universität wien

```
> EHLO grace.univie.ac.at
> MAIL FROM:<florian.holzbauer@univie.ac.at>
> RCPT TO:<defensio@univie.ac.at>
> DATA
```

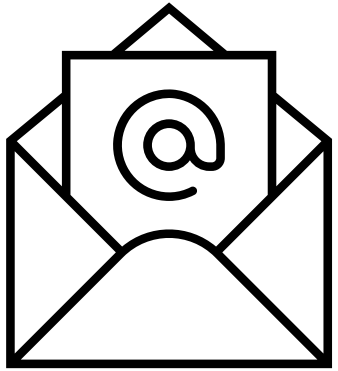
Turning Failure into Knowledge:
Extending the Observable Internet by Leveraging Delivery Failures

Supervisors: Johanna Ullrich (IT:U); Edgar Weippl (Universität Wien)

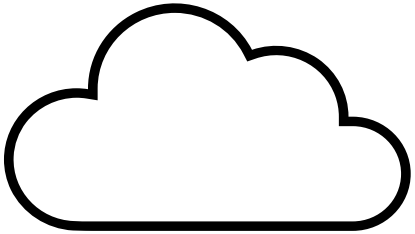
Reviewers: Georgios Smaragdakis (TU Delft); Oliver Hohlfeld (Universität Kassel)

Chair: Helmut Hlavacs (Universität Wien)

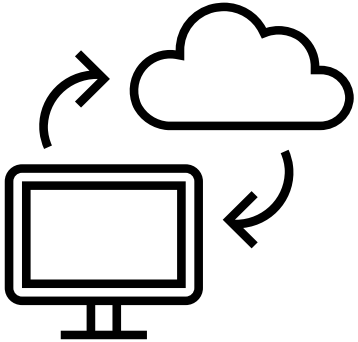
Leveraging Delivery Failures for measuring:



1. Email Security



2. IPv6 Reconnaissance



3. Internet Disruptions

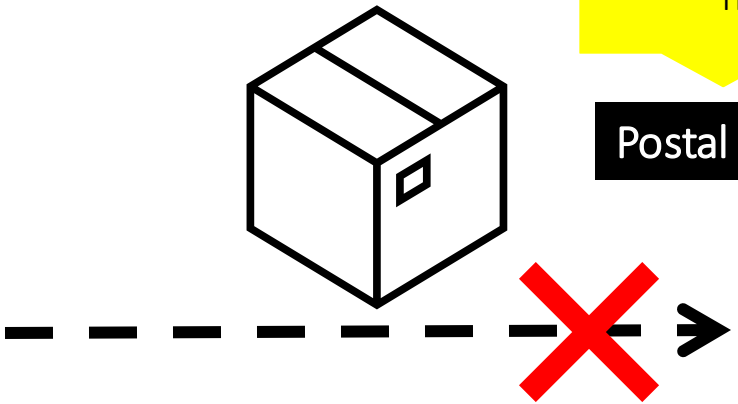
Research Question

Sorry, we encountered an error delivering your packet. The recipient was not present.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   6   | Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Payload Length          |     58        |     56        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 2001:db8:200:1000::ab     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      2001:db8:5ba::1           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     1     |       3       |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Identifier          |        Sequence Number        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Destination Unreachable
+-+-+-+-+-
```

Postal System

Internet



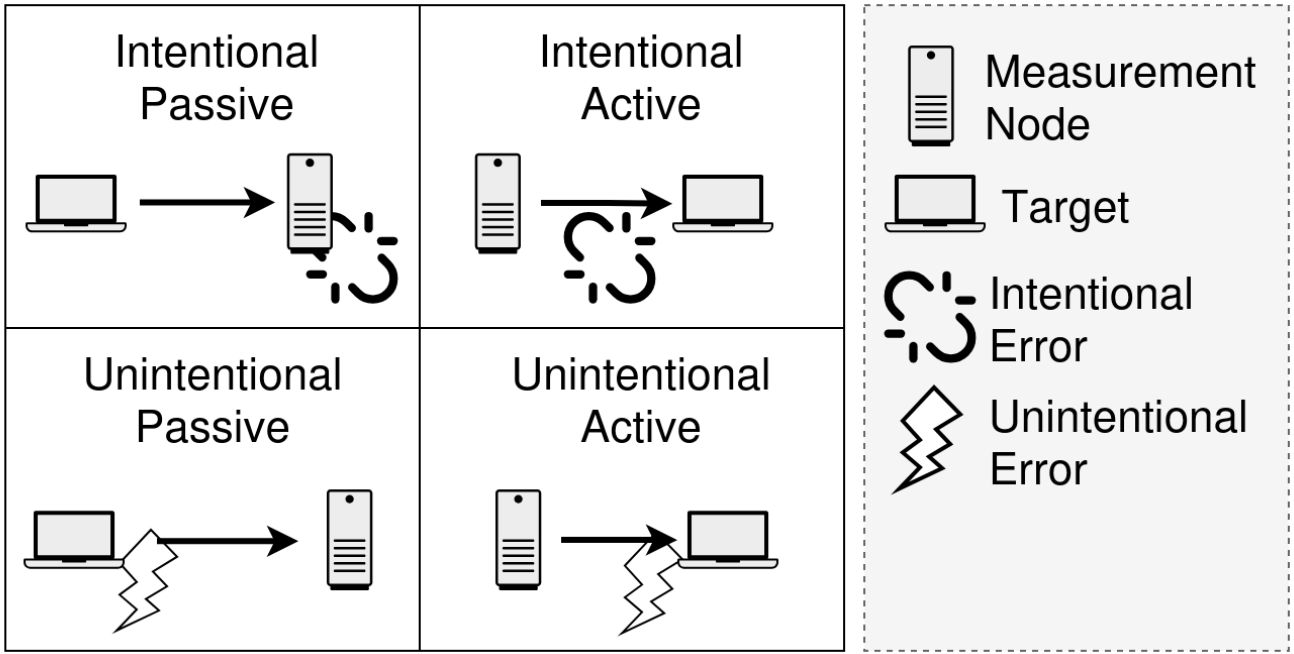
1-Error Message

2-No Response

What can be learned from delivery failures about Internet protocols and reachability?

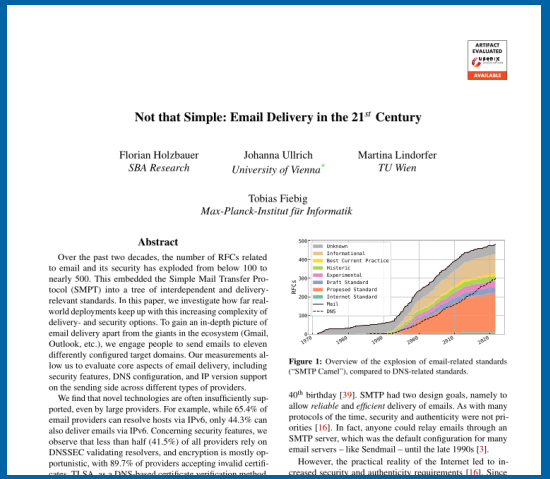
universität wien

Delivery Failures: Intentional vs Unintentional



Delivery Failures: Intentional Passive

Publication at Usenix ATC'22



Not that Simple: Email Delivery in the 21st Century

Florian Holzbauer, SBA Research
Johanna Ullrich, University of Vienna
Martina Lindorfer, TU Wien
Tobias Fiebig, Max-Planck-Institut für Informatik

Abstract

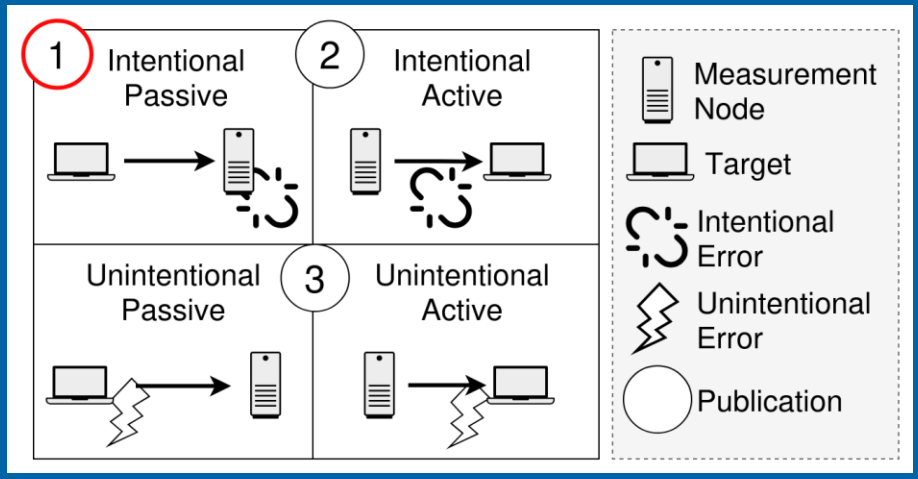
Over the past two decades, the number of RFCs related to email and its security has exploded from below 100 to nearly 500. This embedded the Simple Mail Transfer Protocol (SMPT) into a tree of interdependent and delivery-relevant standards. In this paper, we investigate how far real-world deployments keep up with this increasing complexity of delivery- and security options. To gain an in-depth picture of email delivery apart from the giants in the ecosystem (Gmail, Outlook, etc.), we engage people to send emails to eleven differently configured target domains. Our measurements allow us to evaluate core aspects of email delivery, including security features, DNS configuration, and IP version support on the sending side across different types of providers.

We find that novel technologies are often insufficiently supported, even by large providers. For example, while 65.4% of email providers can resolve hosts via IPv6, only 44.3% can also deliver emails via IPv6. Concerning security features, we observe that less than half (41.5%) of all providers rely on DNSSEC validating resolvers, and encryption is mostly opportunistic, with 89.7% of providers accepting invalid certificates. TLSA- or DNS-based certificate verification method

Figure 1: Overview of the explosion of email-related standards ("SMTP Camel"), compared to DNS-related standards.

40th birthday [39]. SMTP had two design goals, namely to allow *reliable* and *efficient* delivery of emails. As with many protocols of the time, security and authenticity were not priorities [16]. In fact, anyone could relay emails through an SMTP server, which was the default configuration for many email servers – like Sendmail – until the late 1990s [3].

However, the practical reality of the Internet led to increased security and authenticity requirements [16]. Since



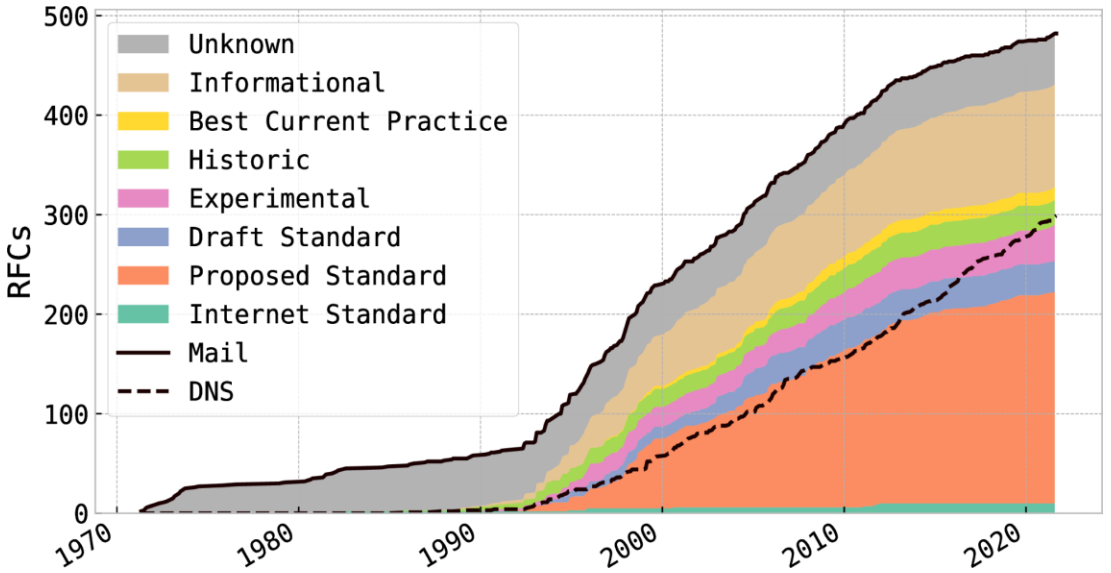
Holzbauer, F., Ullrich, J., Lindorfer, M., Fiebig, T. Not that Simple: Email Delivery in the 21st Century, USENIX Annual Technical Conference (ATC), 2022. CORE: A

universität wien

The Email Ecosystem

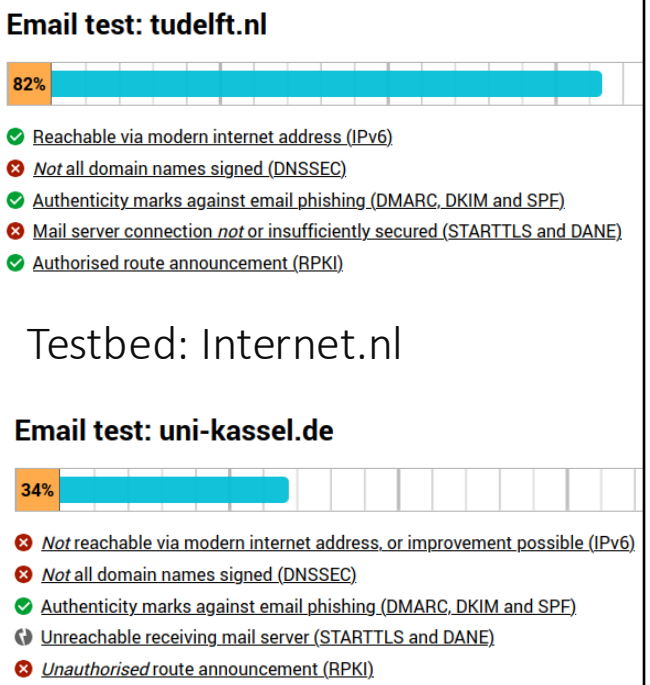
- Standardized in the **early** Internet
- **Billions of emails** transmitted daily
- Many **smaller** operators

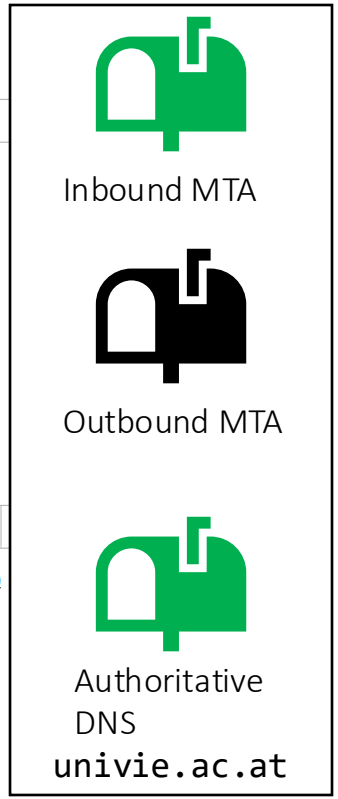
- Transport Encryption: **opportunistic**
- End-to-End encryption: **lacks adoption**



universität wien

The Need to Study Email Delivery





What related testbeds typically miss:

-> How email is actually delivered!

- Which resolver uses the outbound MTA, does it **validate DNSSEC**?
- Delivery in **plaintext**?
- Are **self-signed** certs validated?
