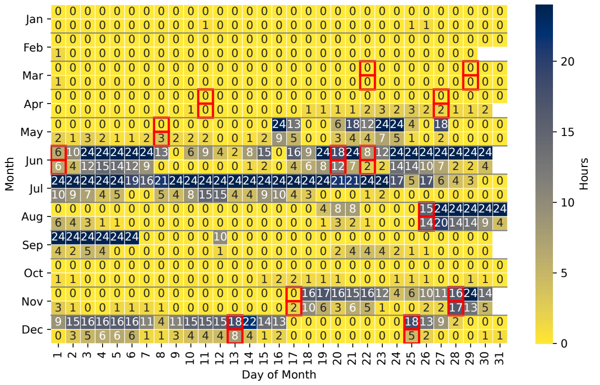

Figure 10: 1 Average hours of power and Internet outages per day for non-frontline regions (2024). Power outages as reported by Ukrainian power grid operator Ukrenergo [32] (top row) and Internet disruptions detected in this work (bottom row) correspond with each other. Days marked in red correspond to attacks on the power grid documented by [11].

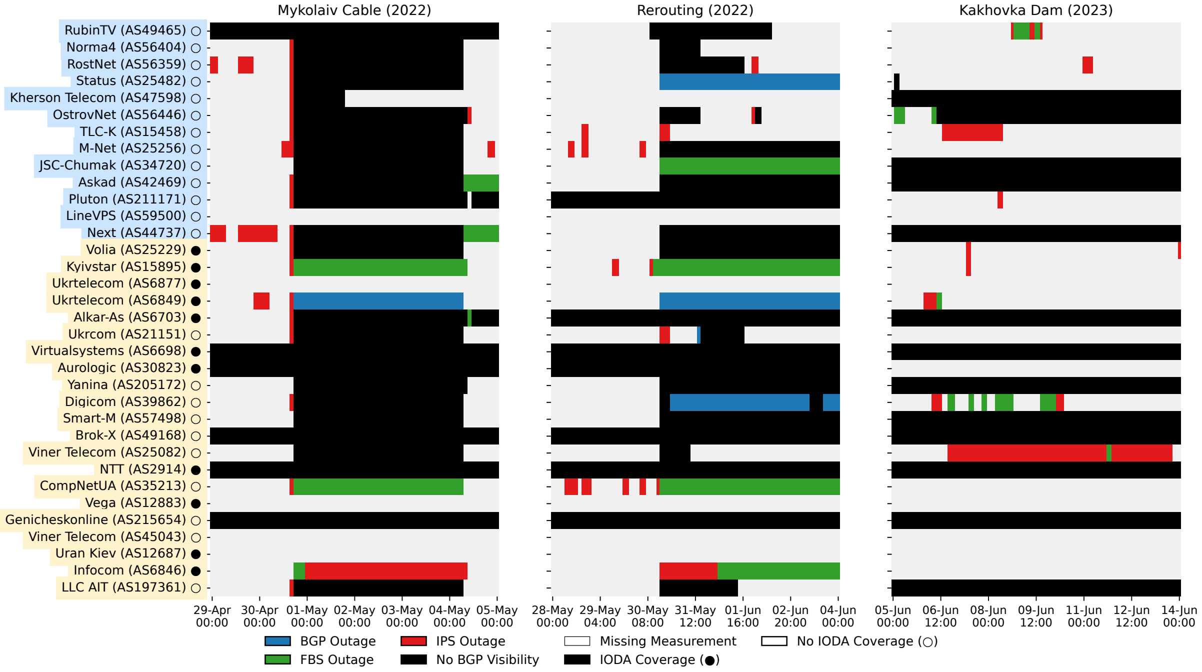

Figure 11: Internet disruptions recorded by any of the three signals for ASes in Kherson for three events to validate regional outages.

With a Pearson coefficient of $r = 0.725$, there is indeed a strong positive correlation between the hours of Internet and power outages in non-frontline regions. In comparison, frontline oblasts yield lower correlations of $r = 0.298$. This indicates that in frontline regions, Internet outages are less directly tied to power outages and are rather caused by other factors such as damage to the network infrastructure. Replicating this analysis with IODA data, see Figure 26 (Appendix G), shows weak correlation, both for non-frontline ($r = 0.328$) and frontline ($r = 0.394$) regions. Moreover, the similar correlation values observed in the IODA dataset for both frontline and non-frontline regions might again be a consequence of IODA being unable to precisely distinguish between the two classes.

5.2 Disruptions in Kherson

In this subsection, we now shift focus to the AS level, analyzing ASes in the region of Kherson; one of the seven frontline regions. We show that our data covers three major Internet disruptions, namely the damage to the Mykolaiv cable, traffic rerouting in Russian-occupied regions, and the destruction of the Kakhovka dam. AS-level analysis introduces additional challenges. Specifically, the *IPS* ▲ signal might be unreliable for ASes with only a few responsive IPs. Consequently, we only consider this signal for months in which the average of responsive IPs exceeds 10. This excluded Digicom (2 months), Infocom (2), Ukrtelecom (2) and Genicheskonline (1).

Timeline of Observed Disruptions. Figure 11 shows how our data covers the three events, distinguishing regional ASes in blue from non-regional ones in yellow. Six (Mykolaiv cable), seven (traffic rerouting), and twelve (Kakhovka dam) ASes were already invisible before the events – indicated by black bars in the figure – we only attribute a disruption if BGP visibility was lost after the event. A complete version of the figure, covering the entire three years of our measurements, as well as a table with information on the number of analyzed regional /24 address blocks and headquarter per AS is provided in Appendix D (see Figure 28, Table 5). Valid outage signals were recorded for 30 out of 34 ASes, indicating high responsiveness, even among ASes with only a single /24 block. Notably, IODA only reports outages for non-regional ASes, emphasizing its limited coverage in the Kherson region.

$\boxed{2}$ ***April 30, 2022.*** Kherson experienced a three-day oblast-wide Internet outage due to damage to the last backbone cable connecting the city [20, 33]. Our outage signal aligns clearly with the timing of the incident. Initially, it caused a drop in responsive IPs and eventually resulted in a loss of BGP visibility for 24 ASes. Most ASes recovered after three days, with the exception of Pluton and Alkar remaining offline afterwards.

