RIPE NCC
RIPE NETWORK COORDINATION CENTER

How the Internet routed around **Cable Damage in the Baltic Sea**

Internet event analysis with **RIPE Atlas**

Emile Aben | ENISA Telecom and Digital Infrastructure Security Forum | 20 March 2025

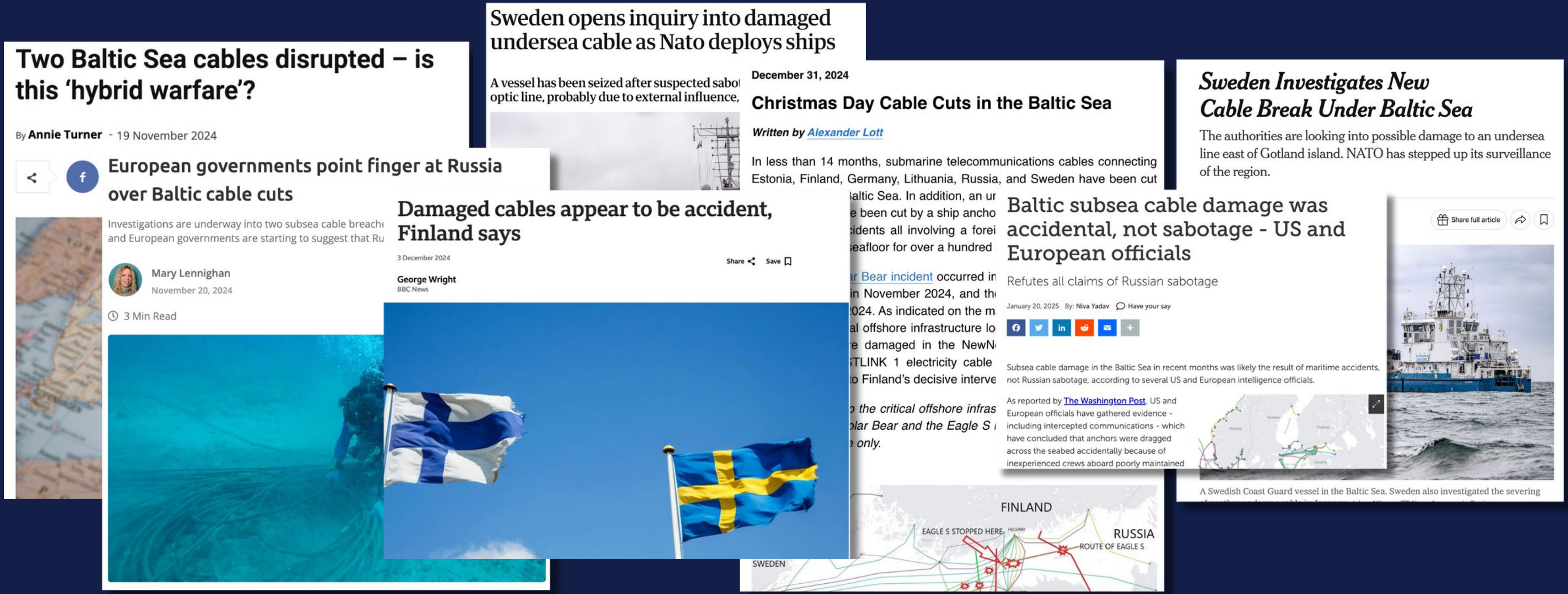
Baltic Sea cable incidents

Timeline of events analysed

- 17 Nov 2024: BSC East-West outage
- 18 Nov 2024: C-LION1 outage
- 27 Nov 2024: BSC East-West restored
- 28 Nov 2024: C-LION1 restored
- 25 Dec 2024: C-LION1 outage
- 06 Jan 2025: C-LION1 restored
- 26 Jan 2025: LVRTC outage
- 28 Feb 2025: LVRTC restored

