Arelion and some trends we see

Mattias Fridström

Vice President & Chief Evangelist

”Sweden's most important company you never heard about”

Jätten på botten

Sveriges viktigaste bolag du aldrig hört talas om

Få bolag är mer samhällsbärande än doldisen Arelion som möjliggör 65% av världens internetanslutning. Nord Stream-attackerna har satt ljuset på bolagets samhällskritiska infrastruktur som löper längs Östersjöns botten. ”Det är inte ovanligt att fiberkablarna går av, både på land och i vattnet”, säger VD:n Staffan Göjeryd till Affärsvärlden.

TEXT: CARL-JOHAN KULLVING

DAGENS NYHETER. Nyheter Sverige Världen Ekonomi Kultur Sport

SVERIGE

Här går den skadade kabeln i Östersjön

Uppdaterad 2023-10-18 Publicerad 2023-10-18

The damage to a Baltic undersea cable was 'purposeful,' Swedish leader says but gives no details

Sweden Says Second Undersea Cable Damaged in Baltic Sea

The incident comes days after Finland and Estonia said sabotage was the likely cause of disruptions to a gas pipeline and a communications cable

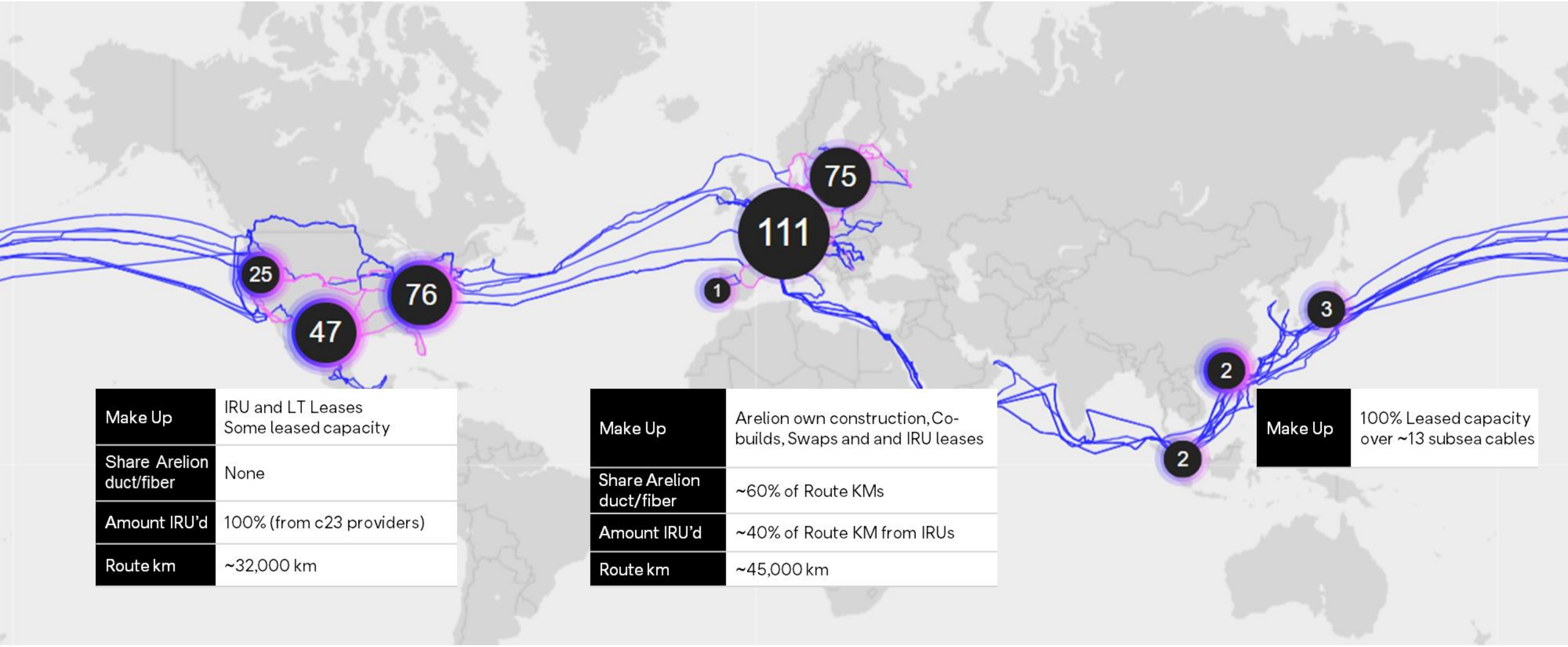
UTRIKES

Utrikes Meny

Undervattenskabel mellan Estland och Sverige skadad

Publicerad 17.10.2023 17:16. Uppdaterad 17.10.2023 19:43.