$\boxed{3}$ ***May – November, 2022.*** As a consequence of Russian occupation, Internet traffic was rerouted through Russian upstream providers and *mir-telekom* was introduced as a mobile network operator [9, 28]. Cloudflare reported rerouting for 15 ASes by identifying Russian ASes on the BGP paths of networks in Kherson. Kentik [27] confirmed this by increased round-trip times (RTTs) for affected ASes. Based on our measurement data, figure 11 shows that 21 ASes experienced outages during this period. While regional ASes

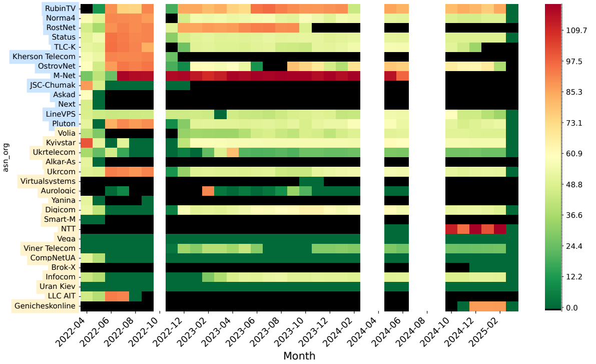

Figure 12: 3 Average monthly Round-Trip-Time (RTT) of ASes in Kherson.

were only temporarily affected and regained BGP visibility later, that was less prevalent for non-regional ASes, see the figure's complete version in the Appendix. Results from our RTT measurements, see Figure 12, confirm increased delays for the regional providers RubinTV, Norma4, Rostnet, Status, TLC-K, Kherson Telecom, OstrovNet, M-Net. For three ASes, namely RubinTV, RostNet, and M-NET, these elevated RTTs persisted even after the Ukrainian liberation of Kherson city end of 2022. The reason might be that their headquarters are, according to their websites, in Kakhovka, Oleshky, and Henichesk, respectively. All cities are in the still Russian-occupied part of Kherson Oblast on Dnipro's left bank. Beyond regional address blocks, several non-regional ASes were also disconnected, see Figure 28. This includes Askad, Next, Volia, Yanina, and Smart-M. Our dataset further confirms increased RTTs for Ukrcom, and LLC AIT.

4 ***June 6, 2023.*** The destruction of the Kakhovka Dam and successive flooding led to significant regional disruption [24]. While Netblocks reported only a single flood-related outage affecting Volia on June 14 [35], we detected additional outages. OstrovNet, headquartered in Kherson city's port district on Korabel Island, appeared to be severely affected by flooding. According to our data, it took three months to restore connectivity, with services resuming in September 2023. Interestingly, the *IPS* ▲ signal remained largely unaffected for providers that retained BGP connectivity. This suggests that most responsive IPs were located outside the flooded areas. We observed disruptions in the *FBS* 🟩 or *IPS* ▲ signal for Viner Telecom, TLC-K, and Digicom not only operating in Kherson city.

5.3 Disruptions at the Status ISP

Finally, we focus on AS25482 Status, a local ISP in Kherson, mainly operating in Kherson city. We were in contact with one of the operators and were able to verify provider-level events in our measurement data.

5 ***March - May 2022.*** In the first months of the occupation, Russian troops seized local ISPs. For Status, there is video footage of soldiers entering the provider's server rooms. Figure 13 displays the video's timestamp alongside our outage signals. At that time of this event, the *IPS* ▲ signal decreased, while *BGP* ★ and *FBS* 🟩 remained stable. This demonstrates the capability of our measurement approach to detect localized, provider-specific outages and emphasizes the sensitivity of the *IPS* ▲ signal to such events. This highlights another important use of the dataset: in a conflict where misinformation is widespread, the data can help verify the authenticity of reported incidents and related footage.

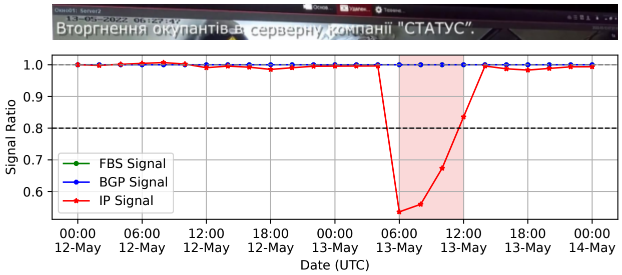

Figure 13: 5 Outage signals for Status (AS25482) on May 12th to May 14th with an incident recorded on May 13th, 06:28. Our dataset verifies that the action in the footage led to a disruption for the service provider.

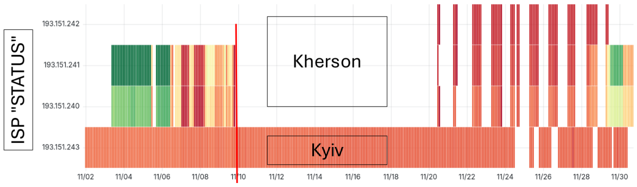

Figure 14: 6 *IPS* ▲ signal for each of the four /24 blocks of Status. The ISP went offline during the Russian retreat from Kherson city and came back online 10 days later using an emergency power supply.

6 ***November 11, 2022.*** Ukrainian forces recaptured Kherson city, eventually restoring control over local infrastructure [23]. Before, Russian troops destroyed infrastructure to disguise their retreat. We confirm outages, including Status ISP. Figure 14 shows the operator's four blocks, three of which are regional to Kherson and another one to Kyiv. According to our results, two blocks in Kherson stopped responding on November 11, while the block in Kyiv remained responsive. Ten days later, the Kherson blocks became responsive again, but only with clear diurnal cycles, potentially reflecting only limited availability of electricity during daylight hours.

In conclusion, our evaluation confirms the validity of our outage signals at multiple levels, from regional and AS-level incidents to outages impacting individual providers and subblocks.

Key Insights from Our Dataset

(1) Longitudinal view. Ukraine's Internet disruptions peaked in winter 2022/23 and throughout 2024 (*IPS* ▲ outages).
(2) In 2024, a total of 1,951 hours of power outages were reported. Our dataset shows non-frontline regions experienced on average 686 hours of Internet disruptions, and a worst-case maximum of 2,822 hours in which at least one oblast was affected. Outage days show a strong correlation with power cuts (r = 0.725).
(3) AS-level insights in Kherson: (I) Apr 2022 Mykolaiv cable cut (24 ASes offline), (II) May–Nov 2022 Russian enforcement (21 ASes, RTT spikes for 8 ISPs), (III) Jun 2023 Kakhovka flooding (OstrovNet offline 3 months).
(4) Insights into small regional ISPs. Our dataset verifies video footage from Status ISP recorded on May 13, 2022. The office search caused interference resulting in a visible *IPS* ▲ outage.

5.4 IODA AS-level Signal Comparison

As with the regional analysis, we compare our detected outages for 1,773 ASes with regional /24 blocks in Ukraine against those reported by IODA, using data retrieved via the IODA API [25]. We include all /24 blocks per AS, as our focus is on AS-wide outages rather than region-specific ones, making them more comparable to IODA. Otherwise, IODA can report outages for non-regional blocks that we do not measure.

Extended AS Coverage. We first evaluate for how many ASes in Ukraine, outages are reported. For comparability, we exclude outages from the *IPS* ▲ signal (absent in IODA) as well as IODA's Merit network telescope signal, which accounts for only 2% of its outages and is not present in our dataset. Figure 15 shows a CDF of the reported outages ordered by increasing AS size (in /24 blocks). Our approach reports 77.6K outages in 1,674 ASes. IODA reports 31.9K outages for 333 ASes and none for the other 1,440. Feedback from IODA confirms that it only reports outages for ASes with 20 or more /24s, affecting many smaller regional ASes in Ukraine.

Probing Interval. We evaluate the effect of the bi-hourly probing interval on our results by quantifying IODA outages (any signal type) that occur during the 100 minutes between our measurements. Out of a total of 31.9K outages, on average 70.5% fall within one of our probing intervals. Examining the signals separately, 23.7% of *BGP* ★ outages and 29.5% of *TRIN* 🟩 outages occur in the 100-minute gap between measurement cycles. This limitation could be mitigated by reducing the probing interval in future *FBS* 🟩 measurements. For instance, hourly scans would miss only 9.5% of outages, though at the cost of doubling storage requirements and necessitating real-time BGP table tracking, as historic RouteViews data is available only in bi-hourly intervals. A 30-minute probing interval with a 10-minute gap would further reduce missed outages to 0.1%. Alternatively, *FBS* 🟩 scans could explore lowering the scan rate, thereby distributing probes across a longer period.