Baltic Sea cable incidents

Media reaction



Measuring incidents with RIPE Atlas

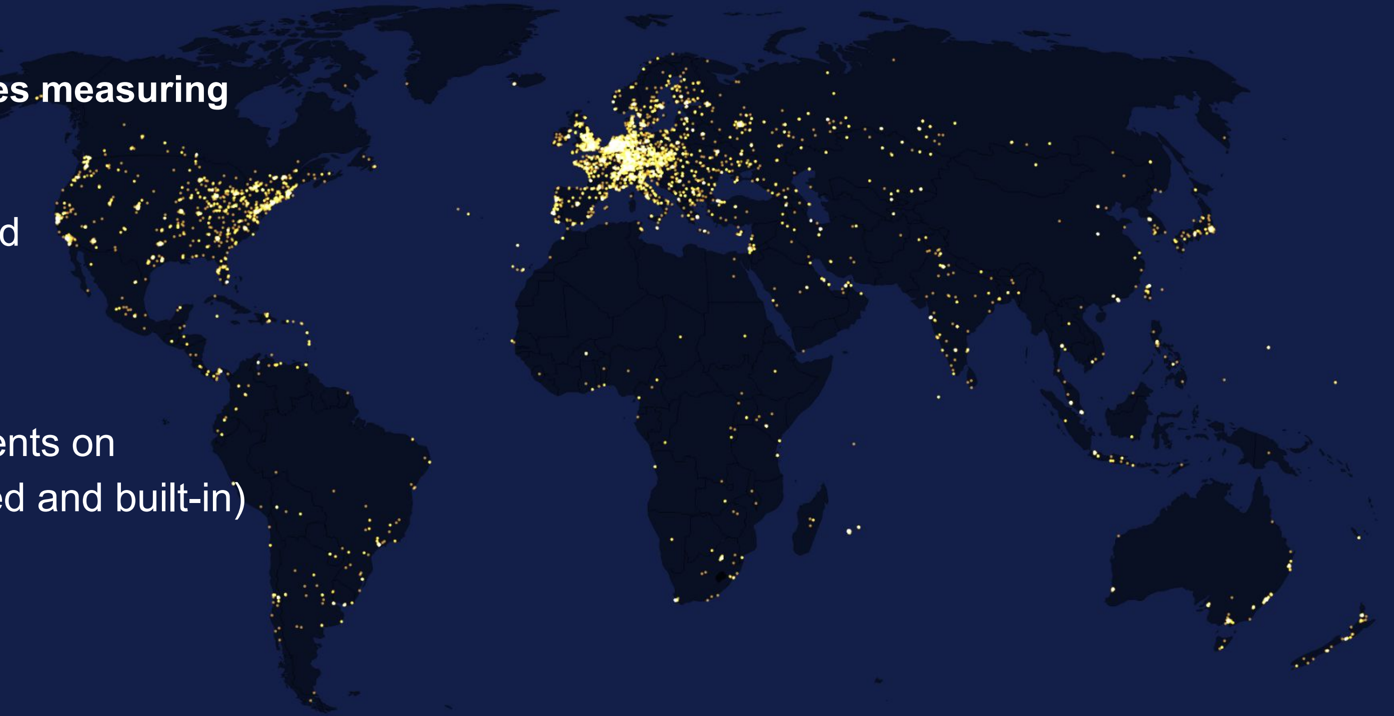
RIPE Atlas

A global network of probes measuring the Internet in real time

13,400+ probes connected

800+ anchors deployed

35,000+ daily measurements on average (both user-defined and built-in)



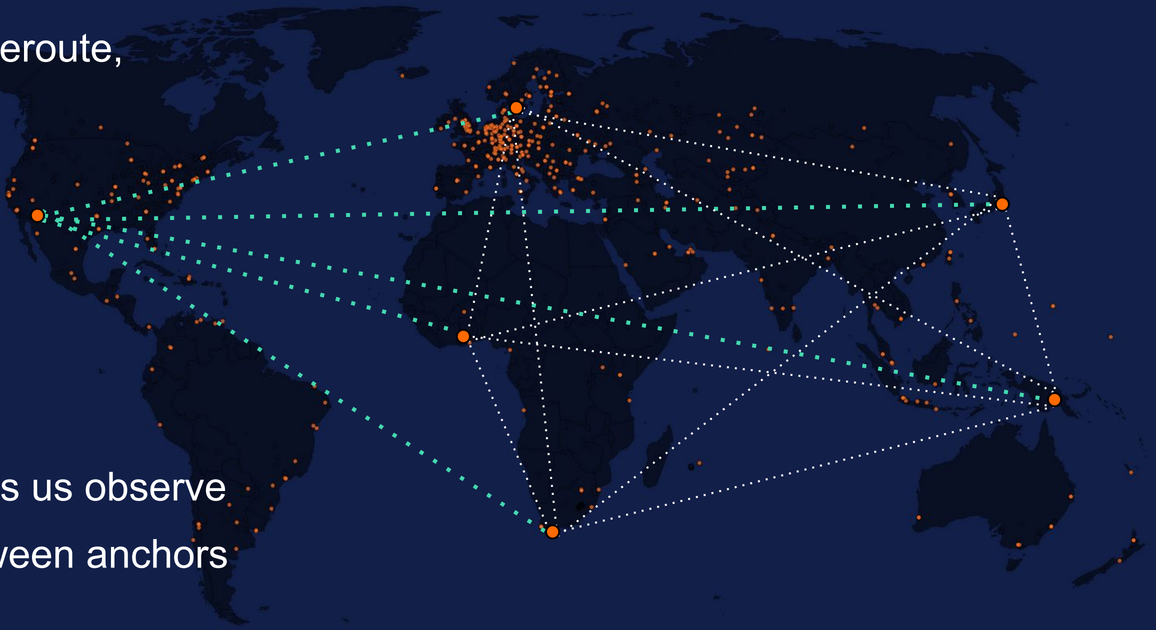
Measuring incidents with RIPE Atlas

Anchor mesh

RIPE Atlas anchors support ping, traceroute, DNS, HTTP/S measurements

Each anchor performs ongoing ping measurements to all other anchors at four-minute intervals

Resulting ‘mesh’ of measurements lets us observe latency changes and packet loss between anchors



First look

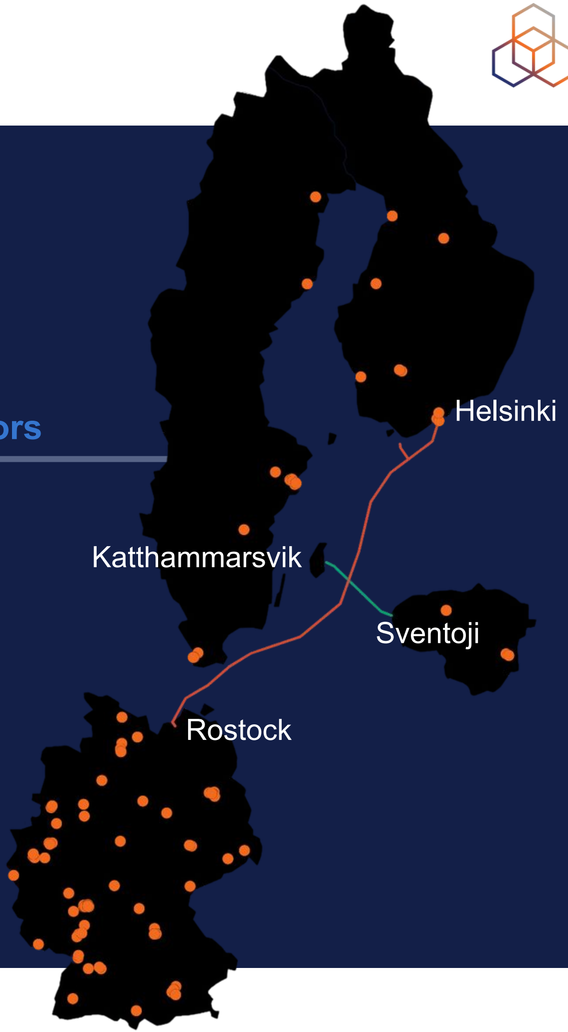
17-18 November

BSC East-West: Sweden-Lithuania

C-LION1: Germany-Finland

We looked at results in the RIPE Atlas anchor mesh between these countries around reported time of the event