ARELION'S BACKBONE IS A COMBINATION OF OWN FIBER, IRU'd FIBER AND LEASED CAPACITY

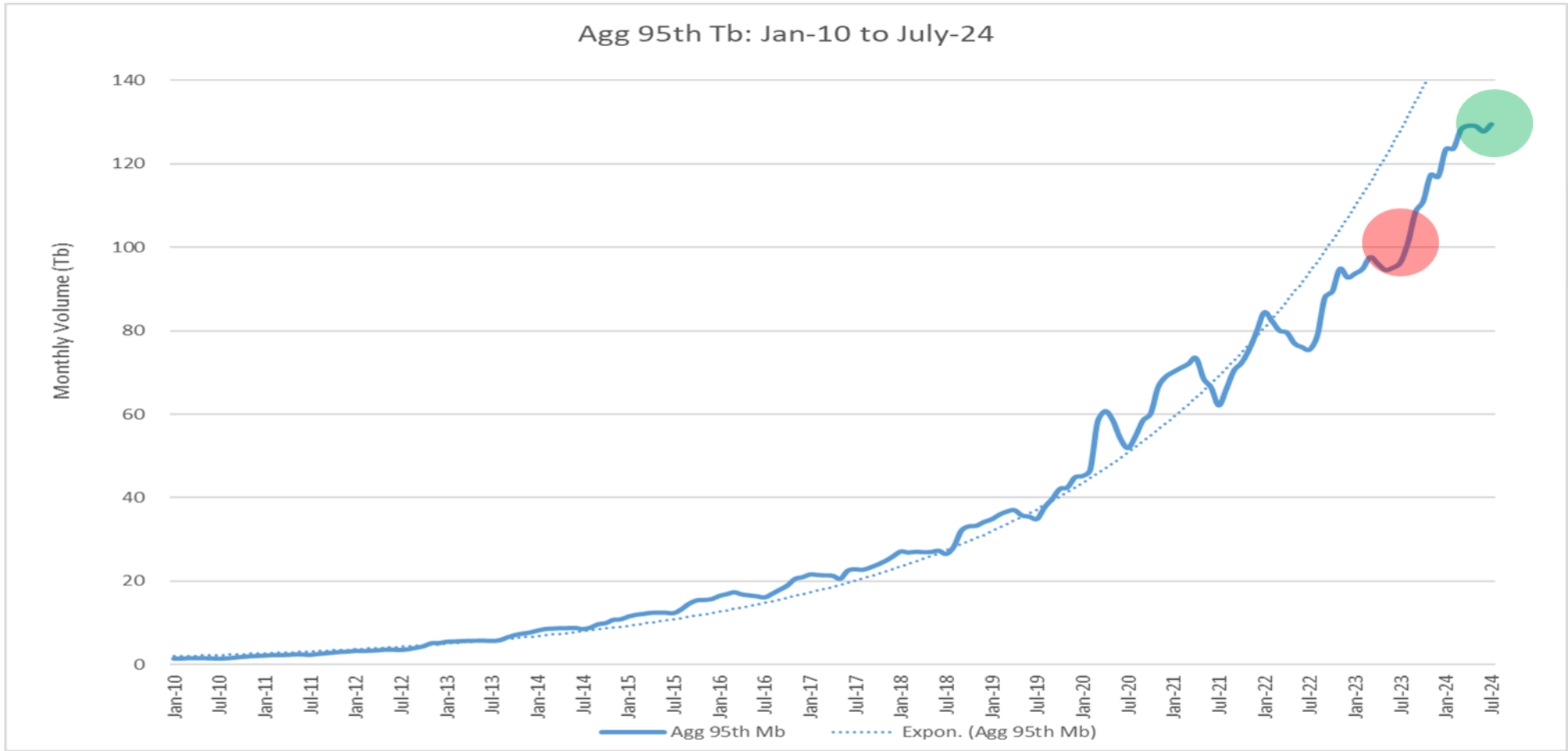


Make Up	IRU and LT Leases Some leased capacity
Share Arelion duct/fiber	None
Amount IRU'd	100% (from c23 providers)
Route km	~32,000 km