Comparison of Common Outages. To align our comparison with IODA, we narrow the set to 182 ASes that reach high coverage in our measurements (target share > 0.9).

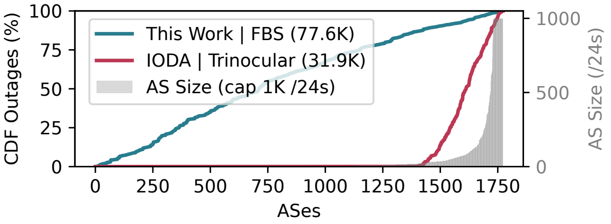

Figure 15: Comparison of AS outage coverage with IODA. CDF of outages with ASes ranked by their their size.

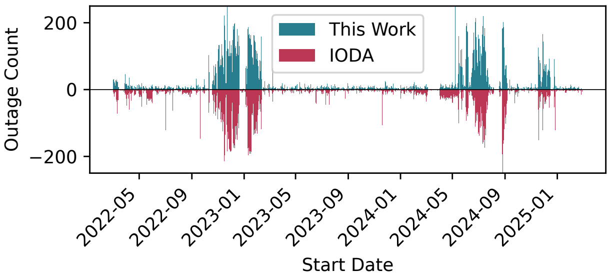

Figure 16: Number of outages starting per day reported by this work and IODA for a set of 182 ASes covered by both datasets.

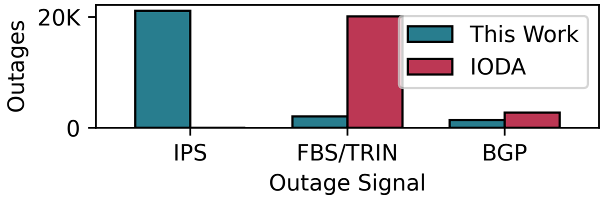

Figure 17: Signals and their share on total outages for the set of common ASes.

For comparability, we subtract our missing measurement periods from IODA outage periods and vice versa. We also incorporate the third signal of responsive IP addresses (*IPS* ▲, see Section 3.1).

Figure 16 shows strong agreement with Trinocular-based IODA data (r = 0.85), while Figure 17 details the contributions of individual signals. IODA primarily detects outages via active /24 blocks (*TRIN* 🟩), whereas our full-block scans rely on responsive IPs (*IPS* ▲). This suggests that many *TRIN* 🟩 events correspond to partial, not full, outages. In our data, *FBS* 🟩 contributes only 2,063 outages compared to 20,113 outages from *TRIN* 🟩 in IODA, since we require full block unresponsiveness, while Trinocular flags a block if only a few probed IPs fail. Our additional signal *IPS* ▲ detects 21,120 outages, capturing sudden loss of responsiveness among previously reachable IPs and indicating that IODA often classifies partial failures as block-wide outages.

Undetected Outages. We now examine cases where the set of ever-active IPs per month changes, and the *IPS* ▲ signal captures an outage while *TRIN* 🟩 does not. Therefore, we compare the outages reported by both signals and quantify the number of days that an outage was detected in one dataset but not the other. In favor of IODA, we observe 6,943 cases in which *TRIN* 🟩 reported an outage and *IPS* ▲ did not, primarily due to short-lived outages lasting less than two hours. In contrast, we identified 12,088 instances in which *IPS* ▲ reported an outage and IODA did not detect a corresponding event. In summary, our approach sacrifices some temporal granularity and therefore provides richer detail and broader coverage of Ukrainian ASes.

Key Takeaways

(1) *FBS* 🟩 provides a stable signal that is particularly useful in countries with many small regional providers and helps increase AS coverage (1,674 vs. 333, IODA).
(2) While we probe more frequently than other IP-based approaches [22, 42], the bi-hourly schedule misses ~30% of short-lived outages; future *FBS* 🟩 scans with 30–60 min intervals could further reduce this gap.
(3) Results correlate strongly with IODA ($r = 0.85$), but signals differ: *TRIN* 🟩 often shows partial outages, while *FBS* 🟩 capture more significant and *IPS* ▲ still allows to detect partial ones.

6 Discussion

Internet Disruption Characteristics. With an address churn of up to 67%, detecting Internet outages on the regional level for Ukrainian oblasts is challenging. Consequently, we develop a novel method that assigns IP blocks only to regions that remain continuously associated with them. By the example of Kherson oblast, regional blocks account for only 38% of all blocks, and only 7% of their IP addresses respond to our measurements, the lowest among all regions. Despite this low responsiveness, we observed outage signals, even for providers with a handful of address blocks, and were able to verify them against reported events.

Advantages Through Regional Classification. A central challenge, also encountered in related work, is the attribution of outages to specific regions. In §4, we address this by leveraging long-term trends in IP geolocation to improve confidence in block-level location assignments. We see a clear advantage in §5.1, where we find a strong correlation (Pearson $r = 0.725$) between Internet outages and recorded power outages in non-frontline regions, significantly higher than the correlation observed in IODA data ($r = 0.328$), indicating that our outage data more accurately represents these regions. Together, our methodology and dataset offer improved insights into Internet disruptions, particularly in countries with high address churn, such as Ukraine.

Insights from Kherson. Internet outages in non-frontline regions appear to be predominantly caused by power outages, whereas the frontline oblast of Kherson is additionally affected by damage to communication lines and network infrastructure, including cable cuts, equipment seizure, and traffic rerouting. In view of the circumstances, the Internet in Kherson was surprisingly resilient. Our personal exchange with a local operator revealed three key aspects, namely (I) the local Kherson Internet Exchange (KS-IX) to share (while originally not intended to) upstream connectivity among operators, (II) the deployment of redundant servers, links, and emergency power systems, and (III) the use of passive optical networks (PON) reducing dependency on electricity.

Advances in Outage Detection. We extended outage detection by a novel signal on responsive IP addresses (*IPS* ▲), which is only feasible when comprehensively probing the address space, to detect partial outages. This way, we are able to extend coverage from 330, as covered by IODA, to 1,674 ASes in Ukraine. This particularly includes outages at smaller ASes, such as our example Status ISP in Kherson, that would remain undetected otherwise, and is particularly relevant for countries as Ukraine with a highly fragmented Internet provider structure. Only a few of the investigated ASes exhibit clear day-night cycles, suggesting that outages of end users might be underrepresented. A promising direction for future work is the integration of IPv6-based signals, especially as we identified growth in its deployment in Ukraine, see Figure 20. Identifying home routers by NTP [39] or ICMPv6 error messages [15] would offer improved visibility on residential networks as they are not hidden behind NAT. This study relies on fixed probing intervals or rates for FBS, future work could further explore the impact of different intervals or explore dynamic thresholds for outage detection.