- Is **strict TLS** supported? (DANE, MTA-STS)

Why should we care: 96% of emails from Tunisia to Google > downgraded to plaintext [14]

universität wien

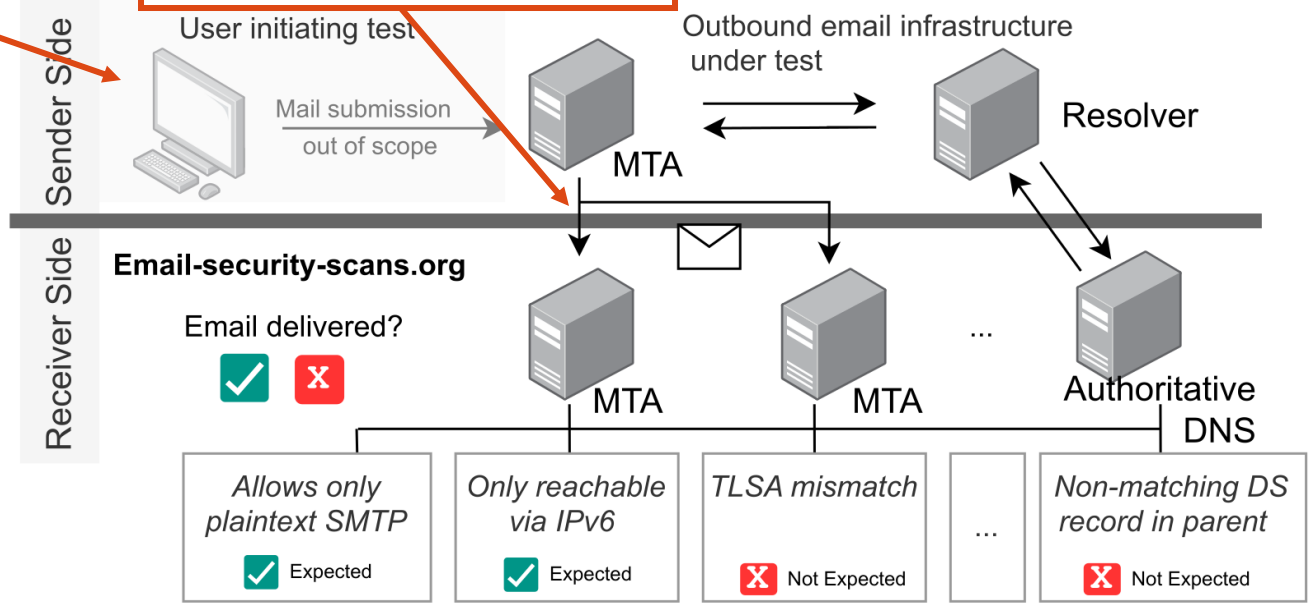
Intentional Passive – Email Testbed

User can choose implicit TLS, HTTPS

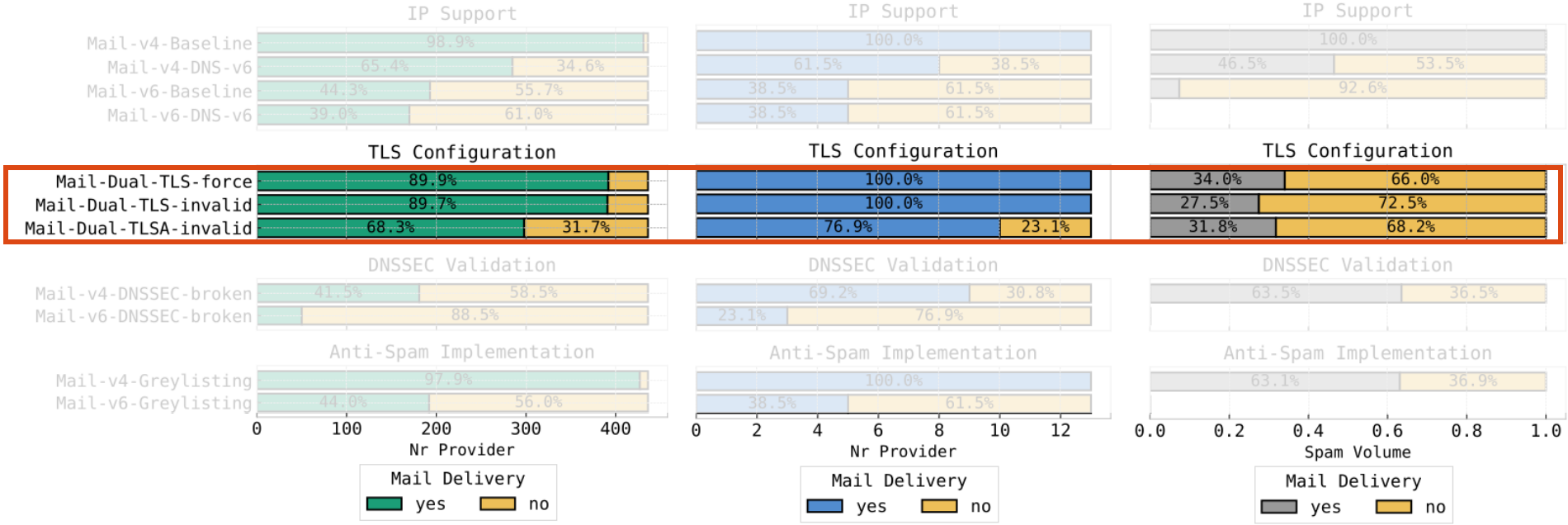
User cannot choose security between Mail-Transfer Agents

email-security-scans.org

Target group: users & operators

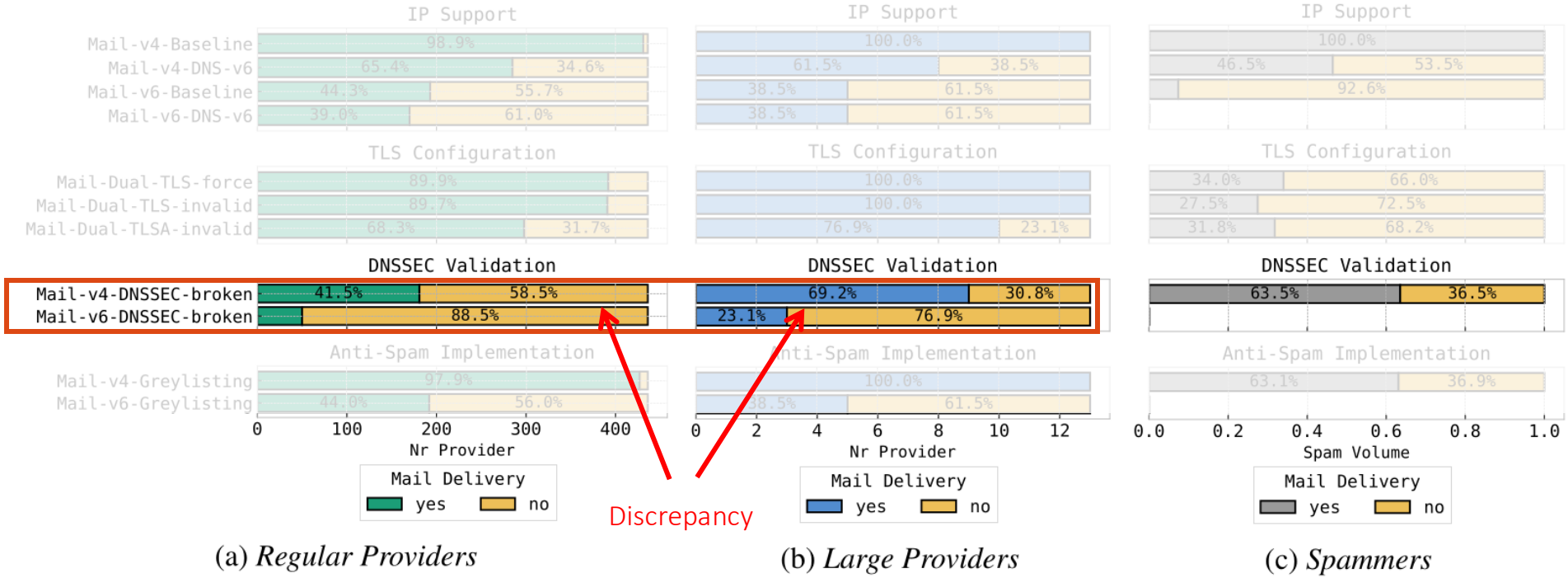


Initial Study: 417 Providers, 53 Countries



(a) *Regular Providers* (b) *Large Providers* (c) *Spammers*

Initial Study: 417 Providers, 53 Countries



(a) *Regular Providers* (b) *Large Providers* (c) *Spammers*

Continuous Operation

- What we learn from email-security-scans.org:

Year	Plaintext	STARTTLS	DANE Validation	IPv6 (MTA)	IPv6 (DNS)
2020/21	99%	90%	22%	44%	65%
2023	97%	97%	27%	58%	73%
2024	93%	98%	30%	56%	77%
2025	**91%**	**99%**	**38%**	**60%**	**82%**

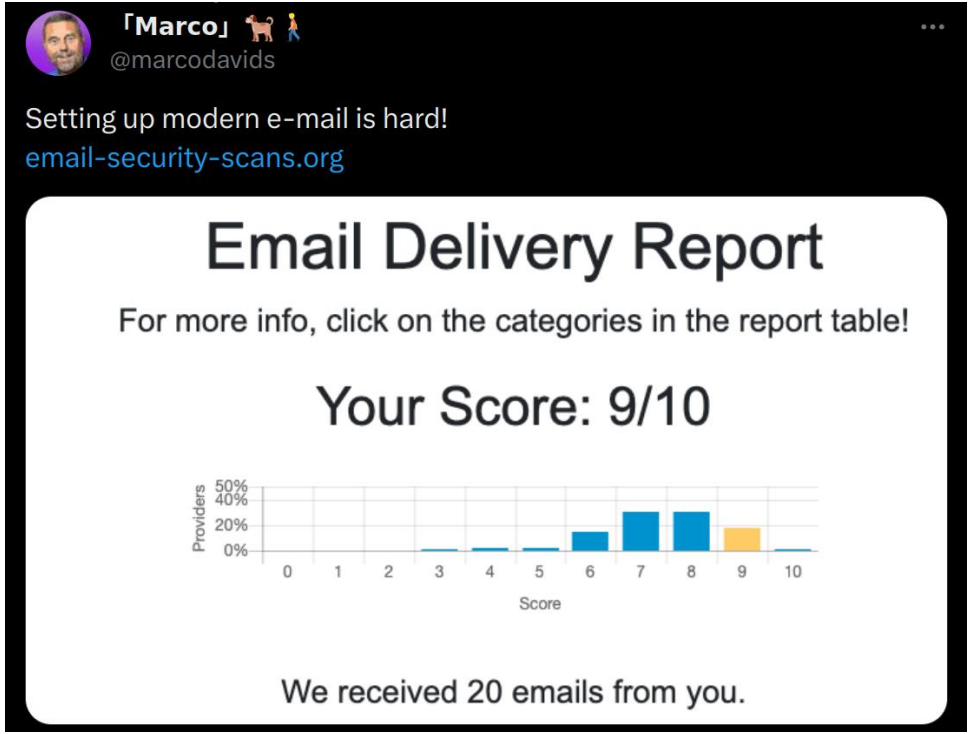
Conclusion Email Delivery

Measurement platforms motivate standard adoption

Over 80% of users (with multiple tests; 1/5 of total) improve their email configuration after the first test

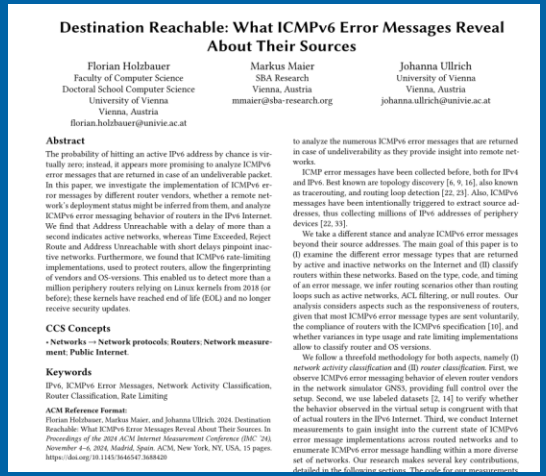
Allows to detect trends in improvements:

- 2023/24: DKIM, DANE and IPv6
- 2025: SPF validity (missing ip6 mechanisms)



Delivery Failures: Intentional Active

Publication at IMC'24



Destination Reachable: What ICMPv6 Error Messages Reveal About Their Sources

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

Markus Maier
SBA Research
Vienna, Austria
mmaier@sba-research.org

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

Abstract

The probability of hitting an active IPv6 address by chance is virtually zero; instead, it appears more promising to analyze ICMPv6 error messages that are returned in case of an undeliverable packet. In this paper, we investigate the implementation of ICMPv6 error messages by different router vendors, whether a remote network's deployment status might be inferred from them, and analyze ICMPv6 error messaging behavior of routers in the IPv6 Internet. We find that Address Unreachable with a delay of more than a second indicates active networks, whereas Time Exceeded, Reject Route and Address Unreachable with short delays pinpoint inactive networks. Furthermore, we found that ICMPv6 rate-limiting implementations, used to protect routers, allow the fingerprinting of vendors and OS-versions. This enabled us to detect more than a million periphery routers relying on Linux kernels from 2018 (or before); these kernels have reached end of life (EOL) and no longer receive security updates.

CCS Concepts

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

Keywords

IPv6, ICMPv6 Error Messages, Network Activity Classification, Router Classification, Rate Limiting

ACM Reference Format:

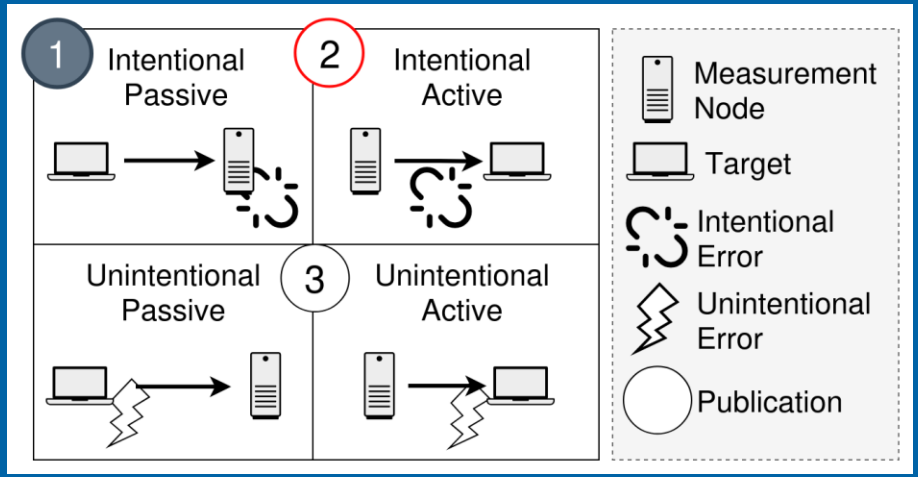
Florian Holzbauer, Markus Maier, and Johanna Ullrich. 2024. Destination Reachable: What ICMPv6 Error Messages Reveal About Their Sources. In *Proceedings of the 2024 ACM Internet Measurement Conference (IMC '24), November 4–6, 2024, Madrid, Spain.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3646547.3688420

to analyze the numerous ICMPv6 error messages that are returned in case of undeliverability as they provide insight into remote networks.

ICMP error messages have been collected before, both for IPv4 and IPv6. Best known are topology discovery [6, 9, 16], also known as traceroute, and routing loop detection [22, 23]. Also, ICMPv6 messages have been intentionally triggered to extract source addresses, thus collecting millions of IPv6 addresses of periphery devices [22, 33].

We take a different stance and analyze ICMPv6 error messages beyond their source addresses. The main goal of this paper is to (I) examine the different error message types that are returned by active and inactive networks on the Internet and (II) classify routers within these networks. Based on the type, code, and timing of an error message, we infer routing scenarios other than routing loops such as active networks, ACL filtering, or null routes. Our analysis considers aspects such as the responsiveness of routers, given that most ICMPv6 error message types are sent voluntarily, the compliance of routers with the ICMPv6 specification [10], and whether variances in type usage and rate limiting implementations allow to classify router and OS versions.