Make Up	Arelion own construction, Co-builds, Swaps and and IRU leases
Share Arelion duct/fiber	~60% of Route KMs
Amount IRU'd	~40% of Route KM from IRUs
Route km	~45,000 km

Make Up	100% Leased capacity over ~13 subsea cables

IP TRAFFIC GROWTH WITH ARELION – THE MAGIC NUMBER PASSED A YEAR AGO



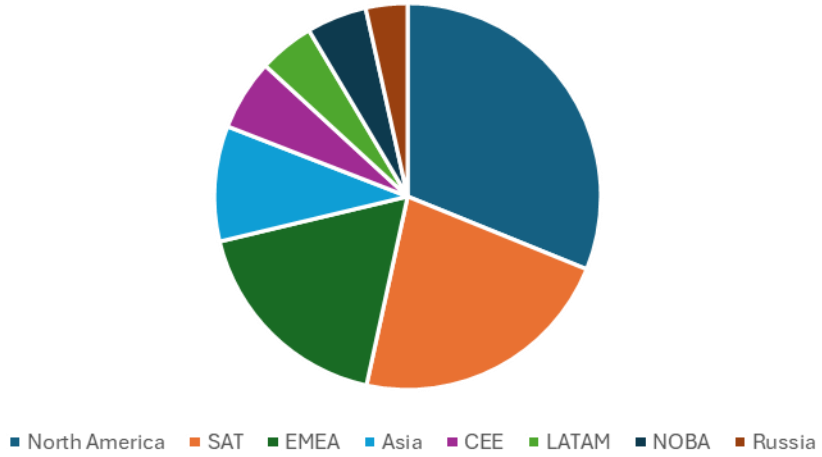
130 Tb/s on Aug 4th 2024

100 Tb/s on Aug 28th 2023

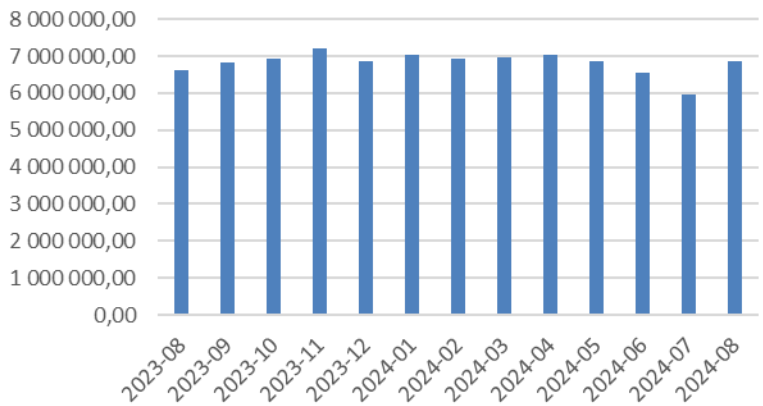
Traffic distribution within Arelion

- We really see ourselves as a global provider
- For obvious reasons we have a strong Nordic foundation with many connected networks
- Largest traffic growth is still outside of Europe and North America

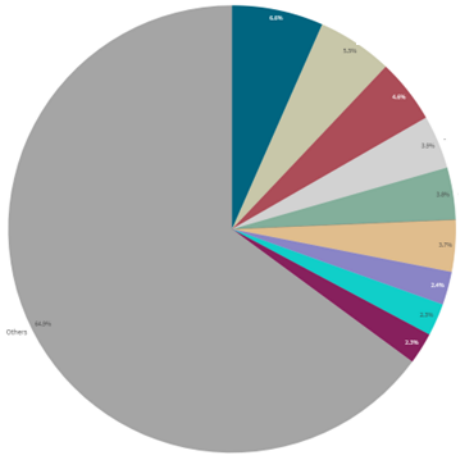
Arelion traffic distribution, customer origin