7 Conclusion

In this work, we demonstrated that Internet outages are reliably detected by active measurements from a single vantage point. Sending ICMP requests to all Ukrainian IP addresses at a two-hour interval, we gained detailed insight into Internet disruptions in the presence of kinetic warfare, and only a single opt-out request was received while measuring a country at war. IP churn motivated a more sophisticated approach to assigning probed addresses to regions in Ukraine. Focusing on regional ASes, we derive three distinct outage signals: BGP visibility, the number of responsive full blocks, and responsive IP counts. This multi-signal approach enabled us to validate disruptions against known events, uncover previously undocumented outages, and correlate connectivity loss with infrastructure damage and power failures. By combining active measurements with regional attribution, we provide a practical dataset that reveals Internet disruptions in Ukraine, which we found not to be fully captured by existing methods.

Acknowledgements

We thank Alexander Kovalenko from ISP Status for sharing valuable insights into ISPs in Kherson throughout the three-year war period. We are also grateful to Zachary Bischof and the IODA team for providing the platform and sharing insights on outage detection. Finally, we thank the anonymous reviewers for their constructive feedback on this paper. This research is supported in part by the Austrian Science Fund (FWF SFB project SPyCoDe 10.55776/F85), the Austrian Research Promotion Agency (FFG TestCat 911248) and SBA-K1 NGC, a COMET Center within the COMET – Competence Centers for Excellent Technologies Programme, funded by BMIMI, BMWET, and the federal state of Vienna.

References

[1] Abdullah. 2023. The radius field in the IP to Geolocation extended database explained. https://community.ipinfo.io/t/the-radius-field-in-the-ip-to-geolocation-extended-database-explained/694 Accessed: 2025-05-16.

[2] Carlos Azevedo. 2023. Gone offline: how Cloudflare Radar detects Internet outages. https://blog.cloudflare.com/detecting-internet-outages/ Accessed: 2025-04-09.

[3] Guillermo Baltra and John Heidemann. 2019. *Improving the optics of active outage detection (extended).* Technical Report. Technical Report ISI-TR-733. USC/Information Sciences Institute.

[4] Guillermo Baltra and John Heidemann. 2020. Improving Coverage of Internet Outage Detection in Sparse Blocks. In *Proceedings of the Passive and Active Measurement Workshop*. Springer, Eugene, Oregon, USA.

[5] David Belson. 2025. A diversity of downtime: the Q4 2024 Internet disruption summary. https://blog.cloudflare.com/q4-2024-internet-disruption-summary/ Accessed: 2025-04-09.

[6] David Belson. 2025. *New year, no shutdowns: the Q1 2025 Internet disruption summary.* Cloudflare. https://blog.cloudflare.com/q1-2025-internet-disruption-summary/ Accessed: 2025-04-22.

[7] Zachary S Bischof, Kennedy Pitcher, Esteban Carisimo, Amanda Meng, Rafael Bezerra Nunes, Ramakrishna Padmanabhan, Margaret E Roberts, Alex C Snoeren, and Alberto Dainotti. 2023. Destination unreachable: Characterizing internet outages and shutdowns. In *Proceedings of the ACM SIGCOMM 2023 Conference.* 608–621.

[8] Center for Countering Disinformation. 2023. *Occupiers use blackmail and threats to force Ukrainian providers to connect to Russian networks.* https://cip.gov.ua/ua/news/okupanti-shantazhem-i-pogrozami-zmushuyut-ukrayinskikh-provaideriv-pidklyuchatisya-do-rosiiskikh-merezh Accessed: 2025-04-24.

[9] Inc. Cloudflare. 2023. *One Year of War in Ukraine.* Cloudflare Blog. https://blog.cloudflare.com/one-year-of-war-in-ukraine/ Accessed: 2025-05-05.

[10] Developing Telecoms. 2024. *Kyivstar starts next phase of network backup-power upgrades.* https://developingtelecoms.com/telecom-technology/energy-sustainability/17551-kyivstar-starts-next-phase-of-network-backup-power-upgrades.html Accessed: 2025-05-12.

[11] DiXi Group. 2025. *Electricity outages lasted almost 2 thousand hours in 2024.* https://dixigroup.org/en/electricity-outages-lasted-2-thousand-hours-for-ukrainian-households-in-2024/ Accessed: 2025-04-22.

[12] Frédérick Douzet, Louis Pétiniaud, Loqman Salamatian, Kevin Limonier, Kavé Salamatian, and Thibaut Alchus. 2020. Measuring the fragmentation of the Internet: the case of the Border Gateway Protocol (BGP) during the Ukrainian crisis. In *2020 12th international conference on cyber conflict (CyCon)*, Vol. 1300. IEEE, 157–182.

[13] Zakir Durumeric, Eric Wustrow, and J Alex Halderman. 2013. {ZMap}: Fast internet-wide scanning and its security applications. In *22nd USENIX Security Symposium (USENIX Security 13).* 605–620.

[14] Romain Fontugne, Ksenia Ermoshina, and Emile Aben. 2020. The Internet in Crimea: a Case Study on Routing Interregnum. In *2020 IFIP Networking Conference.* Paris, France. https://hal.archives-ouvertes.fr/hal-03100247

[15] Florian Holzbauer, Markus Maier, and Johanna Ullrich. 2024. Destination Reachable: What ICMPv6 Error Messages Reveal About Their Sources. In *Proceedings of the 2024 ACM on Internet Measurement Conference.* 280–294.

[16] Intent Press. 2025. *Russians Shell 13 Settlements in Kherson Region, Killing 3 Civilians.* https://intent.press/en/news/war/2025/russians-shell-13-settlements-in-kherson-region-killing-3-civilians/ Accessed: 2025-04-22.

[17] IODA. 2023. Internet Outage Detection and Analysis (IODA). Retrieved Dec 12 2023 from https://www.caida.org/projects/ioda.

[18] IPinfo, Inc. 2025. IPinfo IP Geolocation API. https://ipinfo.io/products/ip-geolocation-api Accessed: 2025-03-19.

[19] Akshath Jain, Deepayan Patra, Peijing Xu, Justine Sherry, and Phillipa Gill. 2022. The ukrainian internet under attack: an NDT perspective. In *Proceedings of the 22nd ACM Internet Measurement Conference.* 166–178.

[20] João Tomé and David Belson. 2022. Tracking Shifts in Internet Connectivity in Kherson, Ukraine. Cloudflare Blog. Retrieved October 14, 2024, from https://blog.cloudflare.com/tracking-shifts-in-internet-connectivity-in-kherson-ukraine/.

[21] Kentik. 2015. Network Traffic Intelligence at Tomorrow's Scale. https://assets.ctfassets.net/6yom6slo28h2/6ByuKfku9UGGuwoKisU4go/b7299a843ccb30872d6b893286297b2b/Kentik-Overview-whitepaper-Jul2015.pdf

[22] Johannes Klick. 2023. How to use Internet scans and passive measurements to analyze Russian attacks and their impact in Ukraine. In *Chaos Communication Camp 2023* (Milliways, Chaos Communication Camp). Slides available.

[23] Mick Krever, Anna Chernova, Teele Rebane, Gianluca Mezzofiore, Tim Lister, and Sophie Tanno. 2022. *Ukrainian troops sweep into key city of Kherson after Russian forces retreat, dealing blow to Putin.* CNN. https://edition.cnn.com/2022/11/12/europe/kherson-city-ukraine-russia-intl/index.html Accessed: 2025-04-22.

[24] Kseniia Kunakh. 2024. *Kakhovka Dam Flooding Detection In Ukraine For PEJ.* EOS Data Analytics. https://eos.com/blog/kakhovka-dam-flooding-detection-in-ukraine-for-pej/ Accessed: 2025-04-22.