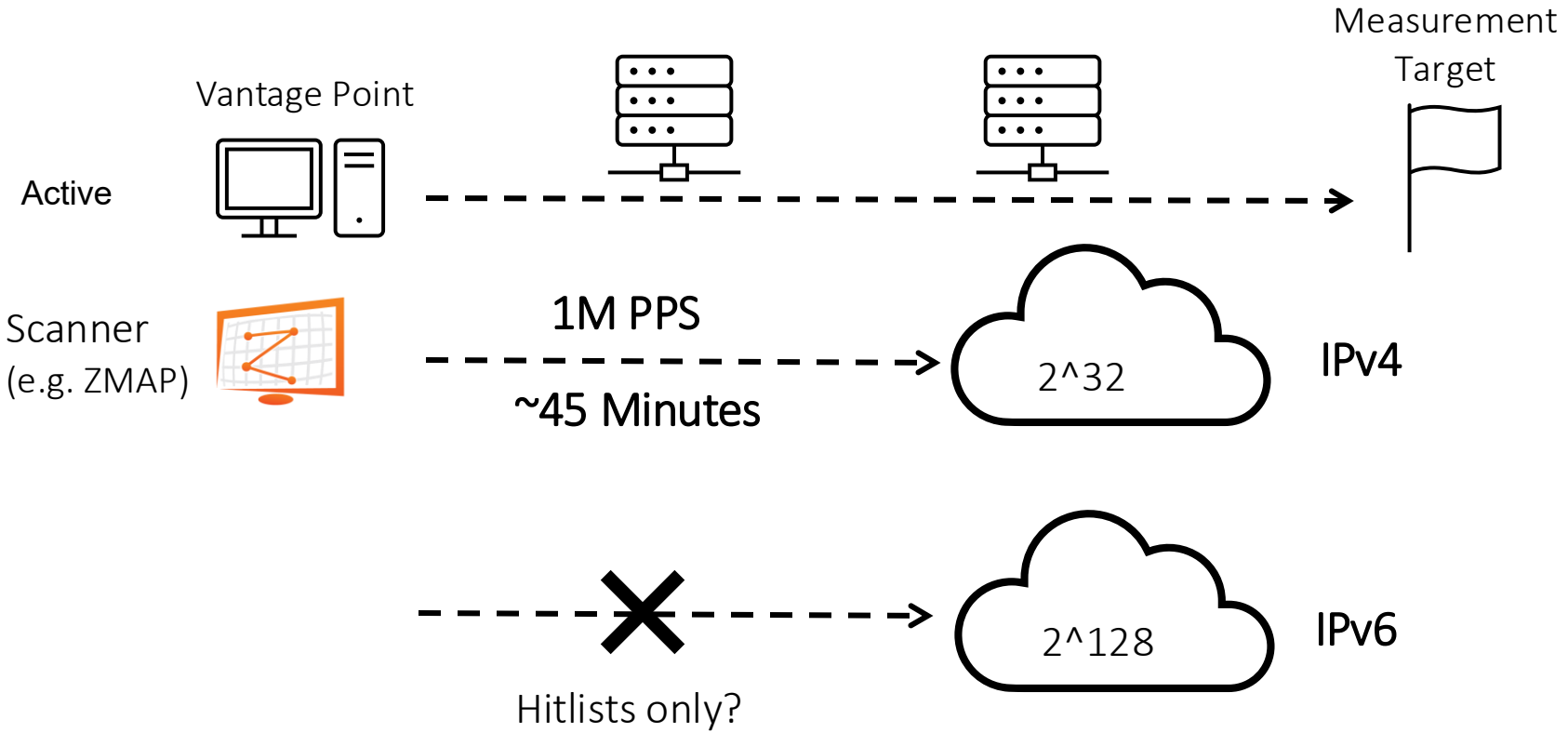
We follow a threefold methodology for both aspects, namely (I) *network activity classification* and (II) *router classification*. First, we observe ICMPv6 error messaging behavior of eleven router vendors in the network simulator GNS3, providing full control over the setup. Second, we use labeled datasets [2, 14] to verify whether the behavior observed in the virtual setup is congruent with that of actual routers in the IPv6 Internet. Third, we conduct Internet measurements to gain insight into the current state of ICMPv6 error message implementations across routed networks and to enumerate ICMPv6 error message handling within a more diverse set of networks. Our research makes several key contributions, detailed in the following sections. The code for our measurements



Holzbauer F., Maier, M., Ullrich, J. Destination Reachable: What ICMPv6 Error Messages Reveal about their Sources, Internet Measurement Conference (IMC), 2024. CORE: A

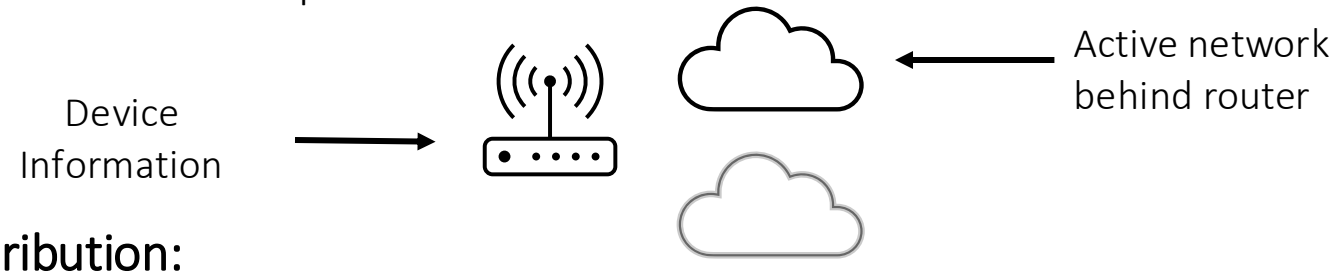
universität wien

Active IPv6 Measurements



Delivery Failures: Intentional Active

Analyze ICMPv6 error messages that are returned by IPv6 periphery even when the target address does not respond



Contribution:

- **Network Activity Classification:** interpret ICMPv6 error messages to infer whether a remote network is active or inactive
- **Router Classification:** ICMPv6 rate limits are different among routes

  and can be used for fingerprinting the router vendor

Network Classification

1. Controlled Environment

Router Lab

2. Verification in the IPv6 Internet

BValue Steps

3. IPv6-wide Measurements

ZMap

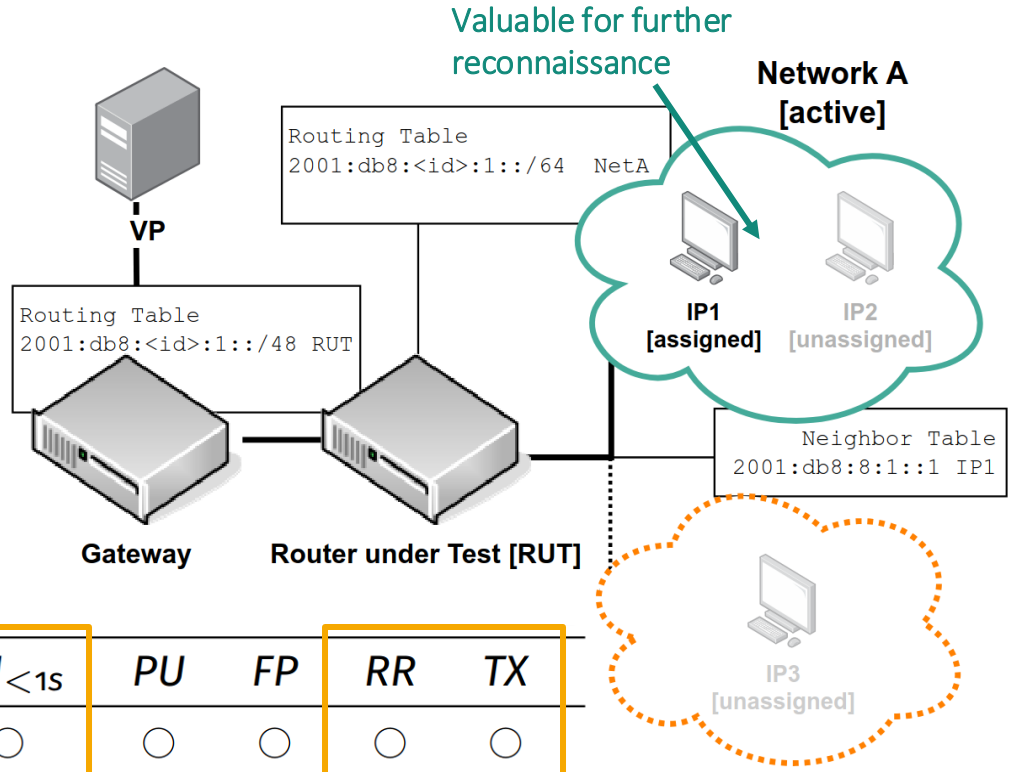
Controlled Environment Router Lab

Investigated **Error Types**:

- Destination Unreachable and its six subcodes (NR to RR)
- Time Exceeded (TX)

6 Routing Scenarios:

- No ACL (2x), ACL (2x), Null Route, Routing Loop



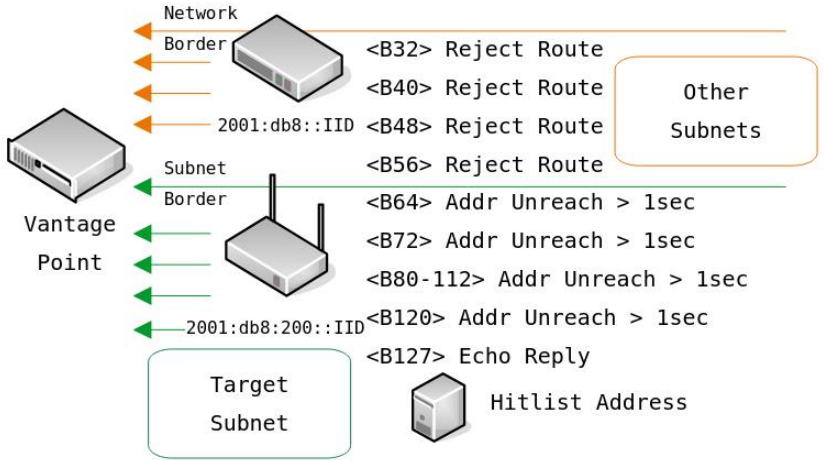
Status	NR	AP	$AU_{>1s}$	$AU_{<1s}$	PU	FP	RR	TX
active	○	○	●	○	○	○	○	○
inactive	○	○	○	●	○	○	●	●
ambig.	●	●	○	○	●	●	○	○

universität wien

sbaresearch/router-lab

Verify: BValue Steps

```
Original hitlist address:
        2001:db8:1234:abcd:1234:abcd:1234:0101
Generated addresses:
        <original bits>          <random bits>
B127    2001:db8:1234:abcd:1234:abcd:1234:0100
B120    2001:db8:1234:abcd:1234:abcd:1234:01e8
B112    2001:db8:1234:abcd:1234:abcd:1234:6aa1
B104    2001:db8:1234:abcd:1234:abcd:1221:f38d
...
B48     2001:db8:abcd:5276:d080:ccd6:7fc3:311c
B40     2001:db8:ab3e:3eb7:4c66:7f16:ade5:2b3d
B32     2001:db8:7438:221f:b244:476c:66bb:8da5
```



Verify: BValue Steps

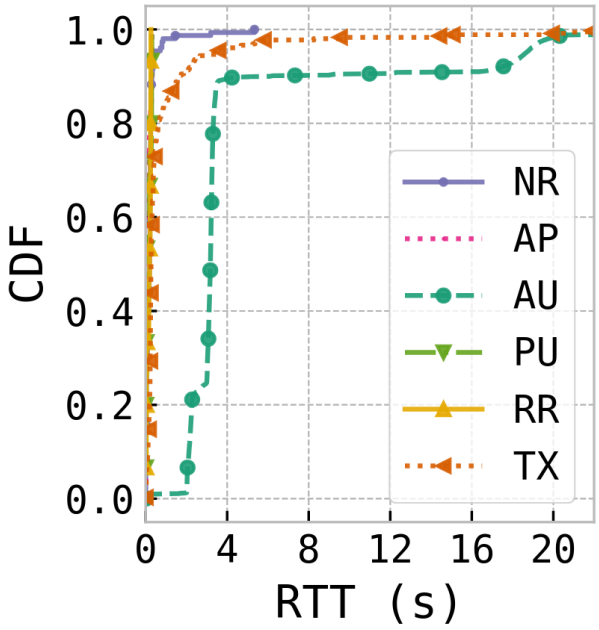


Figure: RTT of error messages for labeled active networks

True Positives

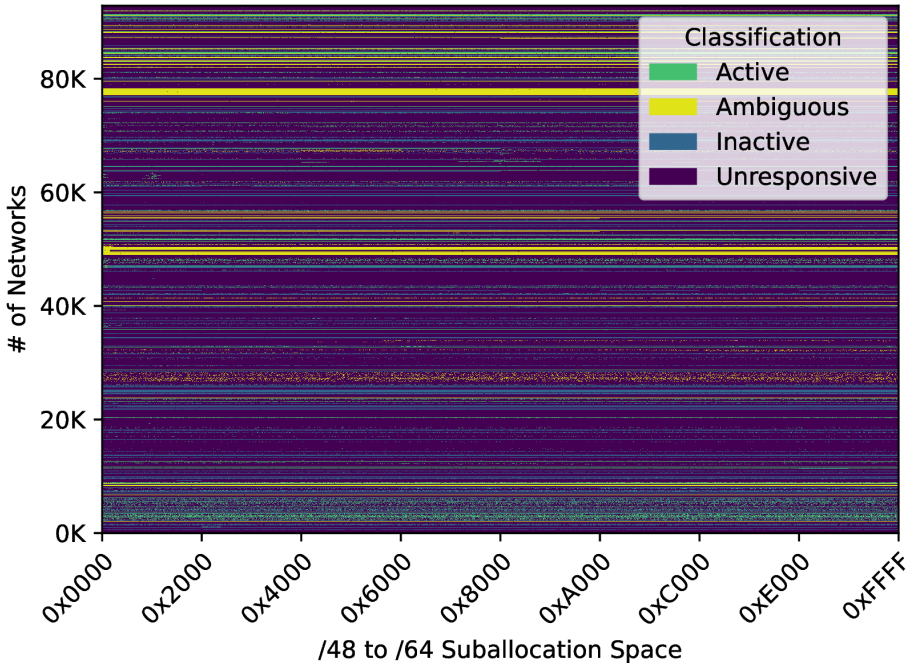
		labeled active			labeled inactive		
		Netw.	σ	%	Netw.	σ	%
active	ICMPv6	17,361	109	95.1%	471	11	4.6%
	TCP	14,522	112	93.7%	620	12	7.4%
	UDP	12,490	82	56.2%	3,687	35	32.0%
ambig.	ICMPv6	352	10	1.9%	1,645	12	15.9%
	TCP	566	10	3.7%	1,552	14	18.6%
	UDP	9,377	91	42.2%	1,455	7	12.6%
inactive	ICMPv6	537	13	2.9%	8,230	34	79.5%
	TCP	405	8	2.6%	6,191	26	74.0%
	UDP	337	12	1.5%	6,396	49	55.4%

NOTE: σ Standard deviation over five days.

True Negatives

universität wien

Result: /64 Prefixes in BGP announced /48s



38% of measured /48 networks remain silent

Measured /64s	6,085,410,816 (100%)
Responsive	1,368,371,825 (22.5%)
Unresponsive	4,717,038,991 (77.5%)

Responsive	/64s
Active	355,616,627 = **26%**
Ambiguous	209,970,342 = 15%
Inactive	802,784,856 = **59%**

At least 1 active /64 in 61% of responsive /48 networks

Only 15% of responsive /64s remain ambiguous

universität wien

Router Classification

1. Controlled Environment

Router Lab

2. Verification in the IPv6 Internet

SNMPv3

3. IPv6-wide Measurements

ZMap

Controlled Environment: Router Lab

Vendor Defaults | Kernel Defaults

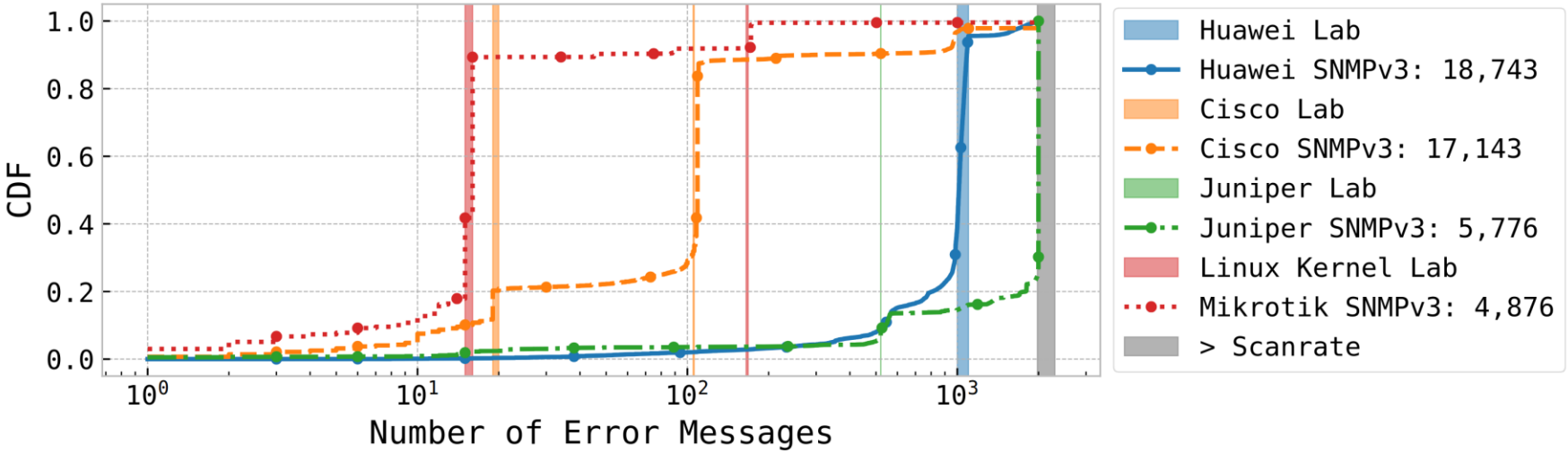
	Router OS	iTTL	Delay	Bucket Size			Refill Interval (σ)			Refill Size			# Error Messages			Per
		All	AU	TX	NR	AU	TX	NR	AU	TX	NR	AU	TX	NR	AU	Src
Diff AU/NR/TX	CiscoXRV9000	64	18	10	10	10	1,000	1,000	1,000	1	1	1	19	19	0★	
	CiscoIOS 15.9	64	3	10	10	10	~100	~100	3,800★	1	1	10	~105	~105	22★	
	CiscoCSR1000 17.03	64	3	10	10	10	~100	~100	3,000★	1	1	10	~105	~105	22★	
	Juniper 17.1	64	2	52	12	12	~1,000	10,000	10,000	52	12	12	~520◇	12	12	
	HPE VSR1000	64	3	∞	∞	★	∞	∞	★	∞	∞	★	∞	∞	★	
	Huawei NE40	64	3	100-200	8	/	1,000	1,000	/	100	8	/	1,000-1,100	88	/	
No diff for AU/NR/TX	Arista 4.28	64	3		∞			∞			∞			∞		
	VyOS 1.3	64	3		6			250*			1			45*		✓
	Mikrotik 6.48	64,255	3		6			1000			1			15		✓
	Mikrotik 7.7	64	3		6			250*			1			45*		✓
	OpenWRT 19.07	64	3		6			250			1			45*		✓
	OpenWRT 21.02	64	3		6			250*			1			45*		✓
	ArubaOS 10.09	64	3		6			250*			1			45*		✓
	Fortigate 7.2.0	255	3		6			10			1			1000		✓
	PfSense 2.6.0	64	3		100			1000			100			1000		

~ ... Refill interval is less stable / ... The response type is not returned by the RUT. ★ ...Affected by the Neighbor Discovery Process. * ... /48 destination prefix; for other prefix sizes see Table 7 ∞ ... RUT is either not rate-limited or > *scanrate* (tested up to 10K pps). ◇ ... Juniper's Neighbor Discovery for hop limit 0 packets causes a 2-second delay also for TX.