Traffic in the Nordics

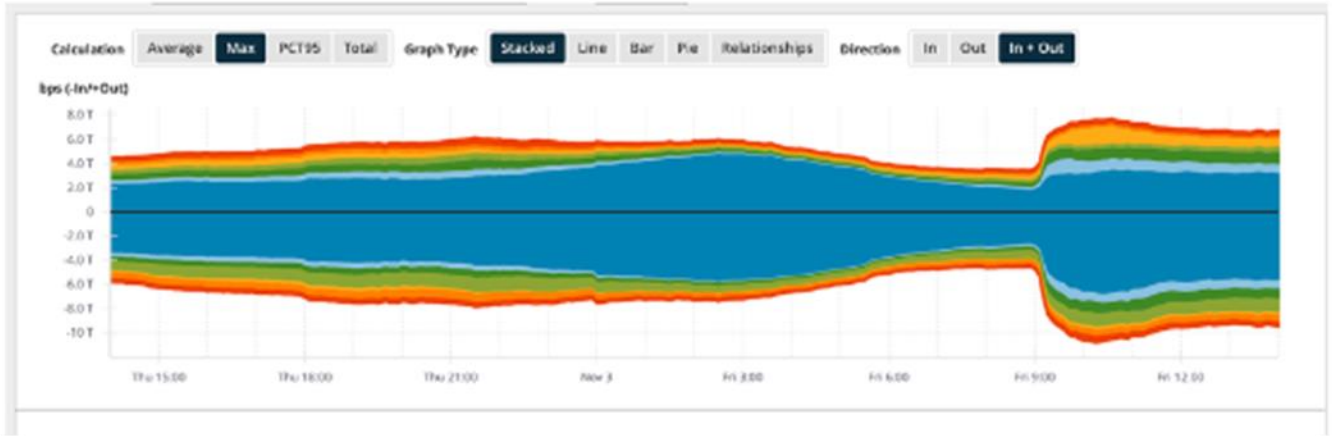


10 largest traffic customers vs all customers



ONE GAME CAN STILL AFFECT THE WORLD

- On Friday morning at 09:00 CET, we began to detect a significant surge in HTTP traffic on the network. It was clearly visible on a global scale, requiring a substantial amount of traffic to be noticed.
- Why was it only HTTP and not HTTPS, which would be the most likely attack vector, accounting for 75% of the surf traffic?
- After conducting some forensic analysis, which didn't provide a clear understanding, the traffic was affecting numerous countries, had the same packet length, and seemed to originate from a specific top CDN customer.
- Thanks to the close cooperation within the industry, questions were sent out to inquire if anyone else had observed the same traffic patterns. Direct queries were also made to the customers. Finally, we got the last piece to the puzzle.
- It turned out to be a **massive Fortnite update**. A single game had the power to impact global traffic patterns and set the security teams in motion. Of course, given the situation in the world, people are more alert



KEY TRENDS INFLUENCING OUR BUSINESS

- The **geopolitical, population and regulatory environment** is shifting – a different context than what gave rise to the "internet geography" of the 2000-2020s. **Continued tensions** also driving needs for security/resilience
- **(Green) Power Grab** – high demand and conflicts of interest around green power to supply the need for AI/Cloud computing

- The **fundamentals growth drivers of the Internet remain the same** – continued expansion of Consumer Video and B2B Cloud services
- **Artificial Intelligence** emerging as potentially huge driver of new capacity requirements – pushing demand towards secondary/tertiary markets
- Shifting demand amongst **large-scale Enterprise customers** remains Arelion's largest "white space"

- **Arelion well positioned for growth its core products and services** – amongst diversified, distracted telcos – though with large difference between European and US markets
- Competitors **stepping out** or **doubling down** – choosing between infra or service plays
- Key players Colt and Cogent **currently busy with post-merger integration** – but may emerge as more formidable rivals over time – AI opportunities turning their attention to networks

- **Accelerated technology change opens new opportunities** – but also requires us to **reimagine our operations and** acquire new skillsets
- New entrants raising the bar for customer experience

DDoS Security

-your first line of defense

Arelion

CURRENT KEY TRENDS

Peak attacks continue to grow in size

- Largest attack so far at 1,45Tbps
- Average attack size at 11,2 Gbps

Global decrease in large volumetric DDoS attacks

- While decreasing globally we see an increase locally (on a national level)