Country	# anchors
Germany:	100
Sweden:	15
Finland:	12
Lithuania:	5



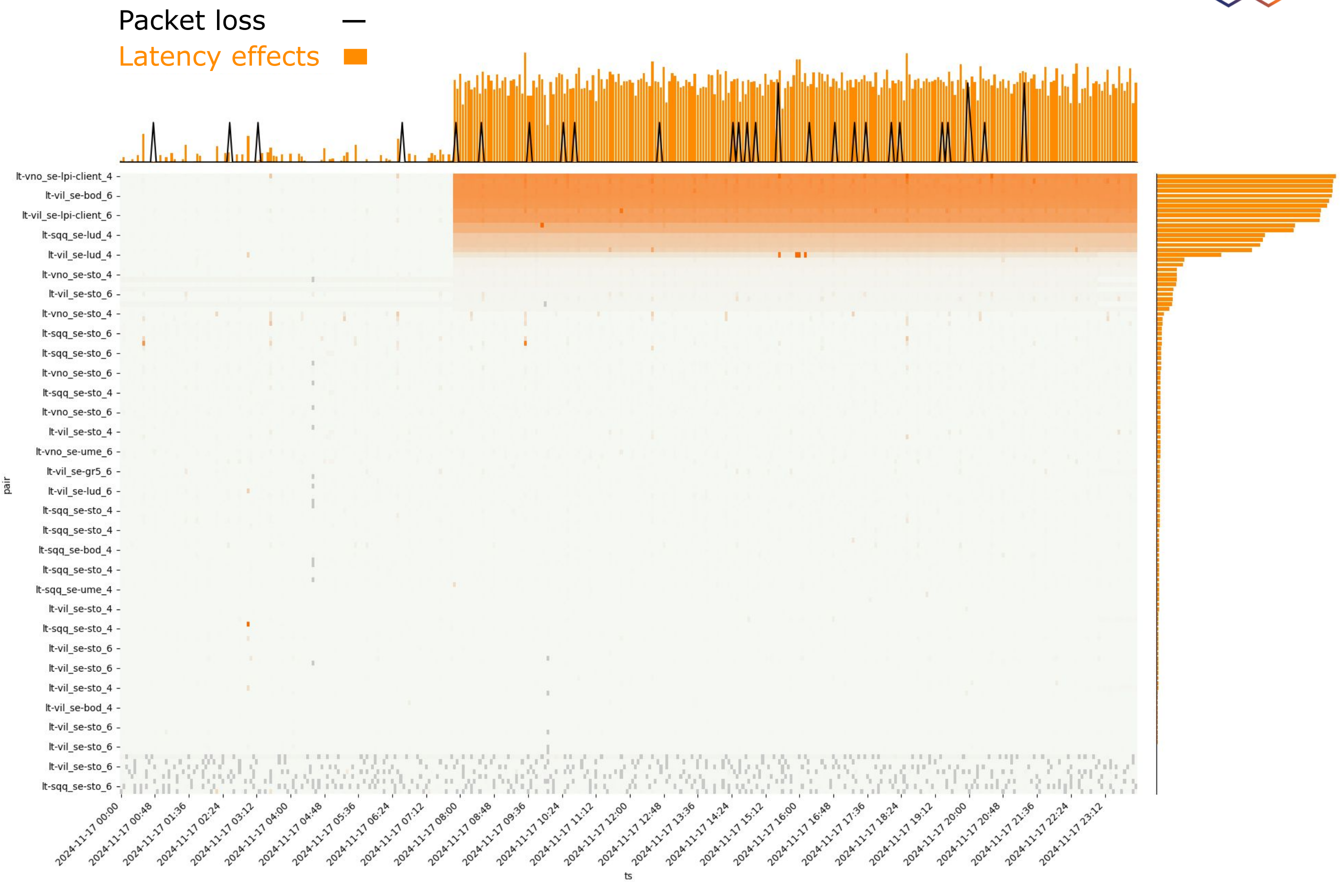
BSC East West

Latency shift

12 hour before/after time of event

Latency increase of approx 10-20 ms shortly before 08:00 UTC on 17 November

We subtract the minimum latency for a path during our observation period to make the latency jumps comparable