Kernels: Linux, Wind River Linux and FreeBSD.

universität wien

Verify: SNMPv3 Label Comparison

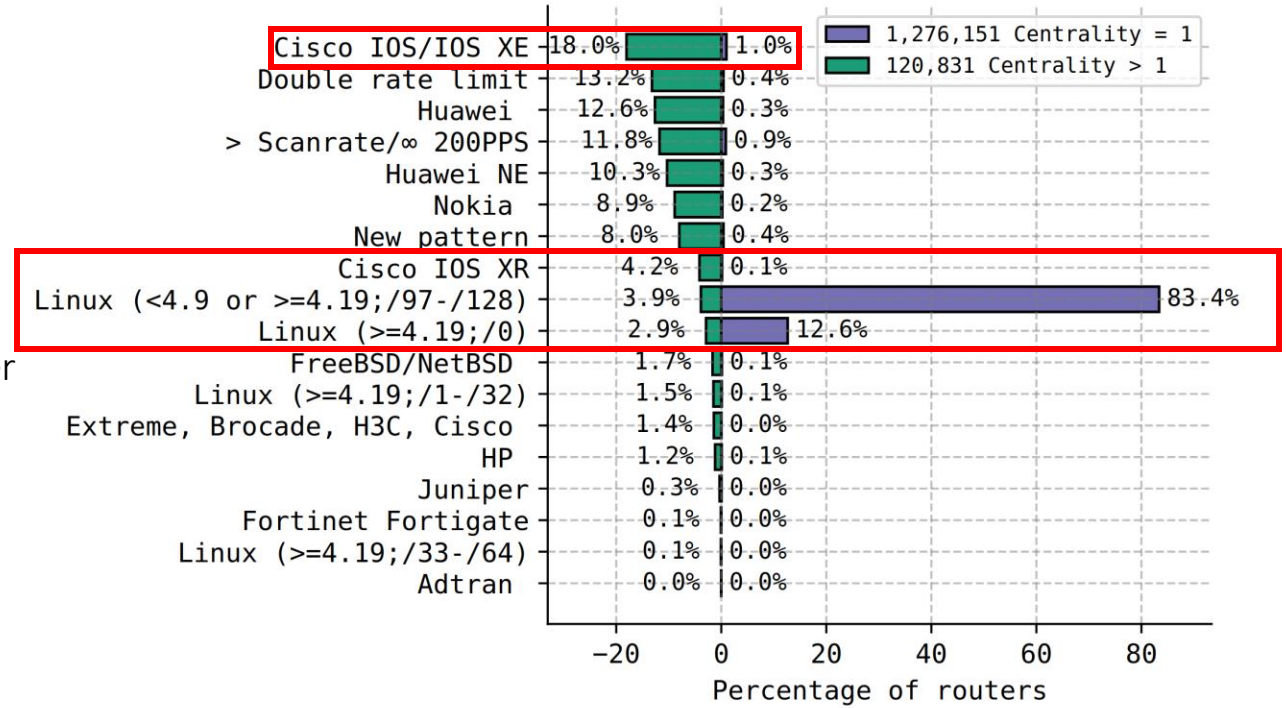


- Huawei labeled match lab default
- Cisco labeled match XRv and IOS lab defaults
- Majority of Juniper labeled is limited above measurement scanrate of 200pps
- Mikrotik matches Linux kernel defaults

universität wien

Result: Rate Limit Matching

- Routers on multiple paths (green), more **distinguishable** rate limits
  - E.g. Cisco (18% IOS, 4.2% XRv)
- Periphery (purple)
  - 83.4% Linux <4.9 or newer version with small dest. prefix sizes (less likely)
  - 12.6% ≥4.19 with default route



Conclusion IPv6 Reconnaissance

- IPv6 network classification based on:
  Active: $AU_{RTT \geq 1\,sec}$
  Inactive: RR, TX & $AU_{RTT<1sec}$

- TX indicates the **presence of routing loops**, further studied by related work
- Not applicable to every network (**38% remain silent**)
- Router & kernel fingerprints **unlikely to be disabled** (TX must be returned, harmonization unlikely)

Delivery Failures: Unintentional Active and Passive

Publication at IMC'25

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

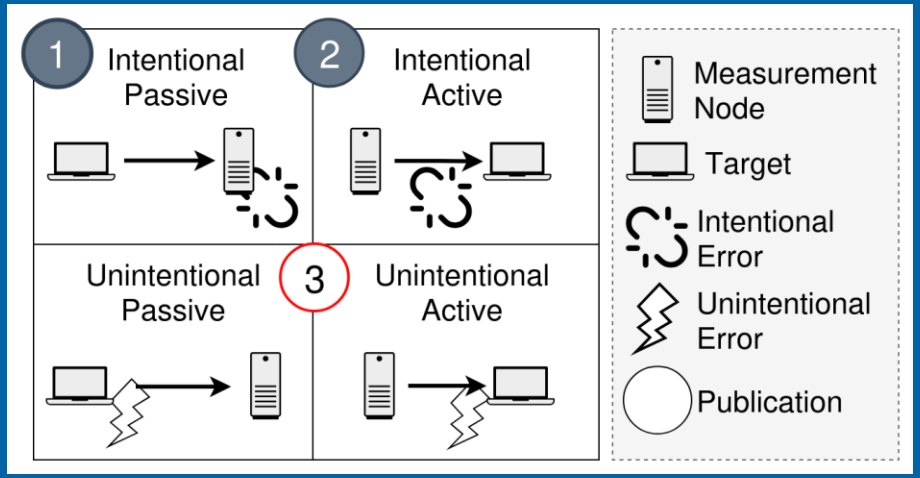
medium for accessing information, such as news and governmental advisories. Since the war in 2022, Internet connectivity in Ukraine has been repeatedly disrupted and has undergone continuous efforts of restoration.

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



Holzbauer F., Strobl S., Ullrich J., Tracking Internet Disruptions in Ukraine: Insights from Three Years of Active Full Block Scans, Internet Measurement Conference (IMC), 2025. CORE: A

universität wien

Tracking the War in Ukraine

Seismic Monitoring

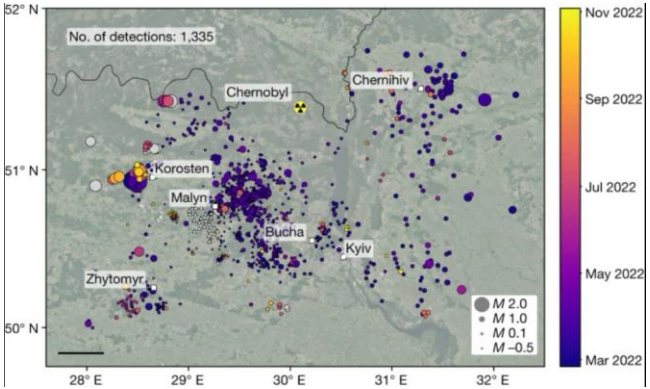


Figure 1: Seismic data obtained from Malyn AKASG array

Radius: 300 km × 222 km

Satellite Imagery

Figure 2: Satellite Image of Azovstal steel works - March 2022

Temporal resolution, weather, image quality, costs

Internet as a Sensor

Active

IODA
INTERNET OUTAGE DETECTION AND ANALYSIS

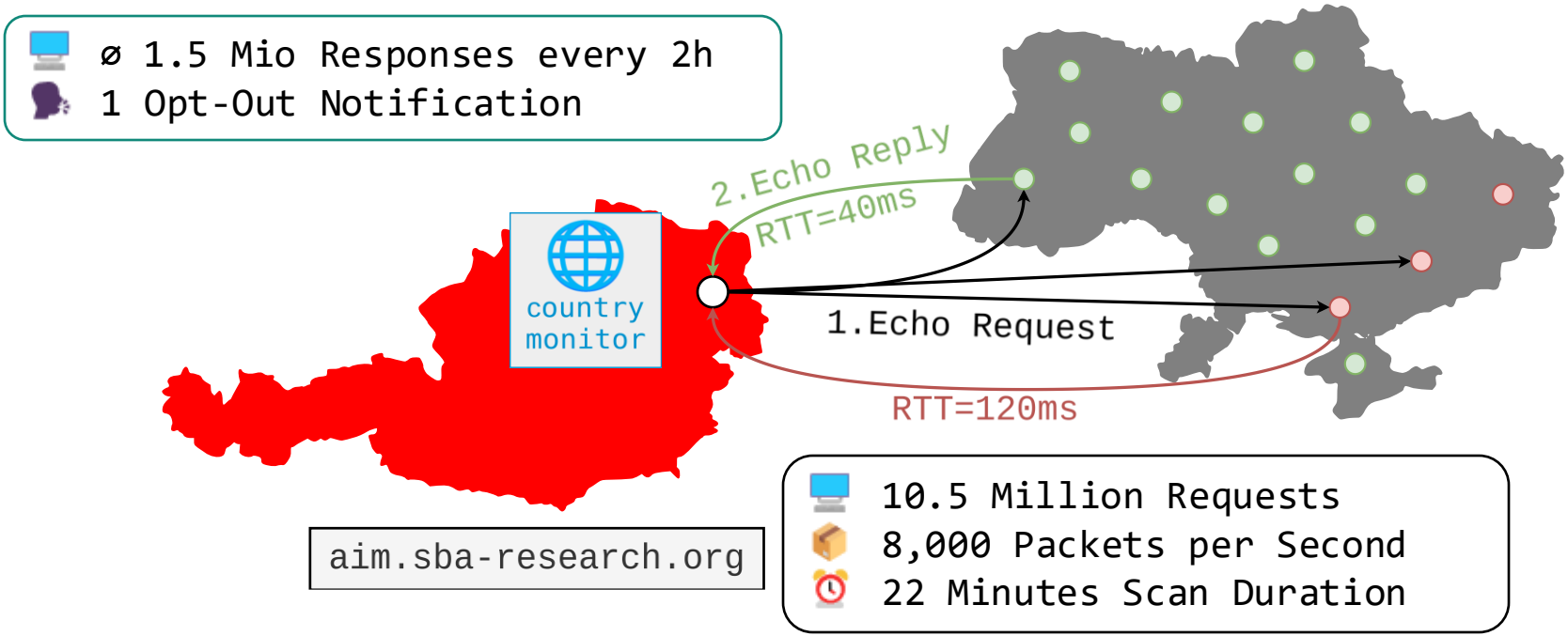
alpha strike labs

Passive

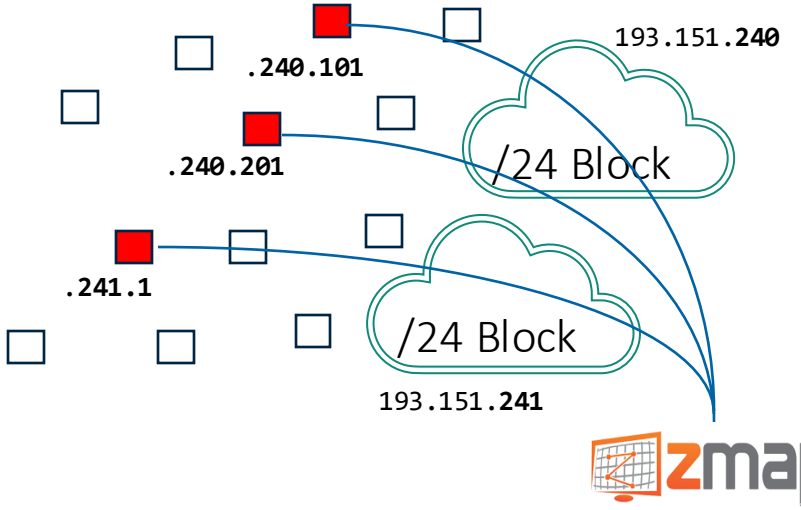
CLOUDFLARE

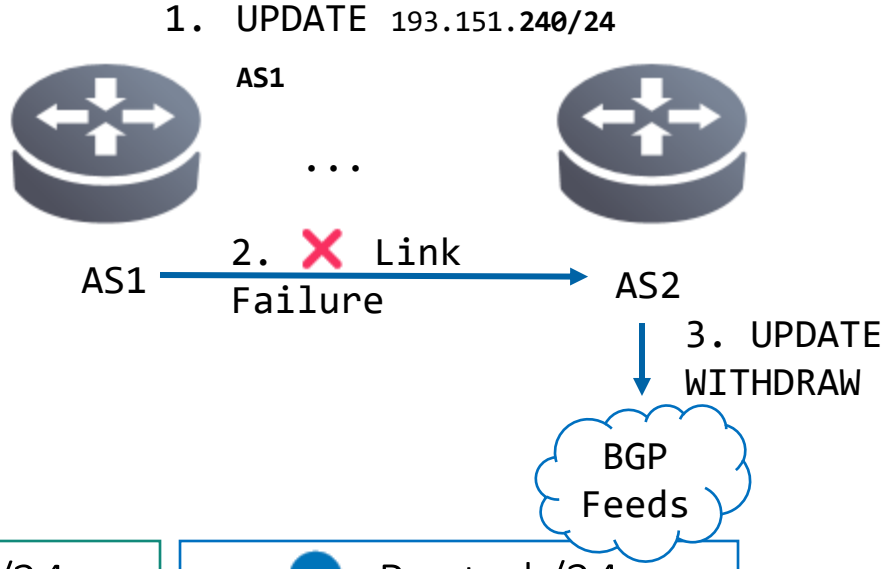
Privileged position, misses silent devices

From Austria to Ukraine and back



From Ping to Outage Signal





zmap

Responsive IPs | Active /24s | Routed /24s

⚠ Outage = current value < X% of moving average of previous week

Dataset Depth: Insights into smaller ISPs

Total: 1743 ASes Ukraine
Our Coverage: 1674 (96%)
IODA: 333 (19%)
Why: Signal Stability

/24 Block

193.151.**240**

AS25482 -> 4 routed /24s

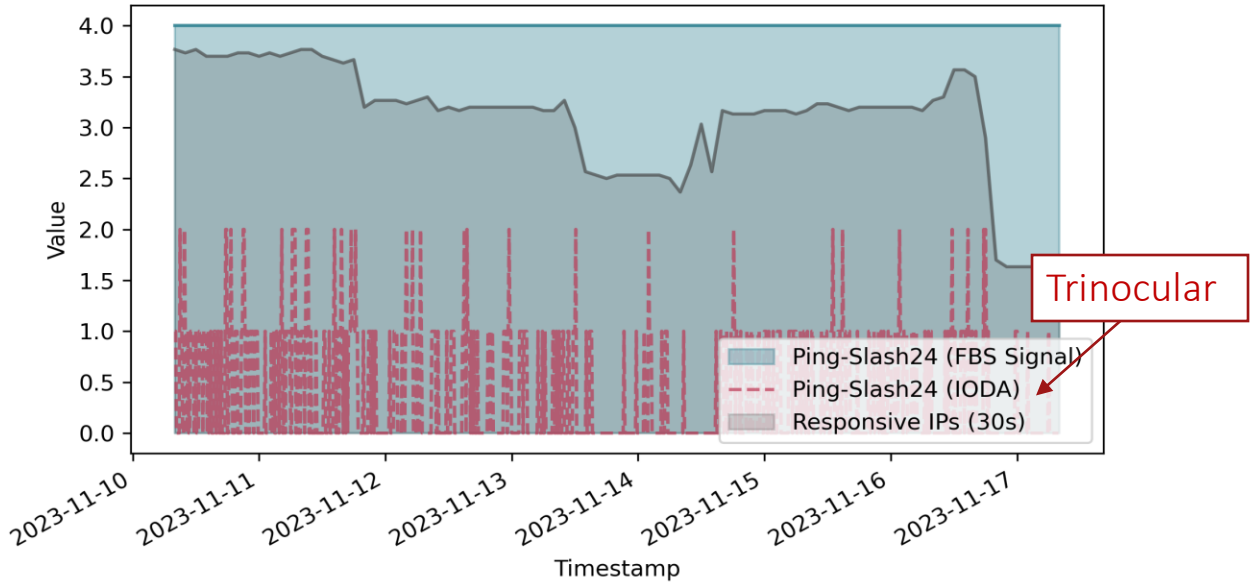
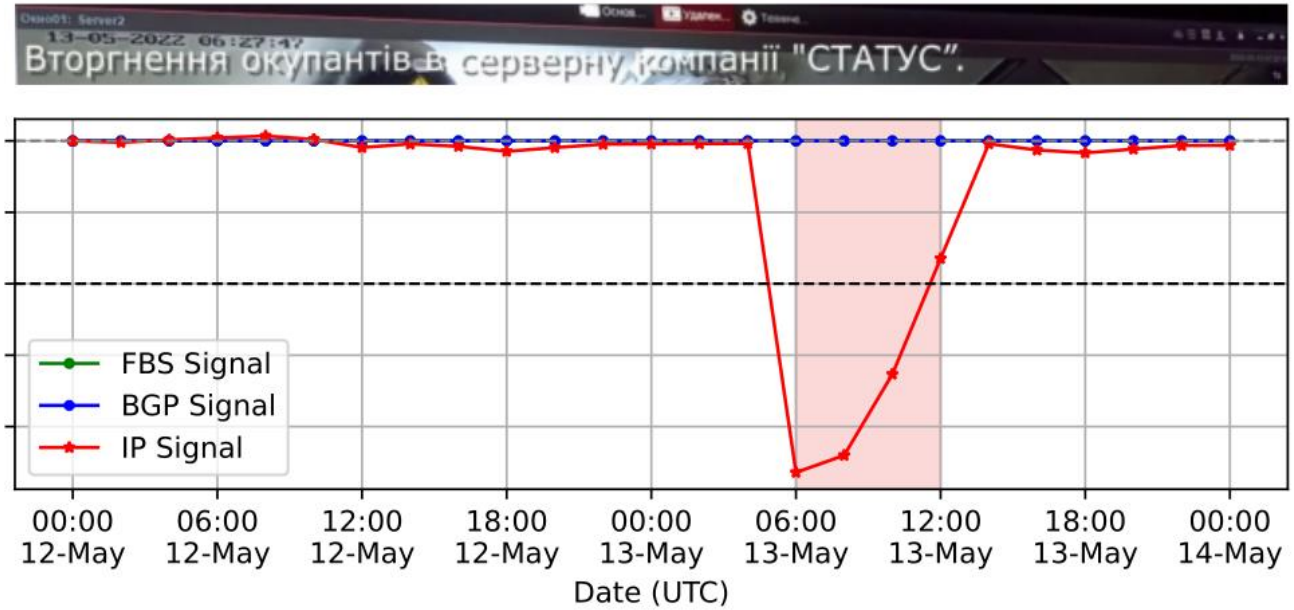


Figure: Raw signals for AS 25482 (STATUS) recorded November 2023.