[25] Internet Intelligence Research Lab. 2025. Internet Outage Detection and Analysis (IODA) API v2. https://api.ioda.inetintel.cc.gatech.edu/v2/. Accessed: 2025-05-04.

[26] Valerio Luconi and Alessio Vecchio. 2023. Impact of the first months of war on routing and latency in Ukraine. *Computer Networks* 224 (2023), 109596.

[27] Doug Madory. 2022. Rerouting of Kherson follows familiar gameplan. Retrieved Jan 16 2024 from https://www.kentik.com/blog/rerouting-of-kherson-follows-familiar-gameplan/.

[28] Doug Madory. 2023. *Ukraine's Wartime Internet from the Inside.* https://www.kentik.com/blog/ukraines-wartime-internet-from-the-inside/ Accessed: 2025-05-15.

[29] Amanda Meng and Tara Kelly. 2025. *How Russia's Recent Attacks on Ukraine's Energy Grid Impacted its Internet Connectivity.* https://ioda.inetintel.cc.gatech.edu/reports/how-russias-recent-attacks-on-ukraines-energy-grid-impacted-its-internet-connectivity-2/ Accessed: 2025-05-16.

[30] Tal Mizrahi and Jose Yallouz. 2022. Internet Performance in the 2022 Conflict in Ukraine: An Asymmetric Analysis. *arXiv preprint arXiv:2205.08912* (2022).

[31] Tal Mizrahi and Jose Yallouz. 2022. Using Internet Measurements to Map the 2022 Ukrainian Refugee Crisis. *arXiv preprint arXiv:2205.08903* (2022).

[32] National Power Company Ukrenergo. 2025. Information on electricity consumption limitation measures. https://map.ua-energy.org/en/resources/0f8f9882-1fb2-47c6-81dc-31fbad914f16/. https://map.ua-energy.org/en/resources/0f8f9882-1fb2-47c6-81dc-31fbad914f16/ Dataset covering planned stabilization electricity outages for households across Ukraine. Data spans from January 1, 2023, to January 20, 2025. Last updated on January 21, 2025..

[33] Netblocks. 2022. Internet disruptions registered as Russia moves in on Ukraine. Retrieved Jan 16 2024 from https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K.

[34] Netblocks. 2022. Mobile internet disrupted in Luhansk, Ukraine amid heightened tensions with Russia. Retrieved Dec 12 2023 from https://netblocks.org/reports/mobile-internet-disrupted-in-luhansk-ukraine-amid-heightened-tensions-with-russia-l8Wx7LAO.

[35] NetBlocks. 2023. *Confirmed: Metrics indicate internet provider Volia in Kherson is experiencing a major outage.* https://x.com/netblocks/status/1668910973011279872 Accessed: 2025-04-24.

[36] Lin Quan, John Heidemann, and Yuri Pradkin. 2013. Trinocular: Understanding internet reliability through adaptive probing. *ACM SIGCOMM Computer Communication Review* 43, 4 (2013), 255–266.

[37] Philipp Richter, Ramakrishna Padmanabhan, Neil Spring, Arthur Berger, and David Clark. 2018. Advancing the art of internet edge outage detection. In *Proceedings of the Internet Measurement Conference 2018.* 350–363.

[38] RIPE NCC. 2024. RIPE NCC Statistics. Retrieved from https://ftp.ripe.net/pub/stats/ripencc/. Accessed: 2022-12-14.

[39] Erik Rye and Dave Levin. 2023. Ipv6 hitlists at scale: Be careful what you wish for. In *Proceedings of the ACM SIGCOMM 2023 Conference.* 904–916.

[40] Aaron Schulman and Neil Spring. 2011. Pingin'in the rain. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.* 19–28.

[41] James Shires and Isabella Wilkinson. 2024. *Internet resilience in Ukraine.* Technical Report. Chatham House. doi:10.55317/9781784136123 Accessed: 2025-04-22.

[42] Rishabh Singla, Shreyas Srinivasa, Narasimha Reddy, Jens Myrup Pedersen, Emmanouil Vasilomanolakis, and Riccardo Bettati. 2023. An analysis of war impact on Ukrainian critical infrastructure through network measurements. In *7th Network Traffic Measurement and Analysis Conference 2023.* IFIP.

[43] TASS. 2022. Integration of power grids of Crimea, rest of Russia completed — Deputy Energy Minister. *TASS* (29 December 2022). https://tass.com/politics/1557425 Accessed: 2025-05-10.

[44] Ukrinform. 2025. Regional chief reveals current population of Kherson region. https://www.ukrinform.net/rubric-society/3953685-regional-chief-reveals-current-population-of-kherson-region.html. Accessed: 23 April 2025.

[45] University of Oregon. 2024. University of Oregon Route Views Project. http://www.routeviews.org/routeviews/. Accessed: 2024-10-14.

A Ethics

We planned our measurements so as not to put additional load on the Internet of a country already at war. This includes only a single probe per two hours, randomized targets, a low probing rate of 8,000 packets per second, i.e., around 500KB/s from a single vantage point spread across all Ukrainian IP ranges and only minimal resources of these systems were used (e.g., ICMP instead of the stateful TCP), while platforms such as Censys are known to

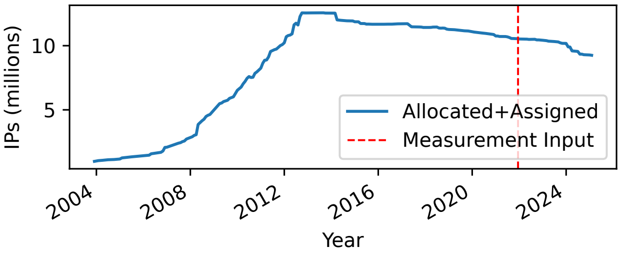

Figure 18: IPv4 address ranges with status allocated or assigned to UA from RIPE NCC over time.

probe multiple ports multiple times a day. Furthermore, we offered additional information, contact details, and the option to opt out via a web server. We received only one opt-out request, not due to resource strain, but because the requester preferred not to be included in our data.

Our results offer insight into the resilience and state of the Ukrainian Internet during wartime, but they do not reveal information that could be directly exploited to further endanger the country. Access to the underlying data is therefore carefully controlled. While Internet outage measurements can be independently collected by others, unrestricted release could enable adversaries to assess the effectiveness of attacks on power supply or network infrastructure (e.g., in frontline regions) without relying on other sources such as satellite imagery or reconnaissance.

At the same time, the data is of clear scientific and societal value: it allows researchers to quantify and verify the impact of concrete events on Internet availability, such as the seizure of infrastructure, as was evaluated in this paper. To balance these interests, we provide block-level availability data to the research community and if requested anonymized IP-level responsiveness, which avoids privacy risks while enabling meaningful analysis. Any further release of more detailed data is coordinated in consultation with the national CERT of Ukraine.

B Country-specific IP ranges

Using a one-time snapshot of the delegated files as input lets us track prefixes over time. While BGP-announced prefixes are subject to frequent changes, allocated and assigned prefixes tend to be more stable.