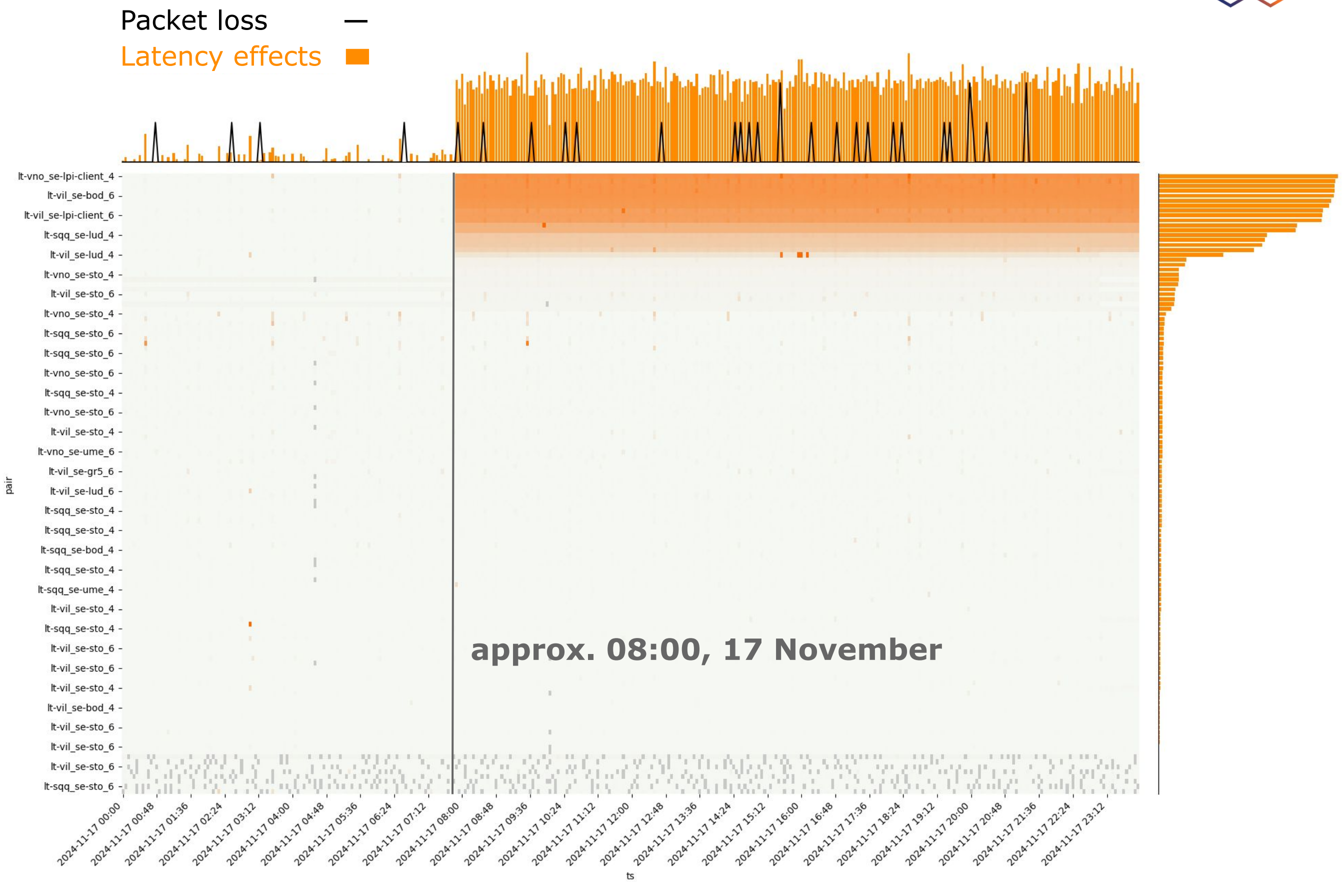
BSC East West

Latency shift

12 hour before/after time of event

Latency increase of approx 10-20 ms shortly before 08:00 UTC on 17 November

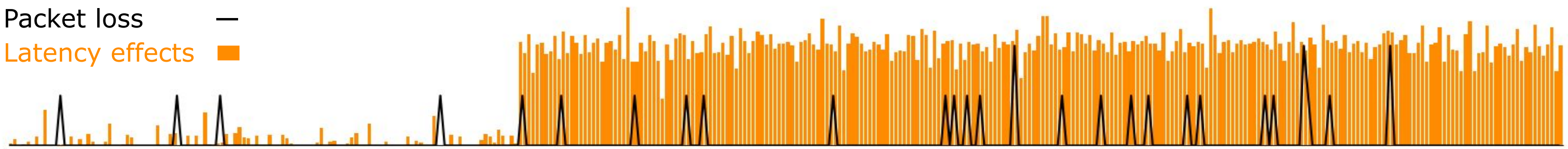
We subtract the minimum latency for a path during our observation period to make the latency jumps comparable



BSC East West

Packet loss

Baseline of 0% packet loss with occasional spikes



No significant increase in packet loss at time of the cable cut (shortly before 08:00 UTC)