Dataset Depth: 13.05.2022 "STATUS" ISP



CountryMonitor: Decline in responsive IPs for ASN 25482 (STATUS ISP) at the same time as the incident

Incident: Russian soldiers search STATUS Office

universität wien

Dataset Breadth: Internet Disruptions per Oblast

1. Intense attacks on the power grid -> **partial outages** through **IPS signal**
   - Infrastructure types (core vs edge)

2. Full block outages (FBS) more **frequent in frontline regions**

3. **Only part** of the outages are passively **visible in BGP**

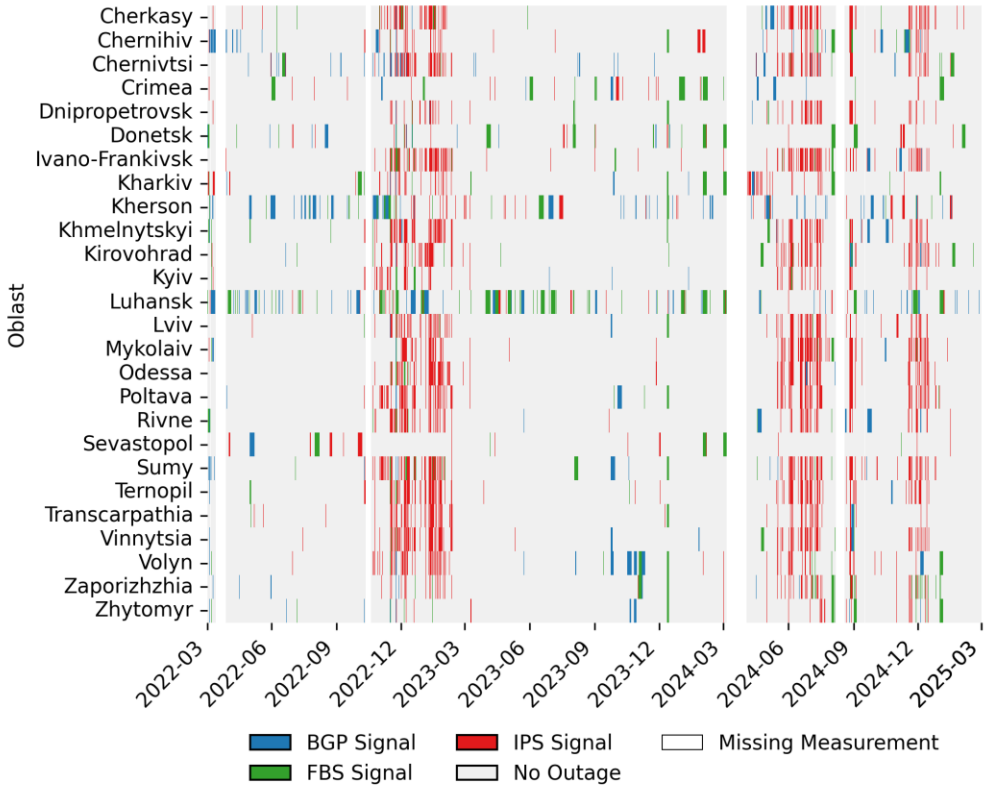


Figure: Outages detected by each signal type across oblasts.

Dataset Breadth: Alignment with Electricity Outages in Non-Frontline Regions

1951 HOURS
with electricity outages in 2024

Avg. 686 HOURS
Max. 2822 HOURS
with Internet outages in 2024

Pearson r=0.725
overlap of days

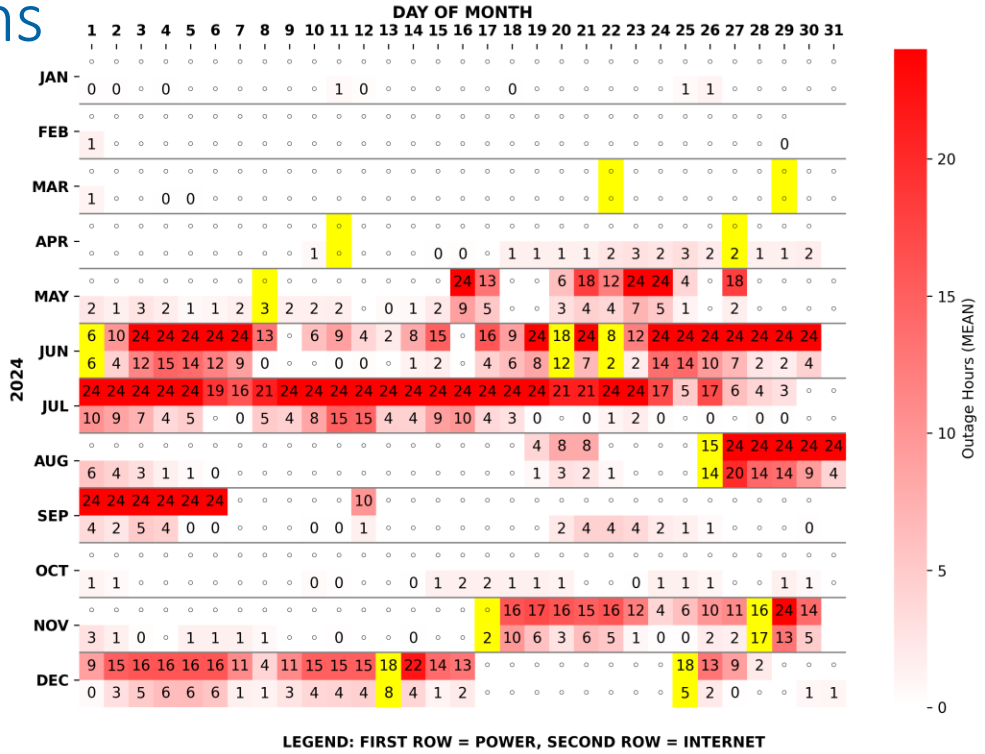


Figure: Hours affected by power and Internet outages in 2024.

universität wien

CountryMonitor Takeaways

	Singla et al.	Klick et al.	IODA	CountryMonitor
Protocols	Modbus, DNP3	60+	ICMP	ICMP
Signal	IP based	IP based	Block based (Sampling)	Block based (no Sampling)
Interval	24 Hours	4 Hours	10 Minutes	2 Hours
War Coverage	6 Months 2022	Until March 2023	Since 2022	Since 2022
Outage Location	IP Geolocation	Static IPs	IP Geolocation	Regional Classification

universität wien

Delivery Failures: Takeaways

- First restrictions of **plaintext** email delivery
- **Opportunistic** encryption to be tackled next
- **Domain specific** IPv6 adoption (Email vs DNS)
- Testbed **helps** operators and users to **improve**

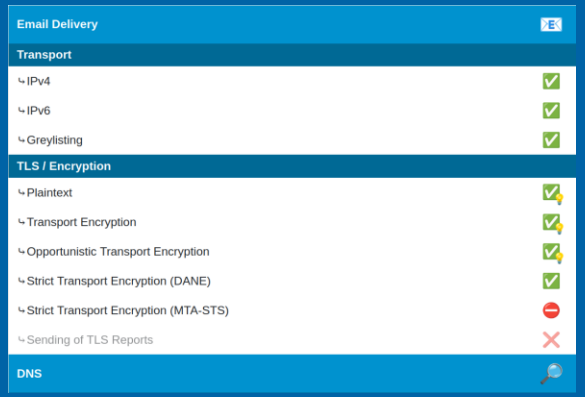
- Combine **IPv6 recon. with outage detection** (counter IPv4 churn, provider equipment)
- Surprising IPv6 **side effects:** SPF fixes, routing loops, Russia failed to censor IPv6

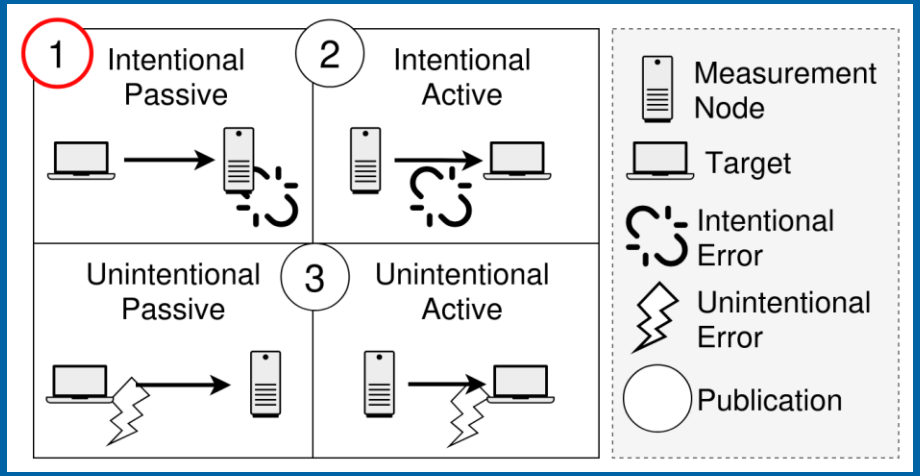
- Different outage signals, different **outage types**
  - Partial outages -> during power cuts
  - Long lasting outages and traffic rerouting -> BGP and latency changes
- Dataset provides insights in **Internet resilience** (repairs, redundancy)

universität wien

Conclusion

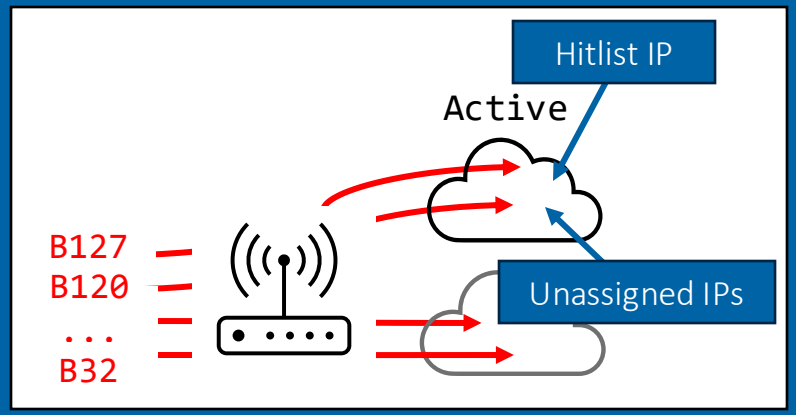
1. email-security-scans.org

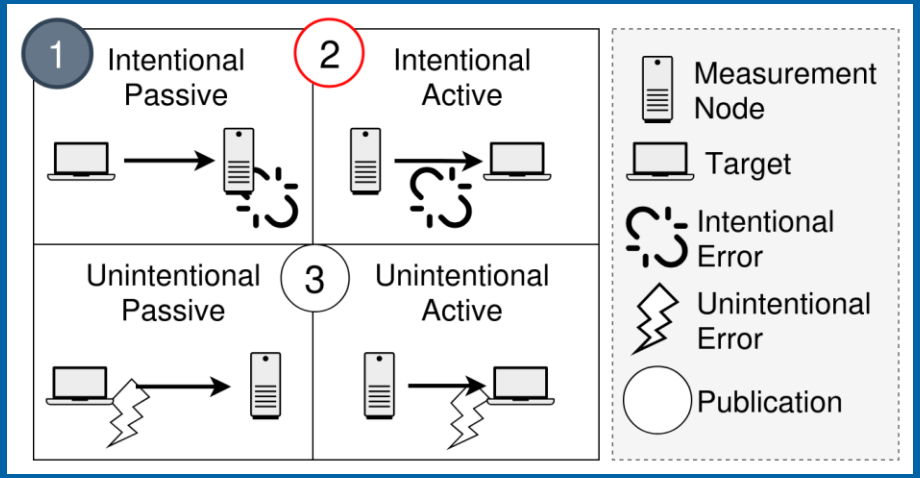




Conclusion

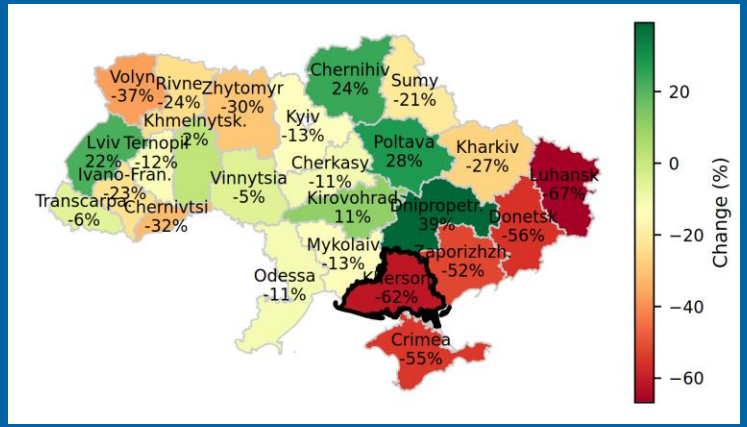
2. Active IPv6 Measurements

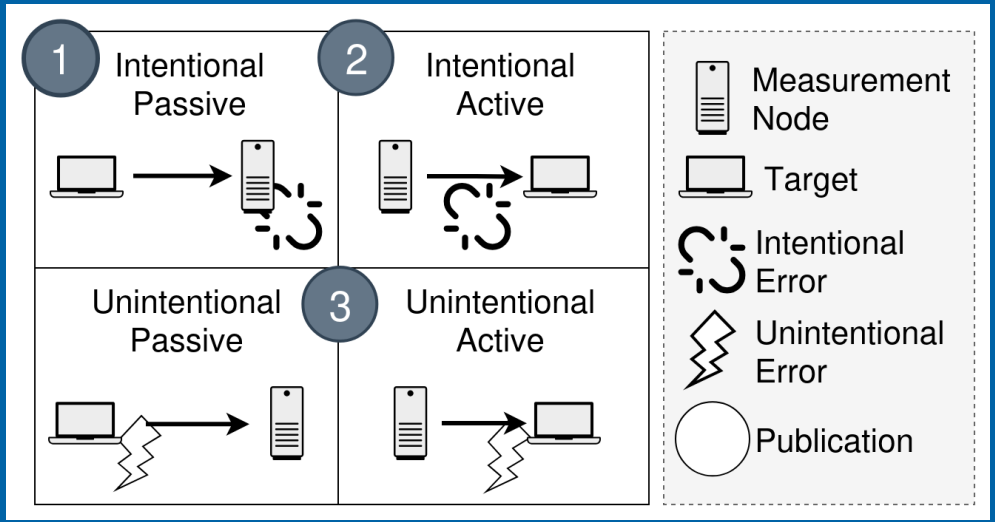




Conclusion

3. CountryMonitor



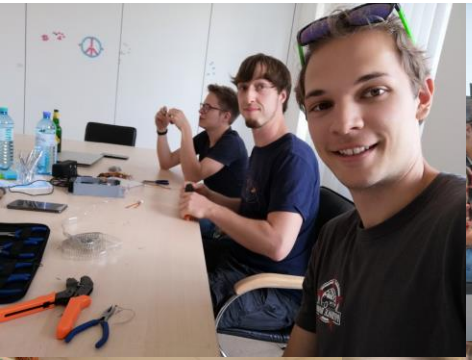


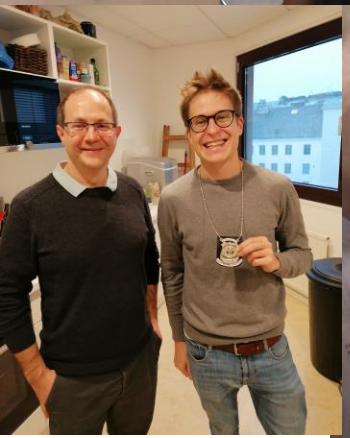
Destination Reached – Reactions/Questions?