For Ukraine, we observed the following trends: out of the initial 3,085 allocated ranges, 3,026 (98%) still existed as of January 2025, with 2,678 (87%) remaining allocated to Ukraine. This means that 348 prefixes (12%) have changed country codes. Among these, 31% are now assigned to Russia (*RU*), 13.5% to the United States (*US*), 11% to Poland (*PL*), 9% to Latvia (*LV*), and the remaining third to other, mostly European, countries. In the second snapshot, we identified a total of 2,876 IP ranges still belonging to Ukraine.

Two key observations emerge from this analysis. First, the total number of IP allocations in Ukraine has decreased by 7%. We find the impact of new allocations to be minor since our snapshot. Figure 18 shows the development since 2004. Second, 12% of previously Ukrainian prefixes have now been reassigned to different country codes, but might still be valuable measurement targets.

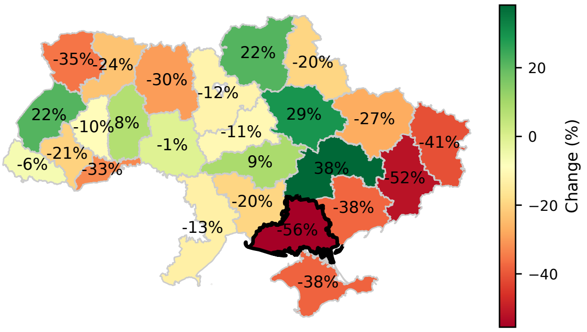

Figure 19: Churn of all IPv4 addresses locating to oblasts in Ukraine, comparing 2022-02-01 to 2025-02-01.

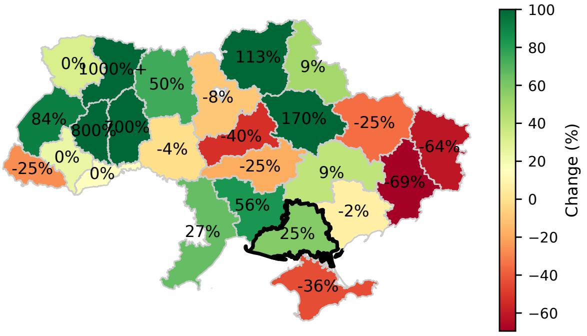

Figure 20: Churn of all IPv6 addresses locating to oblasts in Ukraine, comparing 2022-02-01 to 2025-02-01.

C Extended IP Churn

To compare IP churn of measurement targets to all IPv4 addresses, we include Figure 19, which is the same as Figure 1, without the restriction to our measurement targets in the Appendix. While most oblasts show similar churn, Luhansk differs by 26 percentage points, Crimea by 17, Zaporizhia by 14, Mykolaiv by 7, Khmelnytskyi and Kherson by six, and all others by below five.

IPv6 Churn. . While there is a noticeable decrease in IPv4 addresses across Ukraine, a different picture emerges for IPv6. We replicate Figure 19 in Figure 20 for IPv6. We find a noticeable increase in IPv6 adoption across Ukraine. Regions with low or no IPv6 adoption show a high increase in percentage points (Rivne, Ternopil, and Khmelnytskyi). It could be especially interesting for regions with noticeable decreases in IPv4 addresses, such as Kherson, Mykolaiv, and Sumy, to include IPv6 measurements in the future.

D Regional ASes and Blocks

Mapping blocks to regions in Ukraine shows around 14% of blocks that point to multiple regions. If the block meets the regional criteria in one region, we will only consider the part of the block that is

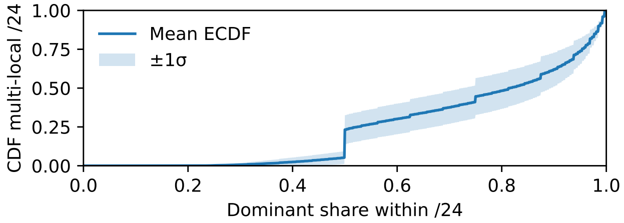

Figure 21: CDF of blocks highlighting the share of IPs pointing to the dominant location for multi-local /24 blocks.

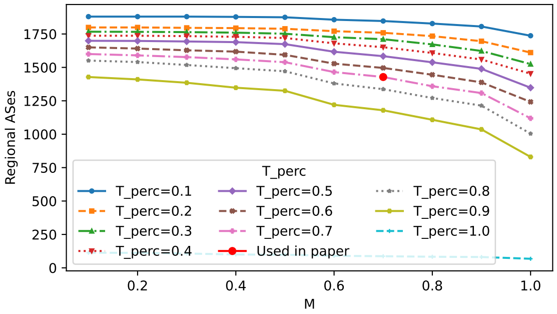

Figure 22: Choice of parameters M and T_perc and their impact on the number of regional ASes.

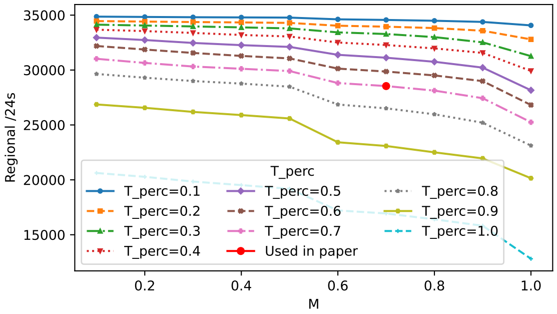

Figure 23: Choice of parameters M and T_perc and their impact on the number of regional /24s

locating to the target region. However, as Figure 21 shows there is usually a majority of IPs in the block that geolocate to the dominant region. To better limit the impact of noise in geolocation data, we separate regional from non-regional blocks and ASes in Ukraine. Figure 23 illustrates the sensitivity on the block level while Figure 22 on the AS level to varying values of the geolocation threshold (M) and the required percentage of routed months (T_{perc}). We test both parameters, ranging from 0 to 1 in steps of 0.1.

Using the strictest setting ($M = 0.9$, $T_{perc} = 0.9$), we classify 1036 out of 2024 ASes (51.19%) as regional, resulting in 21,952 regional subblocks. A majority setting ($M = 0.5$,$T_{perc} = 0.5$) yields 1674 regional ASes (82.71%) and 32,107 regional subblocks. We adopt $M = 0.7$, $T_{perc} = 0.7$ as a balanced configuration, identifying 1428 regional ASes (70.55%) and 28,541 regional subblocks. This compromise avoids over-classification due to noisy geolocation while still capturing consistent regional behavior.

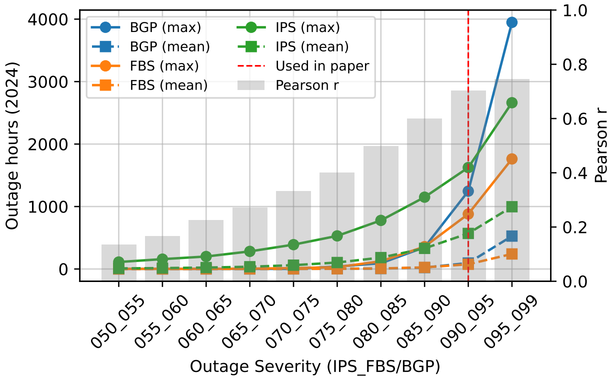

Figure 24: Different regional outage severity thresholds and the respective outage hours in 2024 in non-frontline regions and the correlation coefficient with power outages.