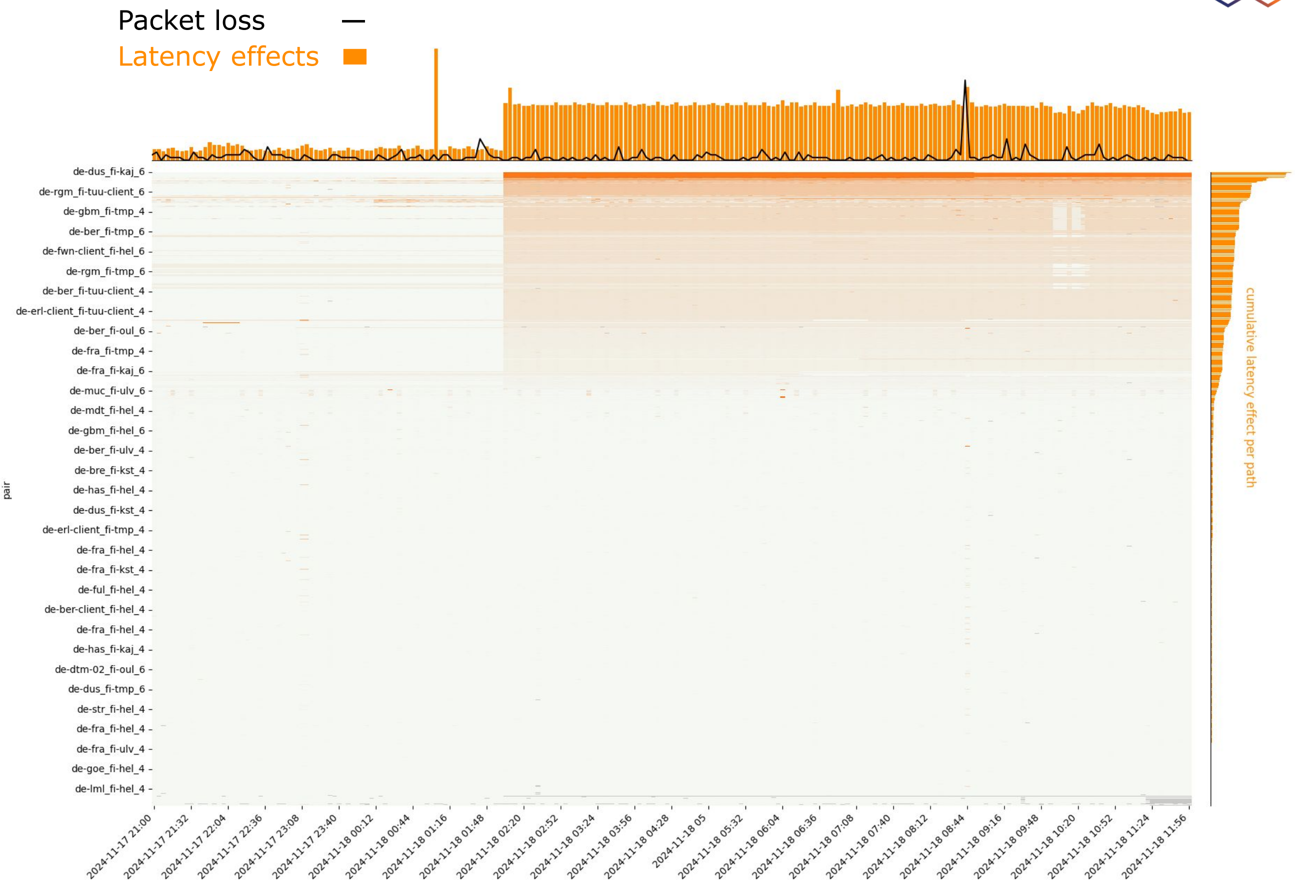
C-LION1

Latency shift

Latency increase of approx 5ms a little after 02:00 UTC on 18 November

Packet loss

Again, no significant increase in packet loss at time of break



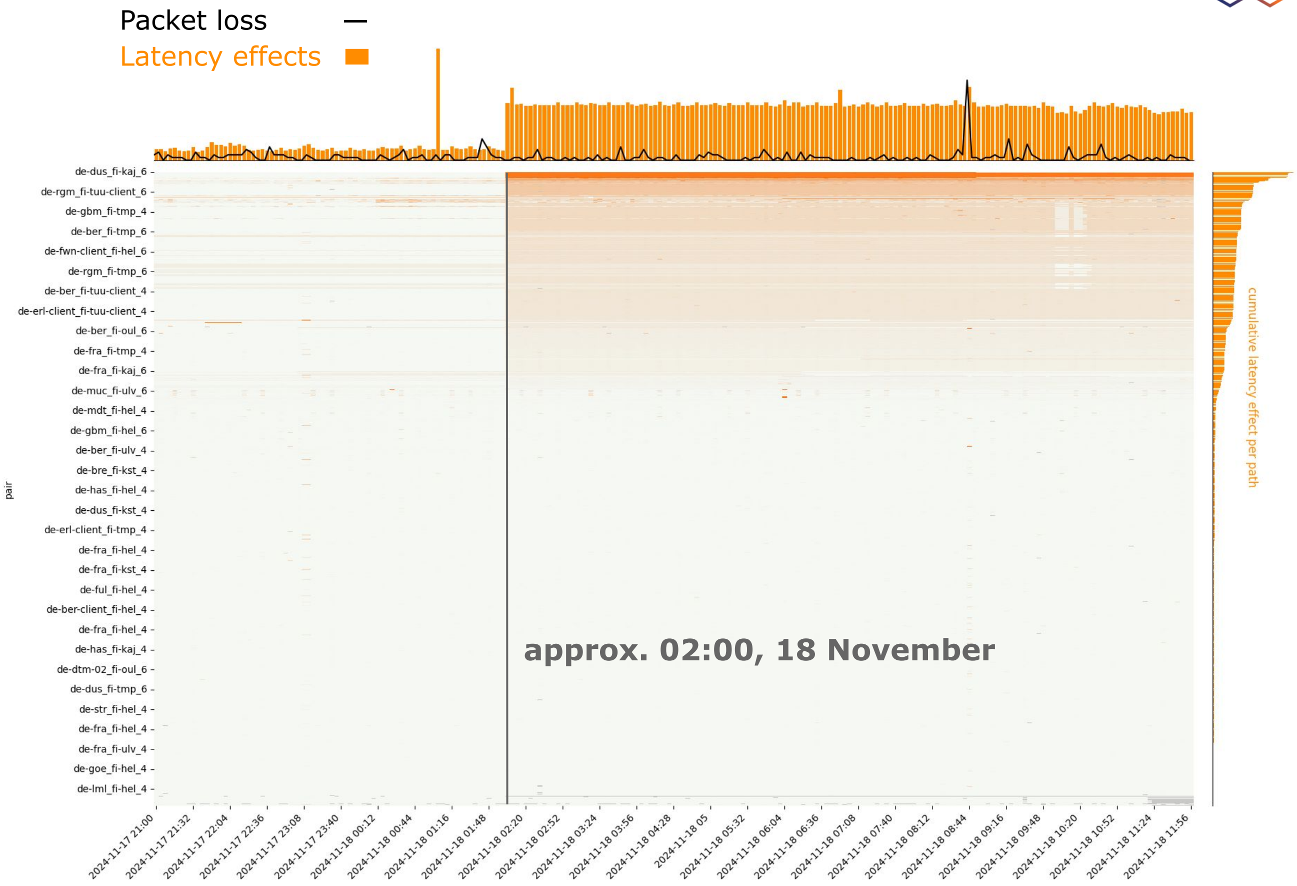
C-LION1

Latency shift

Latency increase of approx 5ms a little after 02:00 UTC on 18 November

Packet loss

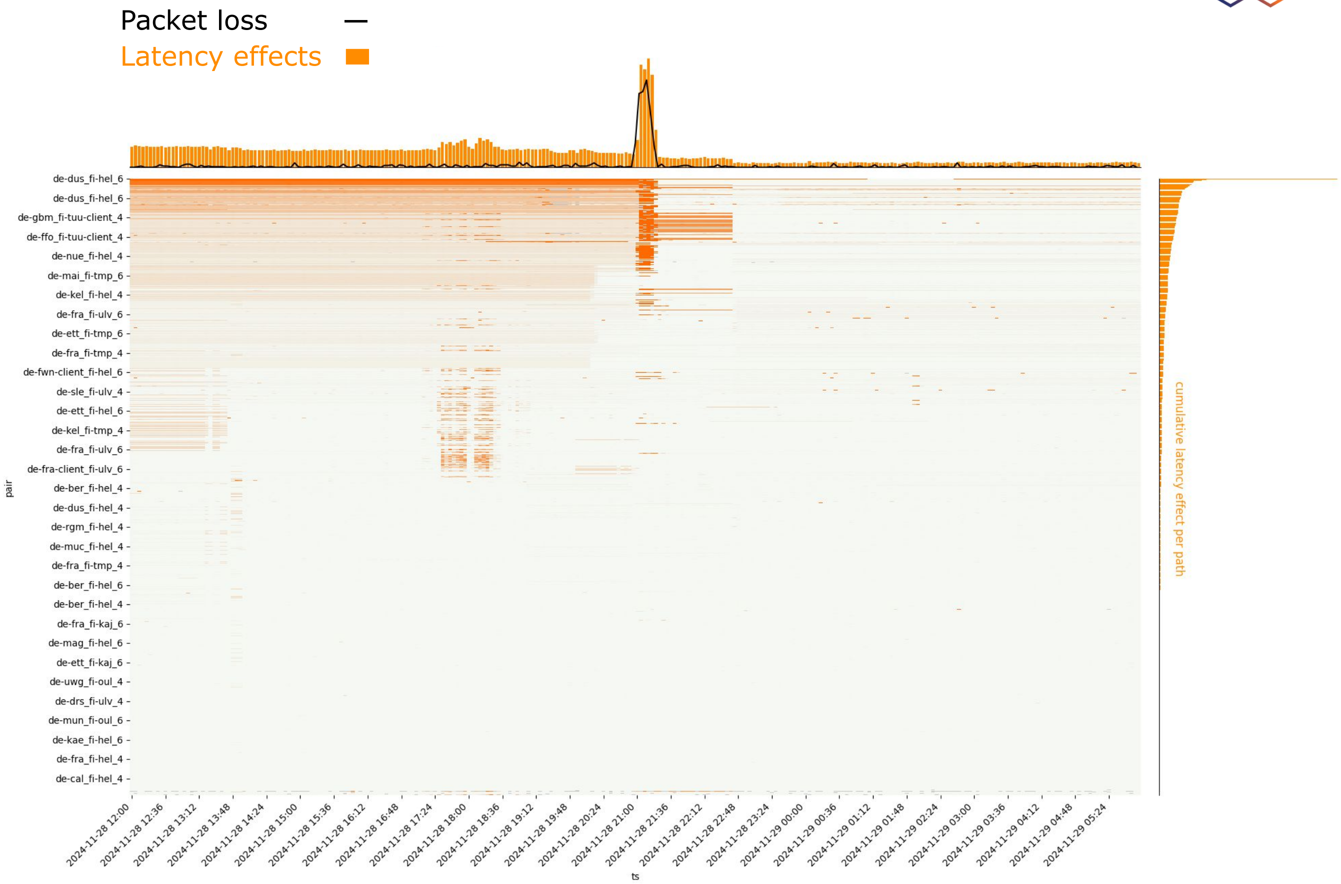
Again, no significant increase in packet loss at time of break