… please set the type and code accordingly! ;)

> Thanks for attending!

Acknowledgements

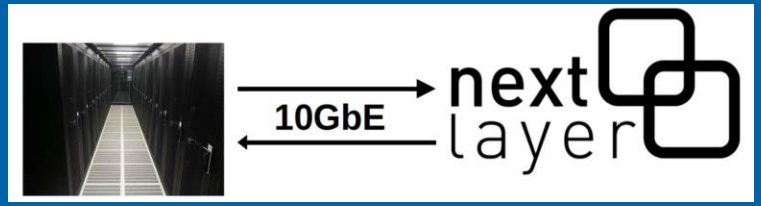




universität wien

Research Methodology

- Empirical research with custom data collection through Internet measurements



- The process:

RFC Analysis	Hypotheses	Measurement Design	Validation	Evaluation
RFC4443	An error message of type Dest. Unreach. Code Addr. Unreach **should** be returned when sending a request to an unassigned IPv6 address.	Router testbed with multiple vendors that forward traffic to an unassigned IPv6 address	Verification with IPv6 networks that are known to be active	Do real world IPv6 networks behave as in the controlled environment?

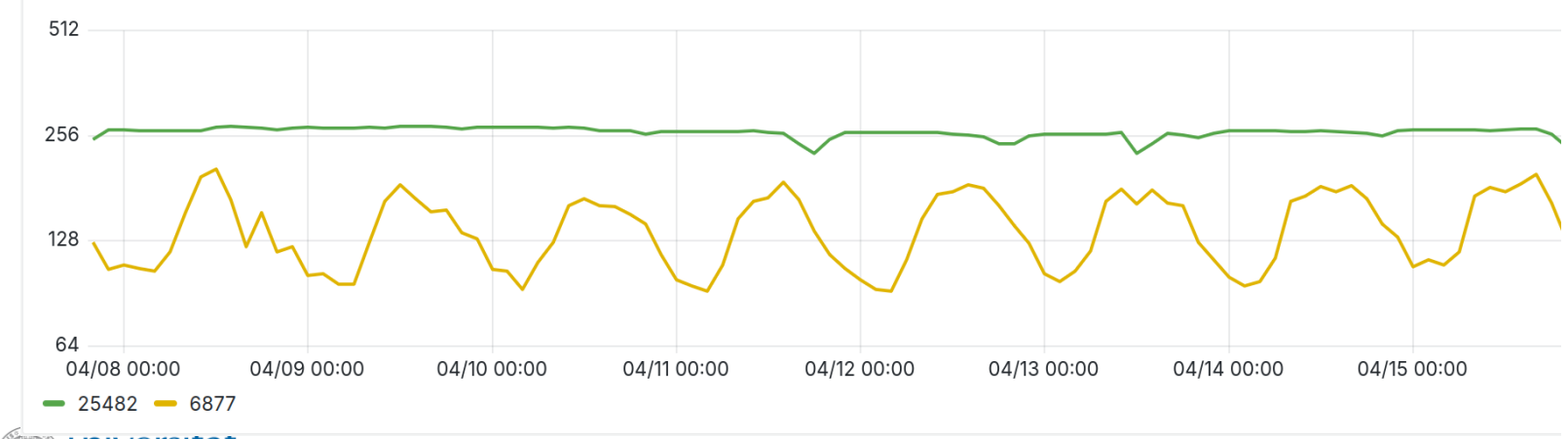
universität wien

CountryMonitor – Outlook

Extending beyond Ukraine

The signal primarily consists of provider equipment → NAT!

- Better protected against outages than home routers
- Expansion of scans to IPv6
- Methodology for collecting home router addresses



CountryMonitor: GREEN - Regional Provider Status vs. YELLOW Ukrtelecom in Kherson (6 AM - 8 PM Cycles)

Future Work

- **New protocols** to add to email-security-scans.org: ARC, inbound DANE, MTA-STS, URL rewriting, ..
- **Outage detection in IPv6**
  - The signal primarily consists of provider equipment → NAT!
  - Better protected against outages than home routers
  - Destination Reachable = Methodology for collecting home router addresses
- **Dynamic thresholds** for outage detection instead of static ones.
- Extend CountryMonitor **outside Ukraine**
- Test **regional classification** (IP to location trends) in other countries
- Explore **Neighbor Discovery security** for active IPv6 networks

Limitations

- Vantage Points

  -> limited in geographic diversity and number

- Protocols investigated

  -> Delivery failures for other protocols were not investigated

  Publication specific:

  - Email: after initial study: 60% of tests from Gmail/Microsoft

  - IPv6: ICMPv6 error message defaults dynamic

  - Internet disruptions: Anomaly origin hard to determine from measurements alone.

Data Collection:

- Email: Pause during development of artifact in 2022, DNSSEC target failed after initial study
- IPv6: Limited period in 2023
- Internet Outages: Interruptions when our vantage point went offline/maintenance.
  - 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

universität wien

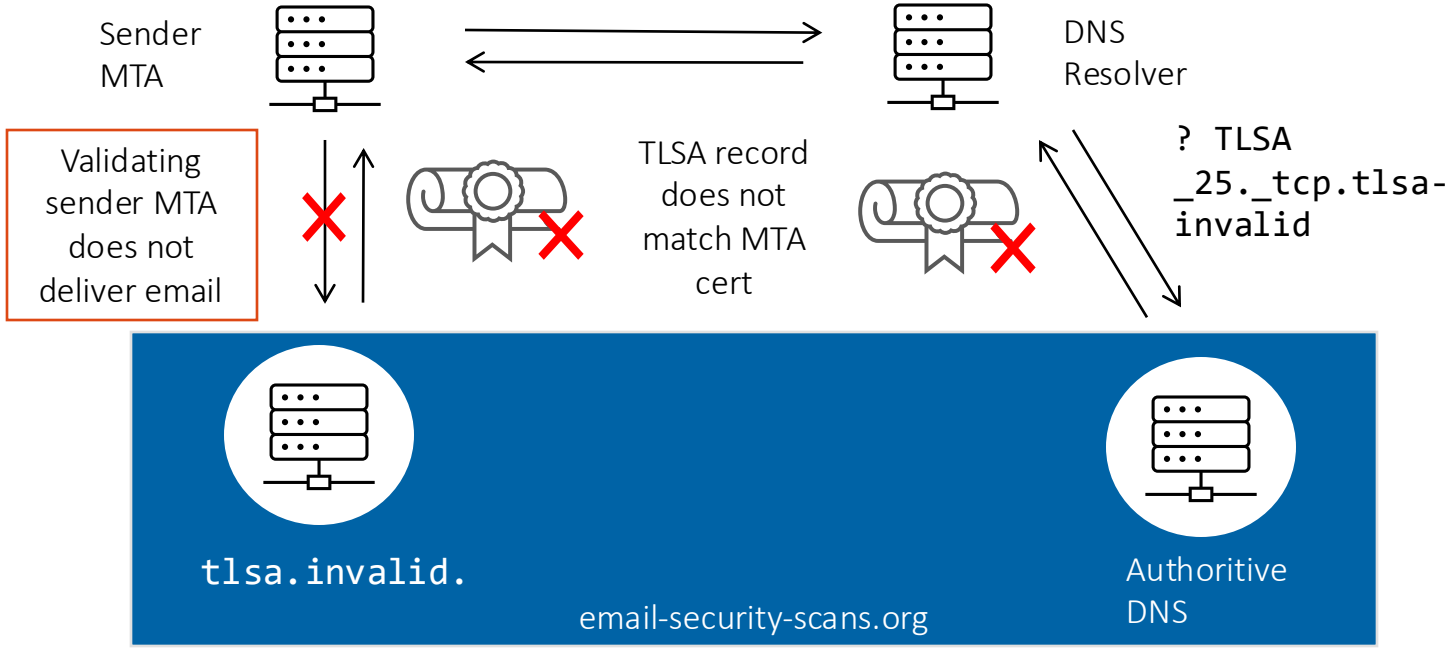
Backup Email

Internet.nl


Email test: univie.ac.at
75%
Reachable via modern internet address (IPv6)
All domain names signed (DNSSEC)
Not all authenticity marks against email phishing (DMARC, DKIM and SPF)
Mail server connection not or insufficiently secured (STARTTLS and DANE)
Unauthorised route announcement (RPKI)

Intentional Passive - Email Testbed

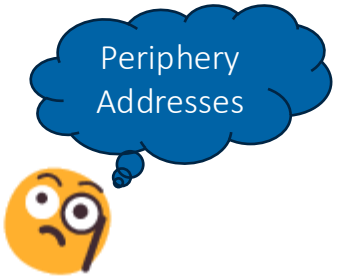
- Example test with target: `mail-tlsa-invalid.(measurement...)`



universität wien

universität wien

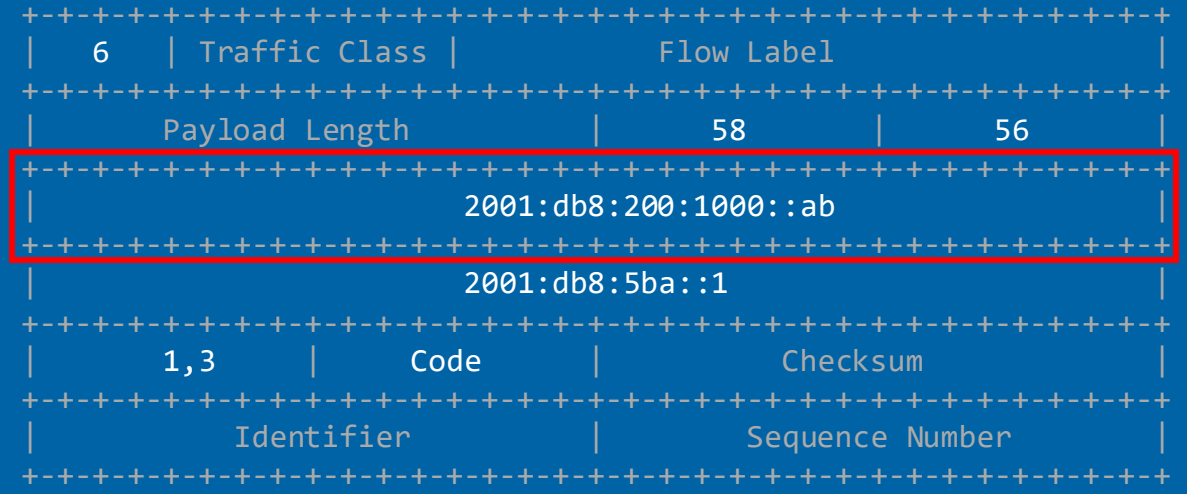
Backup IPv6



Error Messages in Measurements

- Edgy (Rye, 2020)
  - 64.8M Last-Hop Routers
- XMap (Li, 2021)
  - 52M Routers + User Equipment (15 ISP ranges)

- Periphery can include your:
  - Home Router
  - Smartphone

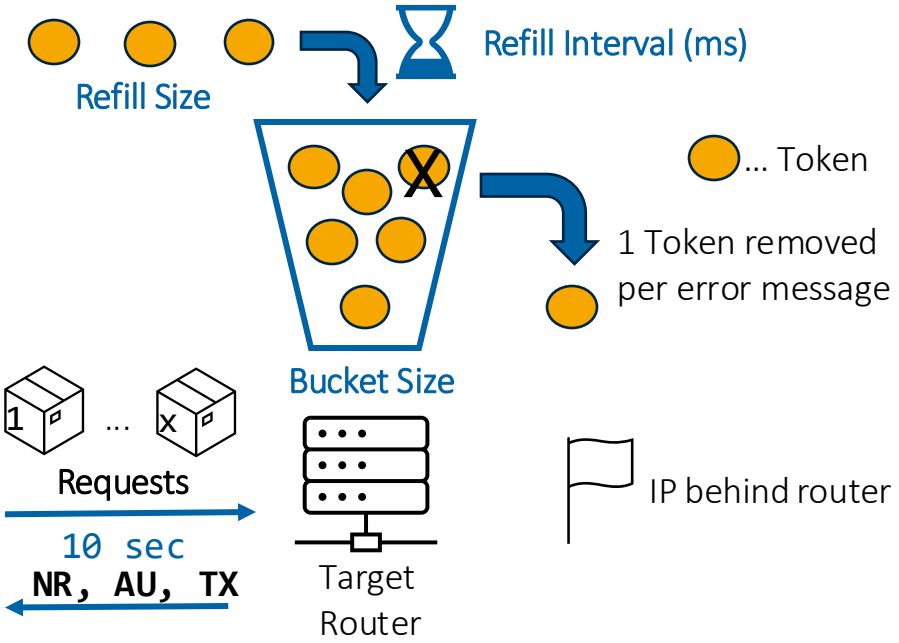


ICMPv6 Error Message

Methods Overview

- Origination of ICMPv6 error messages **must be** rate limited
- Measure & detect **rate limits** that are **unique to vendors**

1. Controlled Environment



NR(10) … Total error messages over timespan of 10 seconds
T1, T2, T10 Number of error messages during 1st, 2nd, .. 10th second

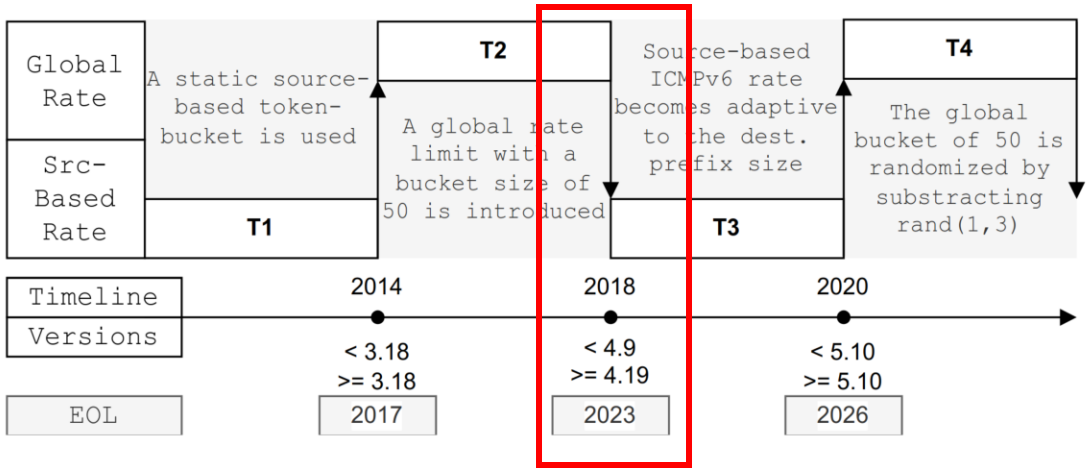
Result I: Changes in the Kernel

	Kernel Version	Release	IPv4	IPv6
Linux	2.6.26-1-2	2008	15	15
	3.16.0-4-6	2014	15	15
	4.9.0-3-13	2016	15	15
	4.19.0-5-21	2018	15	45
	5.10.0-8-22	2020	15	45
	6.1.0-9	2022	15	45
Freebsd	11.0	2016	2000	1000
Netbsd	8.2	2020	1000	1000

- Number of error messages over 10 seconds
- Static and dynamic testing of the Linux kernel shows a change for IPv6 in kernel version 4.