E Outage Severity and Threshold Sensitivity

We evaluate how different outage thresholds affect the number of reported outage hours. Our analysis focuses on Internet outages detected throughout 2024 in non-frontline regions, where we can correlate Internet disruptions with reported power outages from Ukrenergo (see Section 5.1). Outage severity is measured as the deviation from the moving average over the previous week. Figure 24 shows results for thresholds ranging from 50% to 99%. The *IPS* ▲ signal applies a threshold that is five percentage points stricter than the other outage signals, since it is more volatile and IPs typically fail before entire blocks do. We observe that only a small fraction of outages affect 50% or more of IPs or blocks in a region. At the other end of the spectrum, the most sensitive threshold, which is triggered when just 5% of IPs or 1% of blocks go offline, likely overestimates outage hours. We reach a similar correlation with reported power outages already at lower thresholds, namely 10% IP loss or 5% block loss (through unresponsiveness or loss of BGP visibility). Using these thresholds reduces the number of reported outage hours while capturing more relevant events.

F AS-level Disruptions Kherson

Target ASes. Table 5 lists ASes with regional /24s in the Kherson oblast. ASes are split into regional and non-regional and ranked by their number of regional /24s inside the category. For all 34 ASes, we manually investigated the location of their headquarters. Most regional ASes are headquartered in the Kherson oblast, with only one based in Kyiv. In contrast, the majority of non-regional ASes are headquartered in Kyiv. Note that we did not restrict non-regional ASes to those registered in Ukraine; as a result, two foreign ASes appear in the non-regional group. We observe six regional ASes in Kherson that each have only a single regional /24. Similarly,

ASN	/24s	Reg.	Org.	HQ	IODA [17]	RU [20]	⊘ [45]
49465	16	16	RubinTV	N. Kakhov	○	●	○
56404	8	8	Norma4	Kherson	○	●	○
56359	5	5	RostNet	Oleshky	○	●	●
25482	4	3	Status	Kherson	○	●	○
15458	2	2	TLC-K	Kherson	○	●	●
47598	3	2	Kherson Telecom	Kherson	○	●	●
56446	2	2	OstrovNet	Kherson	○	●	○
25256	1	1	M-Net	Henichesk	○	○	●
34720	1	1	JSC-Chumak	Kyiv	○	○	●
42469	1	1	Askad	Skadovsk	○	○	●
44737	1	1	Next	Kherson	○	○	●
59500	1	1	LineVPS	Kherson	○	○	○
211171	1	1	Pluton	Kherson	○	●	○
25229	190	160	Volia	Kyiv	●	○	○
15895	299	52	Kyivstar	Kyiv	●	○	○
6877	239	49	Ukrtelecom	Kyiv	●	○	○
6849	682	31	Ukrtelecom	Kyiv	●	○	○
6703	29	12	Vega	Kyiv	●	○	○
21151	18	10	Ukrcom	Kherson	○	●	○
6698	16	9	Virtualsystems	Kyiv	●	○	○
30823	6	6	Aurologic	Langen(DE)	●	○	○
205172	6	6	Yanina	Kherson	○	○	●
39862	7	4	Digicom	Kherson	○	○	○
57498	4	3	Smart-M	Kherson	○	○	●
2914	2	2	NTT	Redmond(US)	●	○	○
12883	8	2	Vega	Kyiv	●	○	○
25082	12	2	Viner Telecom	Kherson	○	●	○
35213	12	2	CompNetUA	Kherson	○	○	○
49168	2	2	Brok-X	Kherson	○	●	○
6846	7	1	Infocom	Kyiv	●	○	○
12687	1	1	Uran Kiev	Kyiv	●	○	○
45043	4	1	Viner Telecom	Kherson	○	○	○
197361	1	1	LLC AIT	Kherson	○	●	●
215654	1	1	Genicheskonline	Henichesk	○	○	○

/24s in Ukraine, Regional, Non-Regional, ⊘ No BGP prefixes in 2025

Table 5: Regional and non-regional ASes in Kherson, showing number of regional /24s, headquarters, IODA coverage, reports on rerouting, and whether they announced any prefixes in 2025.

five non-regional ASes, mostly larger ISPs, also show a single regional /24 in the oblast. Despite the limited number of responsive IPs (1,400 in 2025), we find that most ASes in Kherson remained responsive if they maintained their service in the region. We also examine third-party reporting. IODA [25] has reported outages for a subset of larger, non-regional ASes in Kherson (see § 5.4). Cloudflare [9] identified 15 ASes in 2022 as rerouting traffic via Russian upstreams; 12 of them are included in Table 5. By 2025, RouteViews BGP tables [45] reveal that seven of the 13 regional ASes had ceased announcing any prefixes, suggesting that many local operators were either decommissioned or had permanently shut down operations in the region.

Disruption Timeline. Figure 28 extends Figure 11 to cover the entire measurement period. Despite only 7% responsiveness for regional IPs in Kherson, we are still able to observe outage signals for most ASes in the region, including those with only a single regional /24. Over the three-year period, a significant portion of regional /24s belonging to non-regional ASes are not visible in BGP. During the Russian occupation, many of these address ranges were disconnected—particularly for ASes such as Vega (Alkar), Smart-M, and Yanina—which remained offline for extended periods. Volia was also disconnected but reappeared after the liberation of the right bank. While for non-regional we see that blocks initially not visible in BGP were announced during the measurement period, as visible for Brok-X, Genicheskonline, NTT. Regional providers show the opposite of being active in Kherson first and then discontinuing their service, probably due to falling subscriber bases, as was reported by the Status ISP. We observe that connectivity in Kherson experienced repeated cycles of disruption and restoration. Major outage periods coincide with known events such as the severing of the Mykolaiv cable and the destruction of infrastructure during the Russian retreat. Additionally, a clearly visible multi-AS disruption occurred on November 28th, as was captured by the IODA regional signal [29] for Kherson.

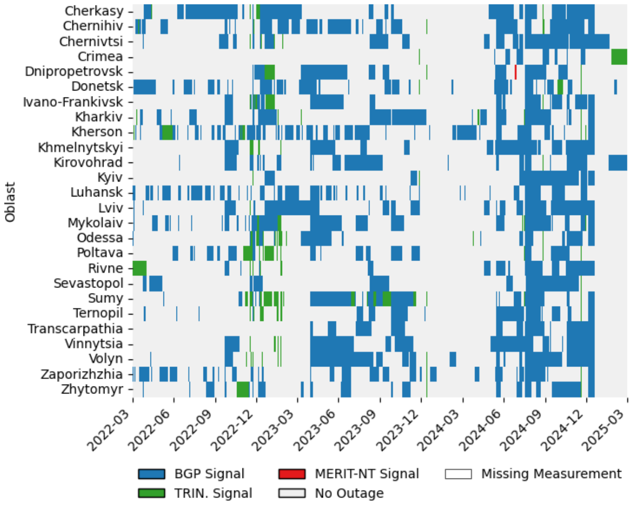

Figure 25: IODA outages reported for regions in Ukraine.