C-LION1 repair

On 28 November at 17:30 UTC, the C-Lion1 cable repair ship reported leaving the area after successful repair

Unclear what exactly causes these latency effects and the temporary increase in packet loss…

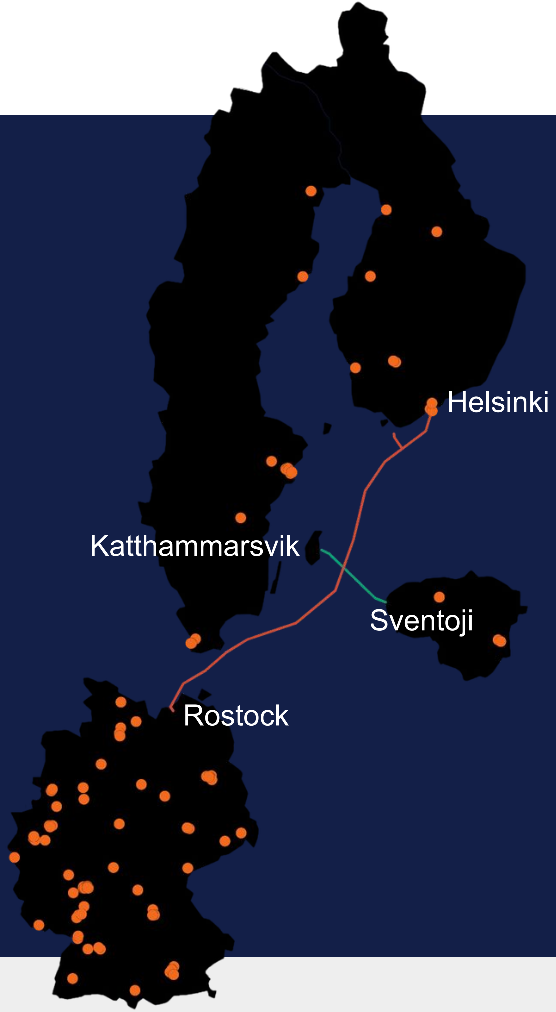


Summing up

There was a relatively minor but visible shift in latency for around 20-30% of paths between observed anchors

But there was no concurrent increase in packet loss

The Internet routed around damage!