Three rate-limiting changes over time:

1. Introduction of global rate
2. **Peer-based becomes adaptive to dest. prefix**
3. Global bucket is randomized



Methods Overview

2. Verification in the IPv6 Internet

- Our Goal:

  1) Validate collected defaults in the Internet

  2) Extend defaults with new rate-limits for which the vendor is known (see Paper)

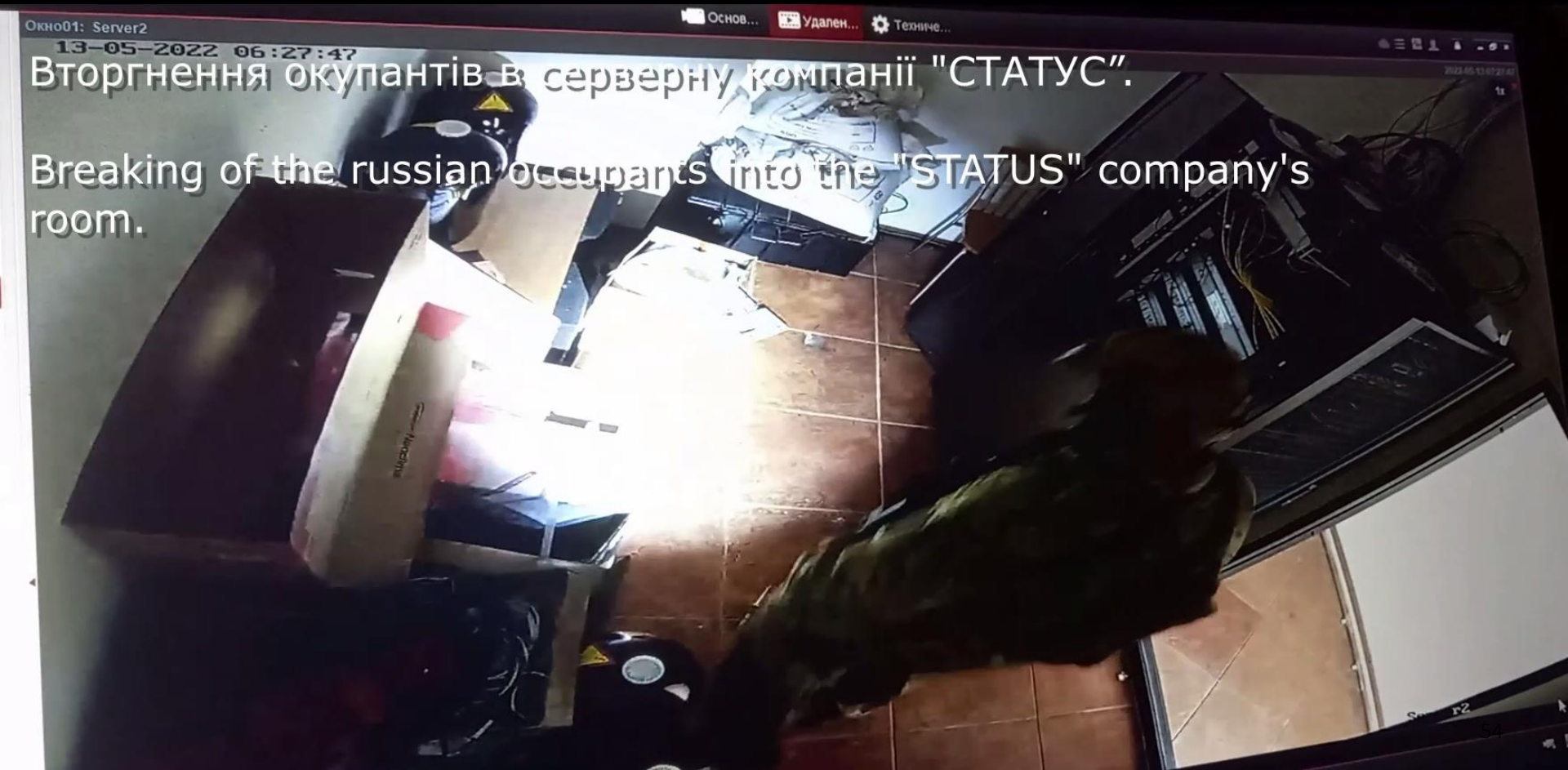
- Data Source:
  - Extract SNMPv3 vendor labels for **476K IPv6** routers (Albakour, 2021)
  - **50,952** match our tracerouting data, for which we can collect rate limit parameters
    - requires:  destination behind router, hop limit

universität wien

universität wien

Backup Ukraine

13.05.2022



Вторгнення окупантів в серверну компанії "СТАТУС".

Breaking of the russian occupants into the "STATUS" company's room.

#4 Regional classification detects long-term trends in geolocation.

Challenge:

Assign outages to a region in Ukraine

Regional Classification: Only consider /24s that have more than *M* addresses in the target region for more than *T_perc* of routed months.

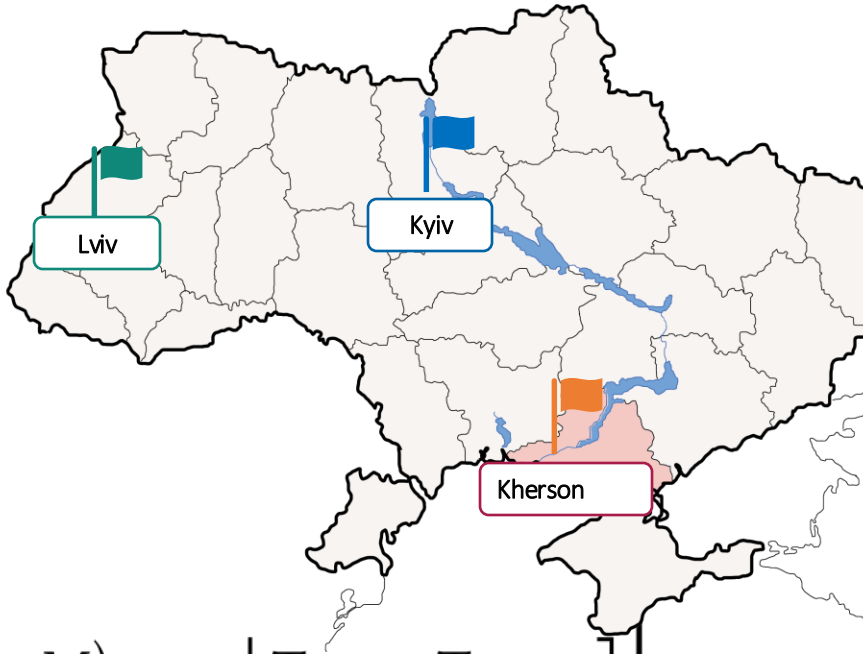
`In the paper: M = T_perc = 70%`

Timestamp	/24	
2022-03-02 10:00	193.151.240	✅
2022-03-02 12:00	193.151.240	❌
2022-03-02 14:00	193.151.240	✅

universität wien

Solution: Regional Classification

- Goal: Identify /24s representative for a region, e.g. Kherson



Regional Classification

st(e) … Regional IPs / 256 (or All IPs of AS)
M … Threshold Share of IPs (0-1): 70%
Trouted … Number of routed months
Tperc … Share of Months (0-1): 70%

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

#4 Regional classification detects long-term trends in geolocation.

Class	Kherson		
	ASNs	*IPs*	*/24s*
Total	118	73.8K	512
Regional	**13**	8.3K	33
Non-Regional	40	65K	465
Target Set	**34**	**41.7K**	**168**

Kherson

1. Identifies 32% of blocks for which outages are representative of the Kherson region
2. Target set serves as input to outage detection.

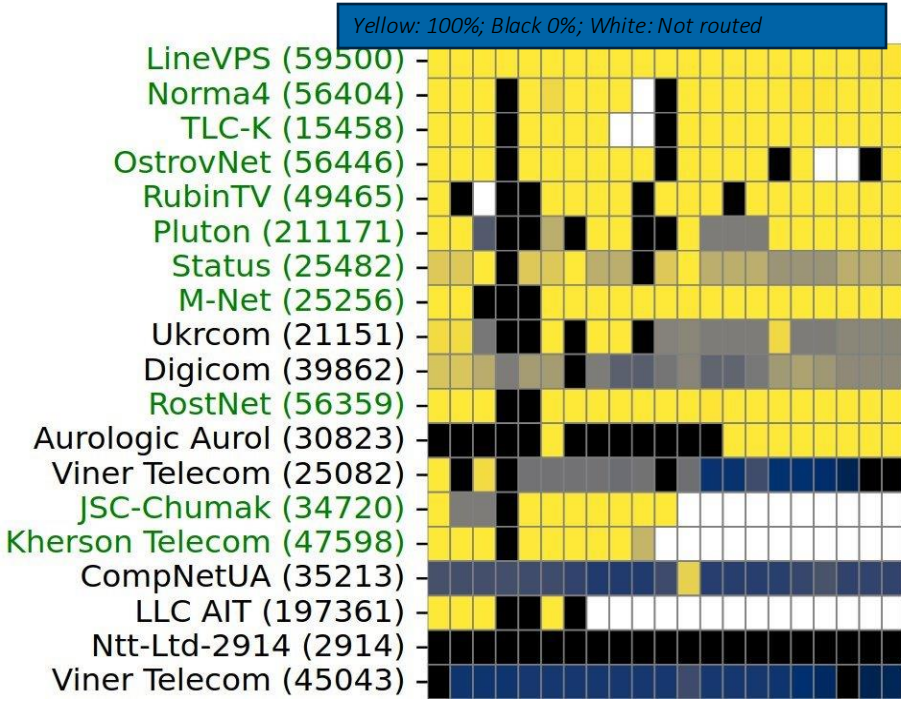


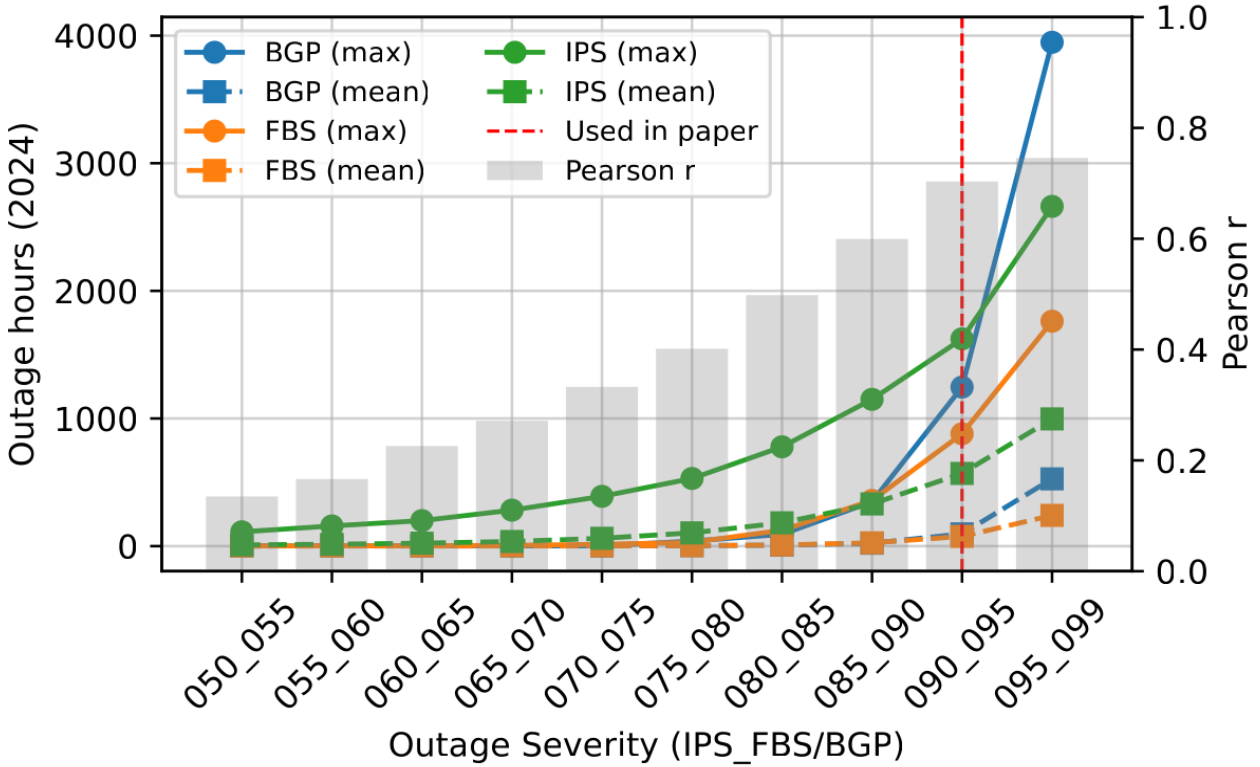
Figure 4: Regional share of IPs in Kherson.

Parameters & Threshold Sensitivity/Severity

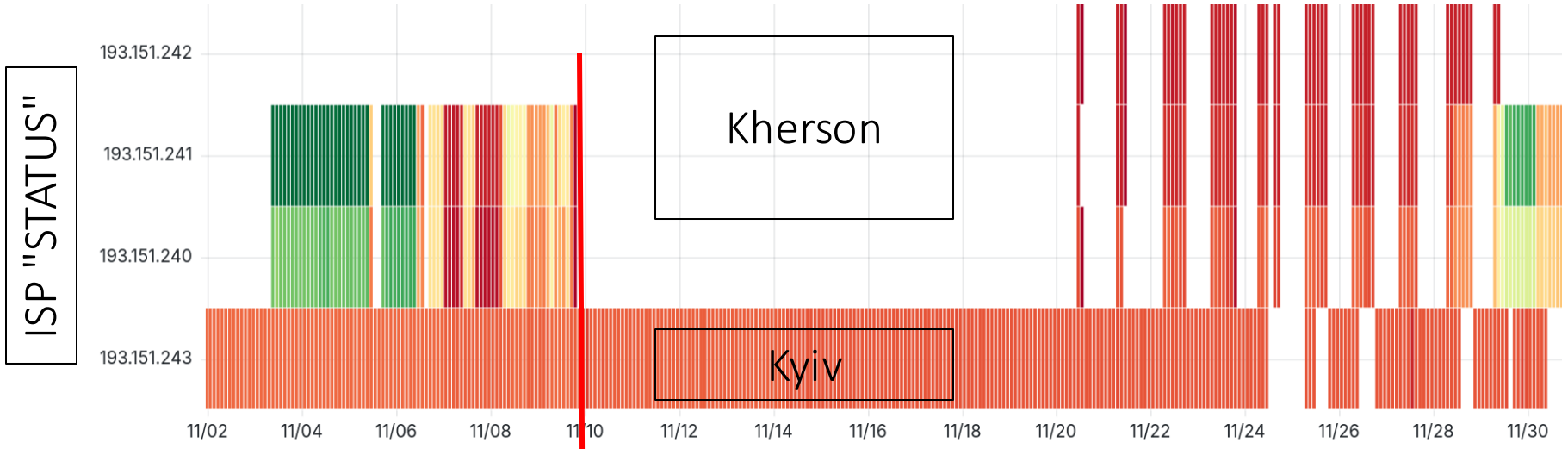
Level	BGP ★	FBS ■	IPS ▲
AS	< 95%	< 80% (if IPS < 95%)	< 80%
Regional	< 95%	< 95% (if IPS < 95%)	< 90%

Solution: Baltra – ISP Availability Sensing (2019)
Filter maintenance activity > additionally responsive IPs have to go down by 5% or more

Parameters & Threshold Sensitivity/Severity



Nov/Dec, 2022: Kherson City runs on Generators



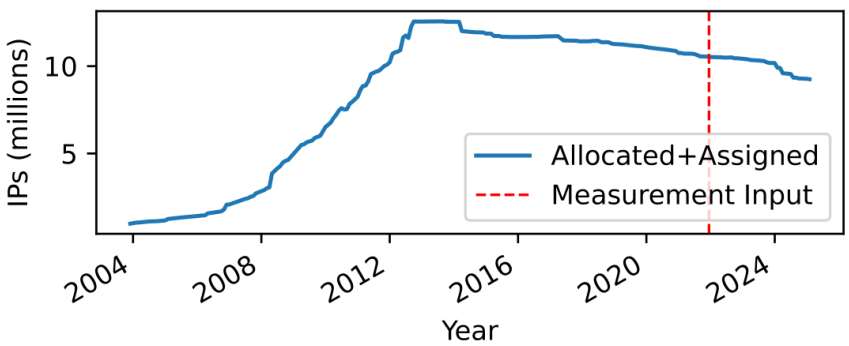
Russian Troops destroy critical infrastructure (TV Tower, Heat/Power Plant during retreat)

Daily Cycles
START: 08:00
END: 18:00

What is the size of the Ukrainian IPv4 address space?