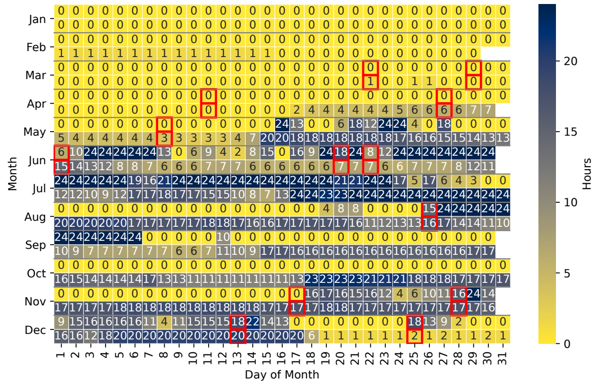

Figure 26: Comparison of daily average hours of power outages reported by Ukrenergo [32] (top row) and Internet disruptions detected by IODA (bottom row) for non-frontline regions in 2024. Days marked in red correspond to reported attacks as documented by [11].

G IODA Signal

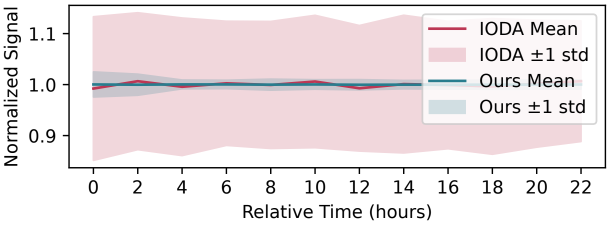

Figure 27: Signal deviation from the mean of one day (March 2, 2023) for the IODA (Trinocular) signal and our signal across 1,073 ASes without signal loss (# of active /24s = 0).

Signal Stability. We further evaluate possible reasons for the differences in AS coverage. First, we look at the number of ASes that IODA includes active /24s (*TRIN*🟩) data. For this, we request raw data for one day in each year from 2022 to 2025 from [25] for each of the ASes (YYYY-03-02). We find that IODA includes data, in at least one year, for 90% of ASes (1,597 out of 1,773). Block eligibility does not seem to be the issue here. As we found that IODA does not report outages for smaller providers, i.e. with less than 20 /24s, we will look at signal stability in the next step. Figure 27 visualizes the IODA and our signal recorded over one day for ASes that include values for each bi-hourly interval. We find the signal spread to be much more prominent for Trinocular (avg Signal to Noise Ratio=7.6) than for our signal (avg. SNR=99.7; higher=clearer signal). This can be a problem when detecting disruptions for smaller ASes, as unresponsive blocks in ASes with few /24 blocks are more likely to trigger thresholds (80% warning, 50% critical). This likely caused the filter by Richter et al. [37] to exclude blocks with many down events.

IODA Outage Events. To compare outage events with IODA on a regional level, we replicated Figure 8 with IODA outage events reported for the different oblasts in Ukraine in Figure 25, showing the number of recorded outages over the three years for each of the outage signals. Compared to Figure 8 showing detected outages by our dataset, which only shows shorter outage periods on the oblast level, IODA shows long-lasting BGP signal-driven outages on the oblast level. We assume the reason to be the following: through assigning both regional and non-regional ASes to oblasts in Ukraine, BPG outages for non-regional ASes have a stronger effect on IODA data. However, this means that the BGP outage of a single non-regional provider can affect outage data in multiple regions. Apart from this, the active probing signal from Trinocular is visible in green, reporting some additional outages not visible in BGP. The merit signal is based on traffic originating from regions in Ukraine to a so-called Darknet, that is routed address space monitored for incoming traffic. The contribution of the two other signals compared to BGP on the regional level is, however, marginal.

Non-Frontline Disruptions. We further investigate reported outages for non-frontline regions, replicating Figure 9 with IODA data in Figure 26. We aggregate hours affected by Internet outages in non-frontline regions and plot them on a daily basis in 2024. The figure visualizes the lower Pearson coefficient for IODA data in relation to reported power outages in non-frontline regions, which is highly likely caused by IODA's long-lasting BGP outages.

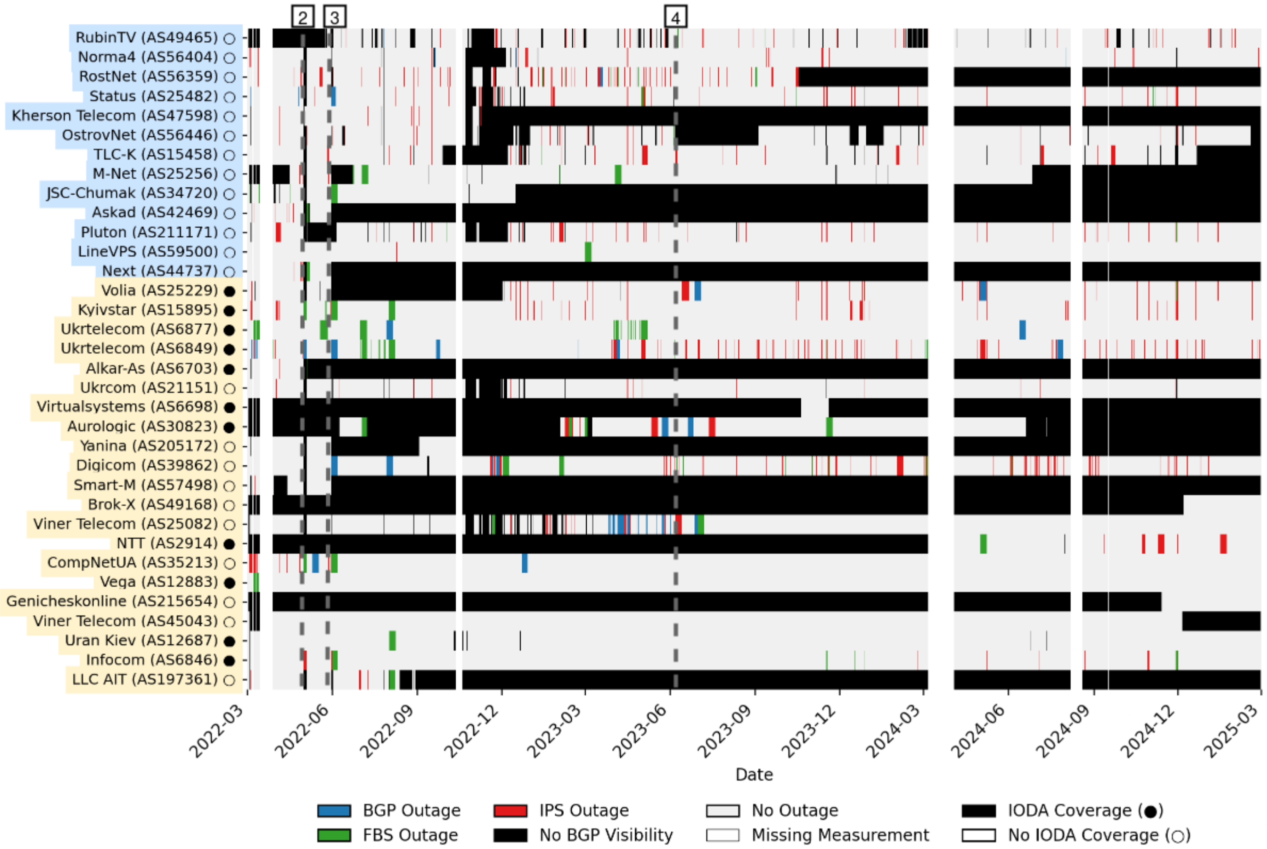

Figure 28: Internet disruptions recorded by any of the three signals for ASes in Kherson from 2022 to 2025. Most ASes show long-lasting BGP visibility loss in the region.