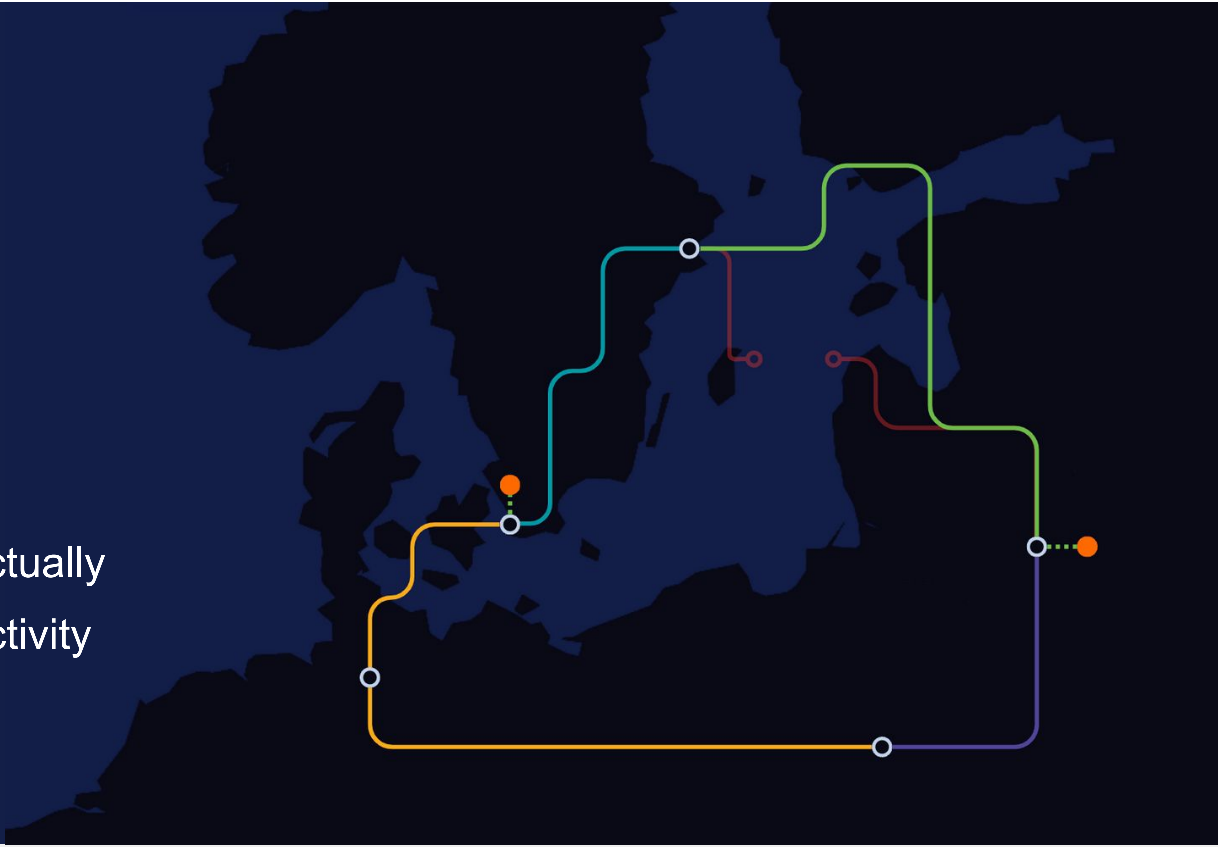


Deeper dive

Initial analysis was based on ping (end-to-end latency) data

We followed this up with in depth analysis using traceroute data

Aim: to examine how the paths actually changed while end-to-end connectivity was maintained



Levels of resilience

Inter-domain rerouting:

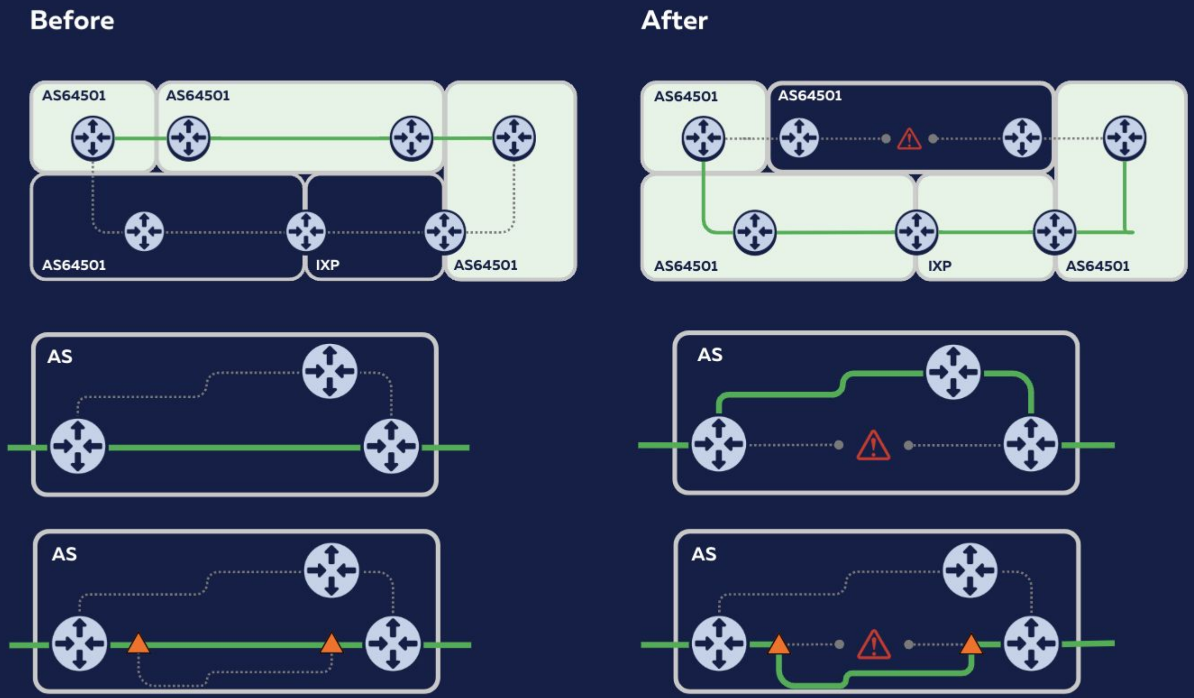
Traffic rerouted through alternative ASes/IXPs (eBGP routing protocol)

Intra-domain rerouting:

Rerouting *within* networks over alternative paths (IGP: OSPF, IS-IS)

Circuit-level rerouting:

Rerouting along alternative circuit-level connections between routers (same IP address!)



Levels of resilience

Of the 2,141 paths between anchors in Germany and Finland used for this analysis:

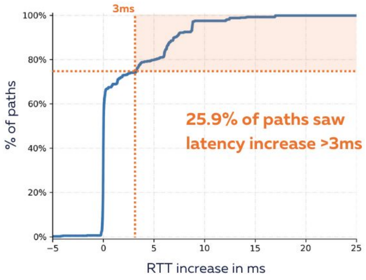
Inter-domain changes: 637 (29.8%)

Intra-domain changes: 1,044 (48.8%)

Other changes: 460 (21.5%)

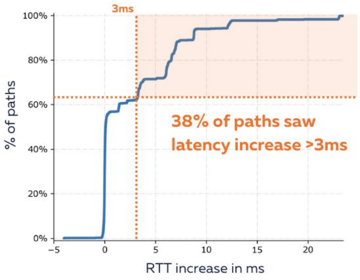
Inter-domain rerouting

RTT profile for paths where inter-domain routing changed.