RIPE Allocations

Might not always reflect actual usage!



- 3,085 IPv4 ranges (~10.5M IPs) in 2022; trend declining
  - 98% still exist in 2025
    - 87% allocated to Ukraine
    - 13% changed country codes
    - one-third to Russia
      - Still valid measurement targets

IP Geolocation

- Leased Prefixes?
  - 3.3% of delegated IPs located outside the country
    - Included in our measurements ✅
    - Not valuable measurement targets?
  - Reverse case: 7.4% of IPs locate to Ukraine but delegated to other countries
    - Not included in our measurements ❌

#5 Internet disruptions in Ukraine peaked during winter 2022/23 and throughout 2024.

1. Intense attacks on the power grid -> partial outages through IPS signal
   - Infrastructure types (core vs edge)

2. Full block outages (FBS) more frequent in frontline regions

3. Only part of the outages are passively visible in BGP

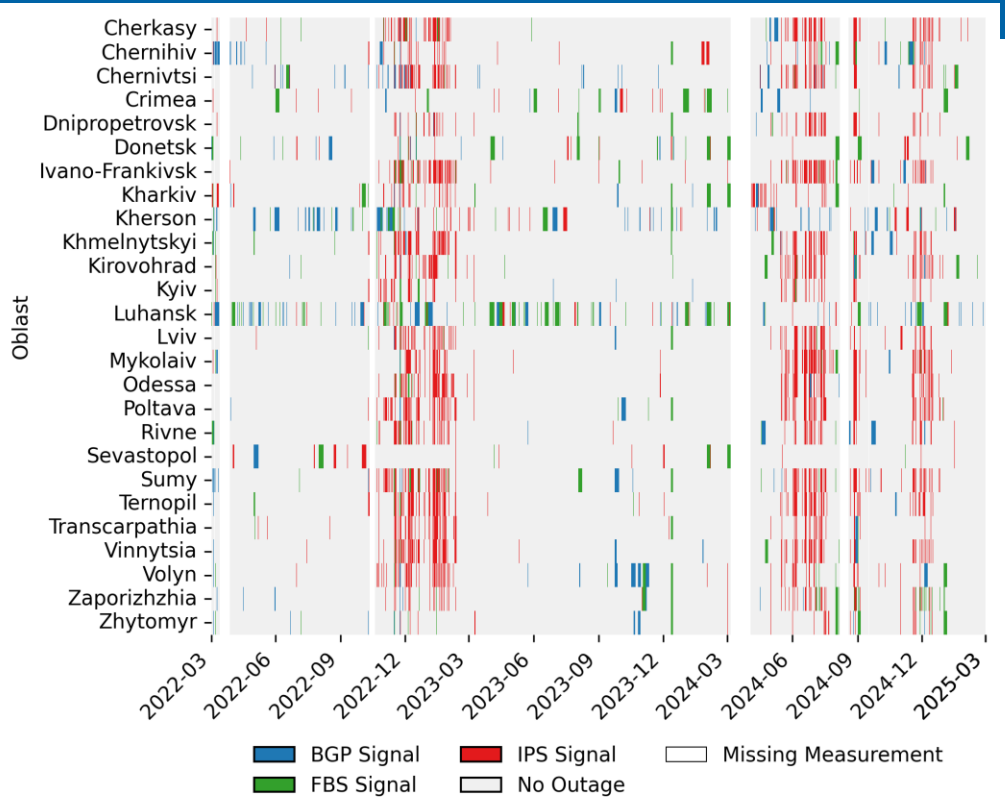


Figure 5: Outages detected by each signal type across oblasts.

universität wien

#7 Strong correlation of days with outages & power cuts in non-frontline regions.

1951 HOURS
with electricity outages in 2024

Avg. 686 HOURS
Max. 2822 HOURS
with Internet outages in 2024

Pearson r=0.725
overlap of days

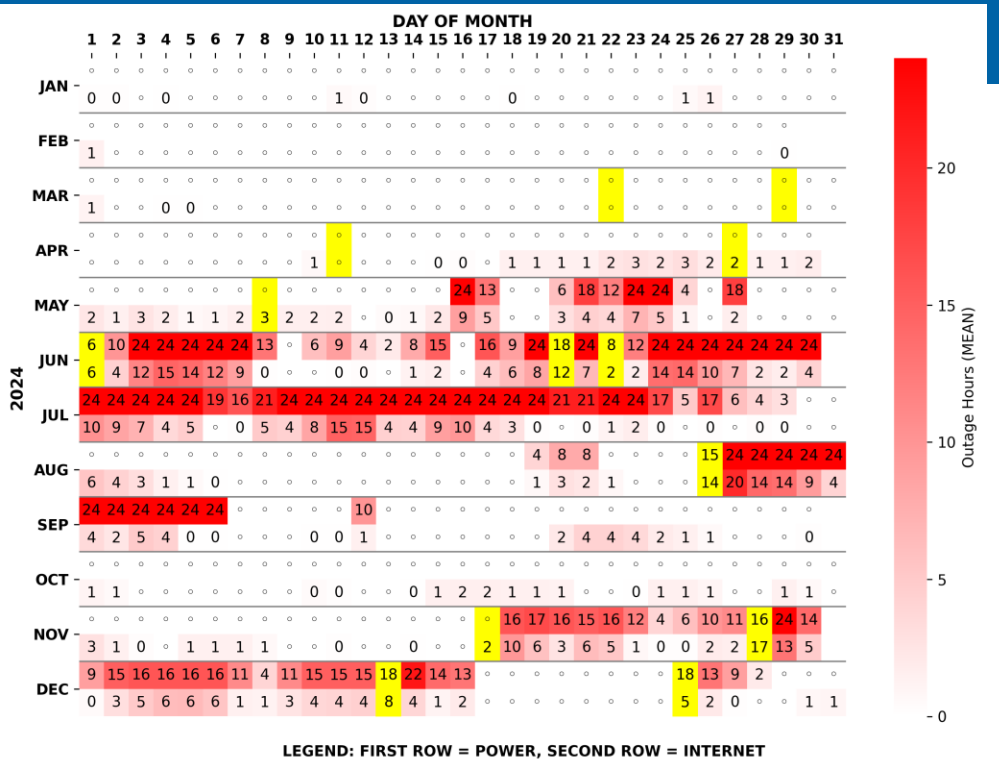


Figure 8: Hours affected by power and Internet outages in 2024.

#BONUS Dataset provides insights into smaller regional providers in Kherson.

Damage to Mykolaiv cable
> multi day outage in Kherson (May 1 to May 4)

Rerouting over Russian upstreams during summer
> Short outages for regional operators; then routed over Miranda
> Non-regionals often disconnected

Kakhovka dam impacts ISPs in flooded areas

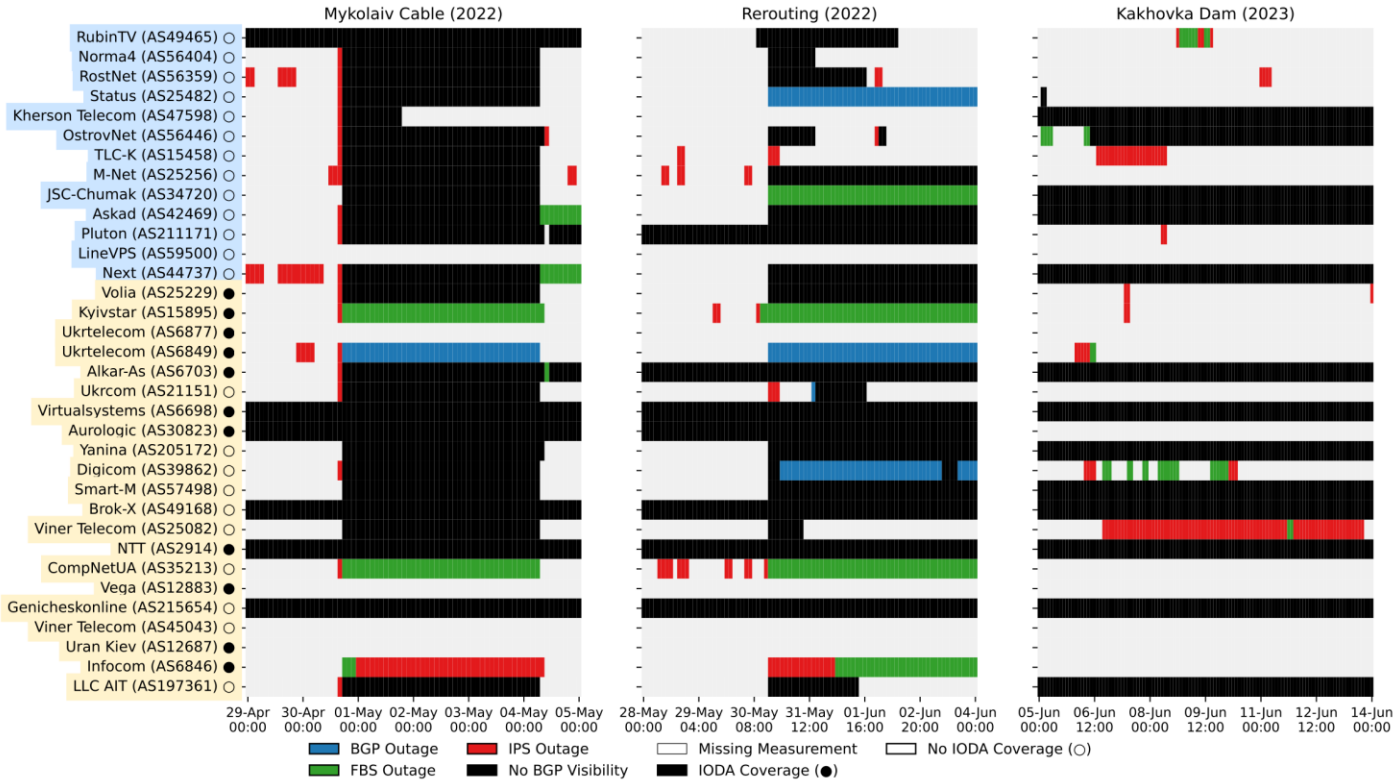


Figure 9: Three events with significant impact on ISPs in frontline region Kherson.

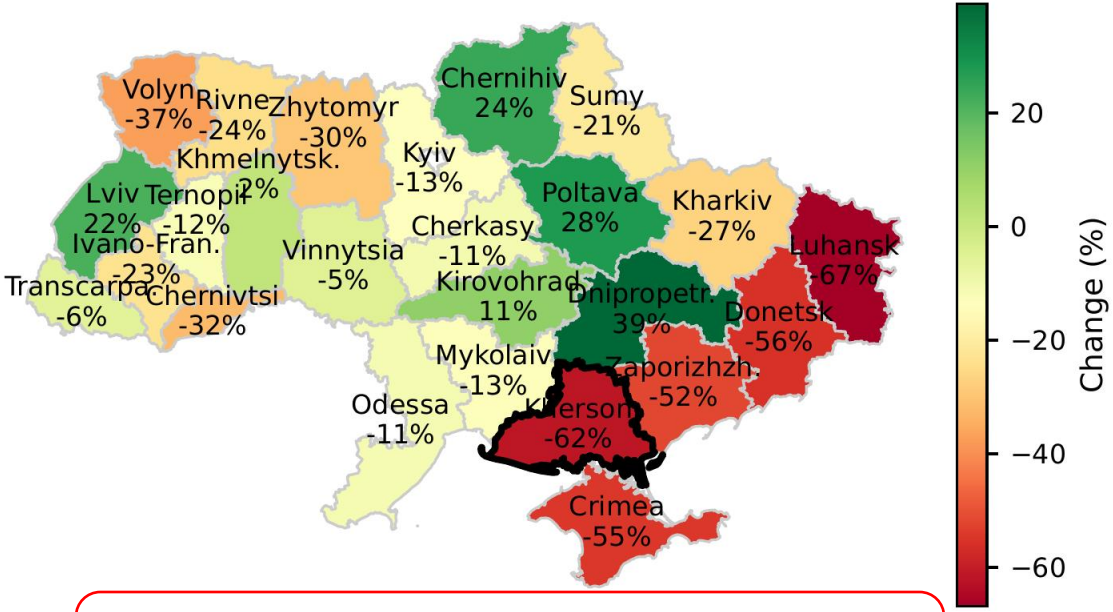
Challenge: Regional Attribution of Outages

60% between Oblasts

`Ukrtelecom, Kyivstar, Vodafone, Vega`

40% to other Countries (1.5M IPs)

33% amazon

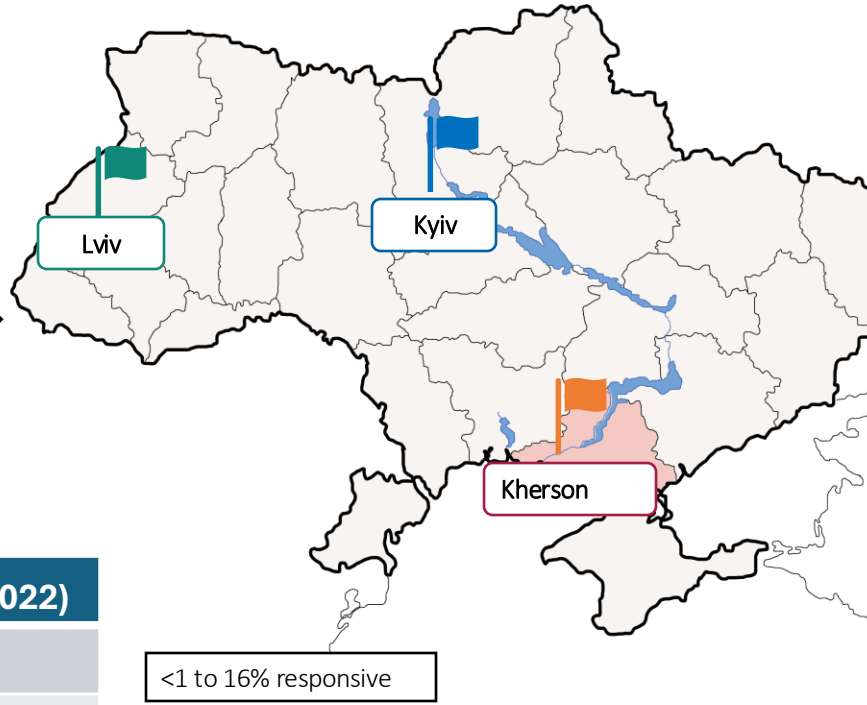


IP Churn – Comparing 2022 with 2025
3.7M IPs affected

Easy Solution: Ctrl + D National Mobile Operators

Kyivstar 🥺

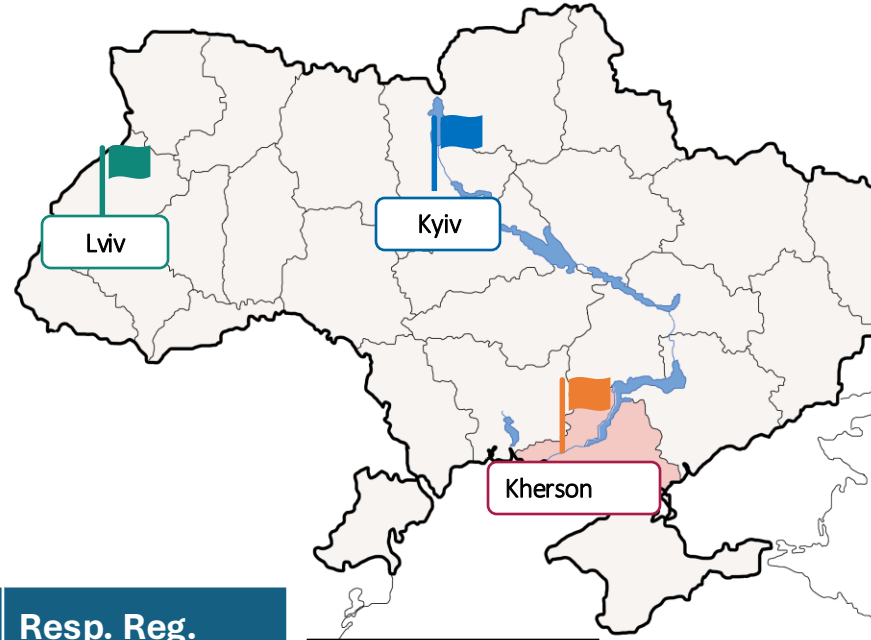
Vodafone 💔



Provider	ASN	IPs (2022)
Kyivstar	15895	760K
Vodafone	21497	348K
Lifecell	34058	386K

Kyivstar 🥺

Vodafone ❤️



Provider	ASN	Resp. Reg.
Kyivstar	15895	82.2K
Vodafone	21497	23.7K
Lifecell	34058	3K

up to 80%
of responsive are
regional