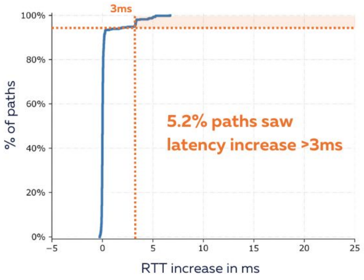
Intra-domain rerouting

RTT profile for paths with IP-level changes, but no inter-domain changes.



Circuit-level rerouting

RTT profile for paths without IP-level changes.



Conclusions

What can we learn from this?

In the Baltic Sea:

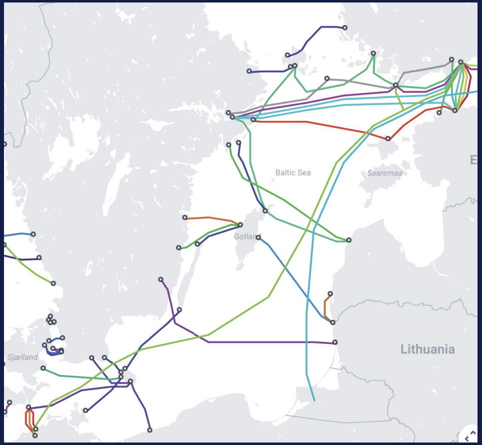
- “The Internet routed around damage”
- Internet resilience due to defence in depth against local damage
    - Redundancy within networks (circuit and routing)
    - Redundancy between networks

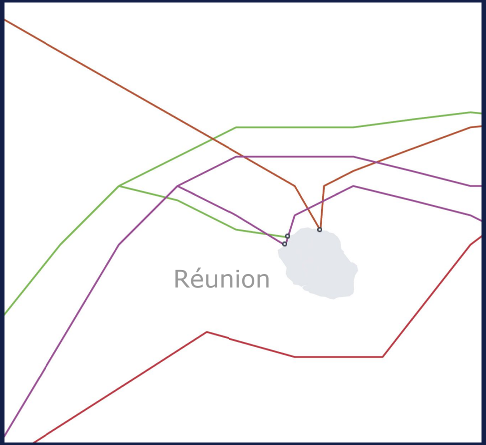
Conclusions

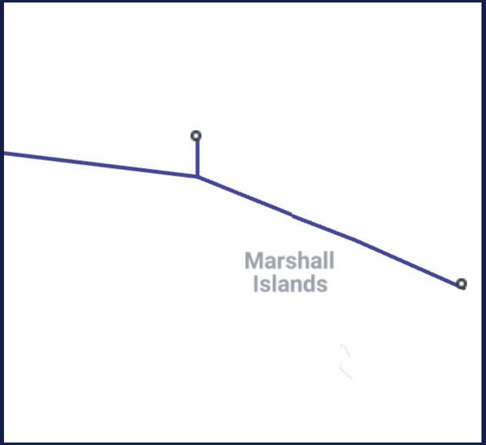
What can we learn from this?

What do we need to model a-priori information about resilience, redundancy and capacity?

- It is complex! 1 cable = multiple fibres = multiple lambdas with upgradable capacity
- Monitoring is a vital part of the puzzle







Ongoing incidents

There have been multiple further instances of damage to cables in the Baltic Sea since November 2024

Last known reported incident occurred on: XXXX

We are continuing to monitor and analyse events!

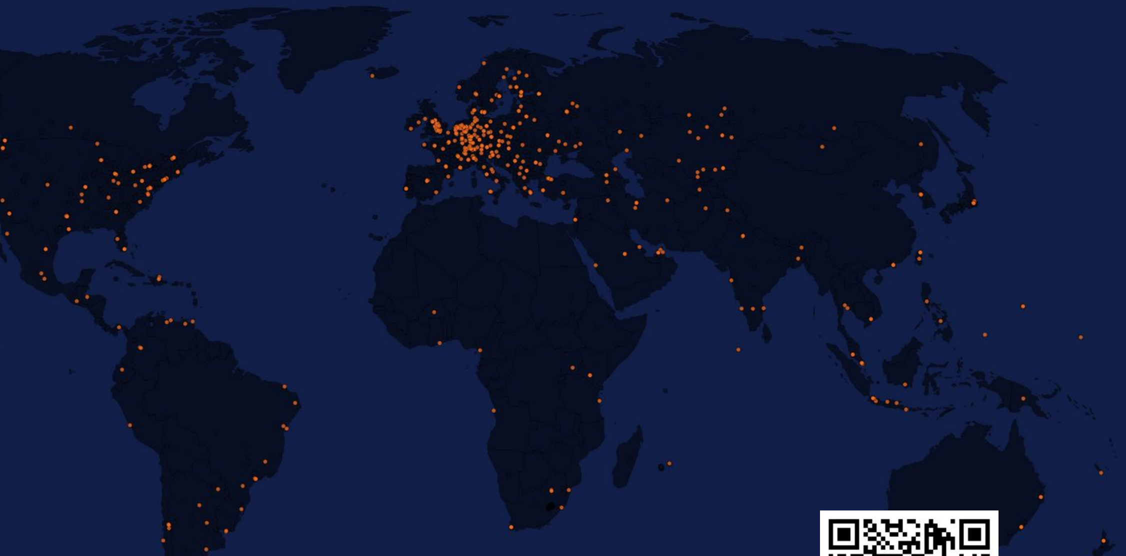
- Sweden-Latvia Internet cable belonging to Latvia State Radio and Television Center (LVRTC) was reportedly cut on 26 Jan 2025.
- This is another in a series of cuts on submarine cables in the region in recent months.
- Packet delays between selected RIPE Atlas anchors increased by 5-20ms at around 00:45 UTC – *but absence of packet loss indicates that the Internet successfully routed around the damage*

Read further analyses of cable cuts and Internet outages on RIPE Labs:
https://labs.ripe.net/search/tag/outages/

Beyond the Baltic Sea

We have a relatively high number of RIPE Atlas anchors in **some** countries around the Baltic Sea

Damage to cables is not so easy to analyse: e.g., much less visibility into recent damage to Taiwan cables



We are actively seeking hosts who can help us get RIPE Atlas probes and anchors set up in locations where they can shed light on the state of the Internet. Learn more:

Questions & Comments ?

eaben@ripe.net

RIPE NCC
RIPE NETWORK COORDINATION CENTER

THANK YOU!