Overall decline in packets-per-second attacks

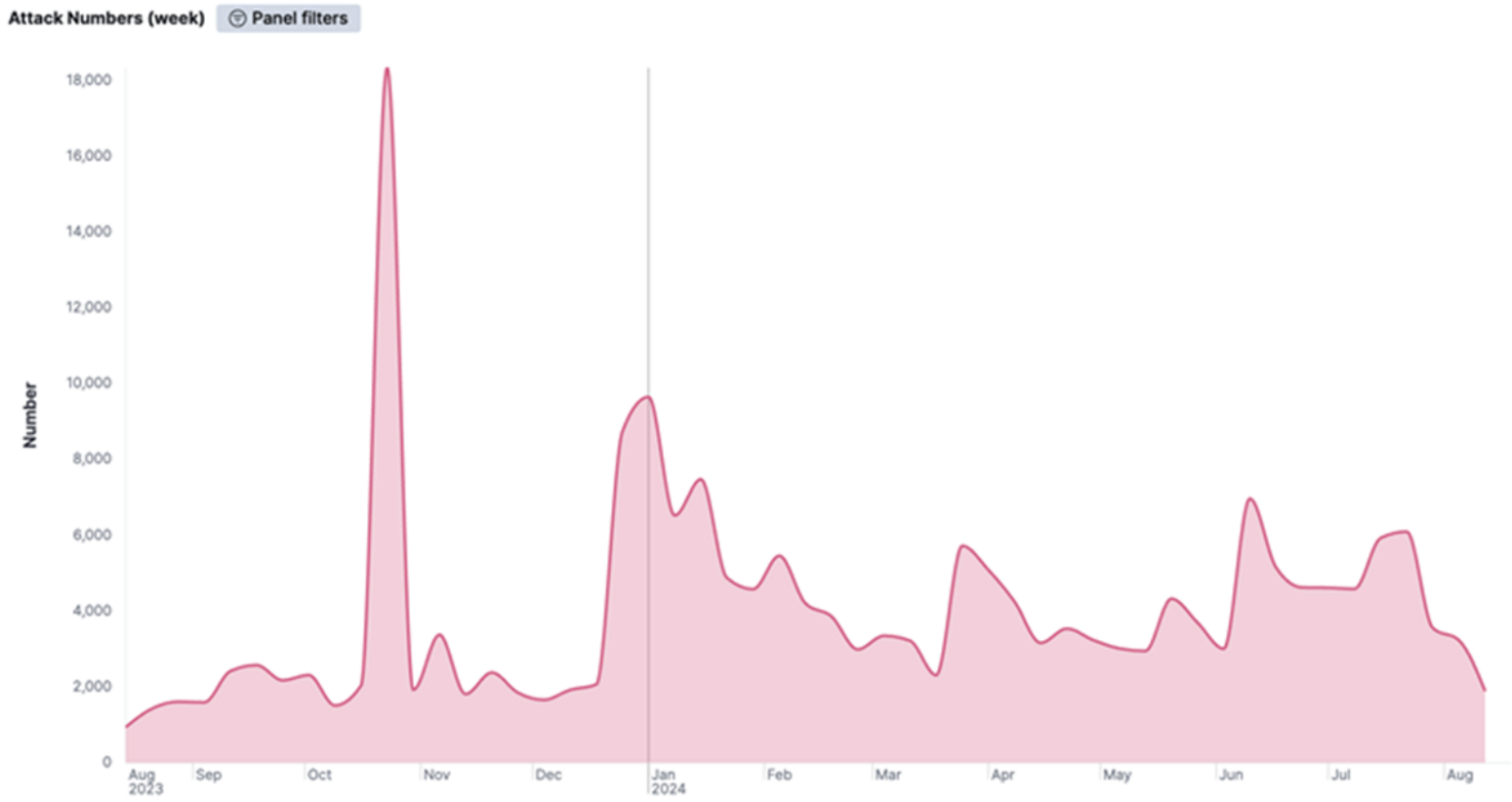
- Hackers work “smarter not harder”

Attack duration is down

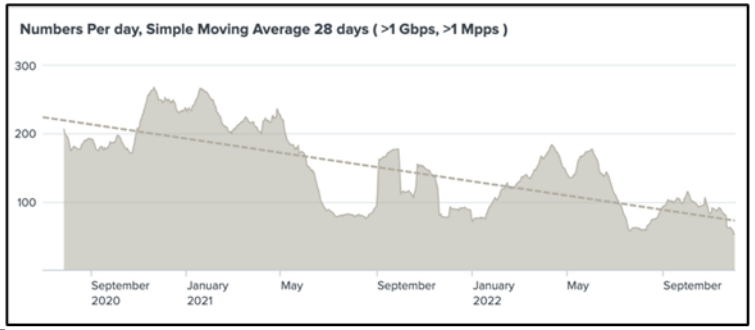
- Most likely due to that unsuccessful attacks are called off quicker

THE NUMBER OF ATTACKS ARE SLOWLY INCREASING

- While the fight towards attacks continuous we see a slow growth in the number of attacks inside AS1299
- The war between Russia and Ukraine still provides an increasingly portion of the number of attacks



September 2020 – December 2022

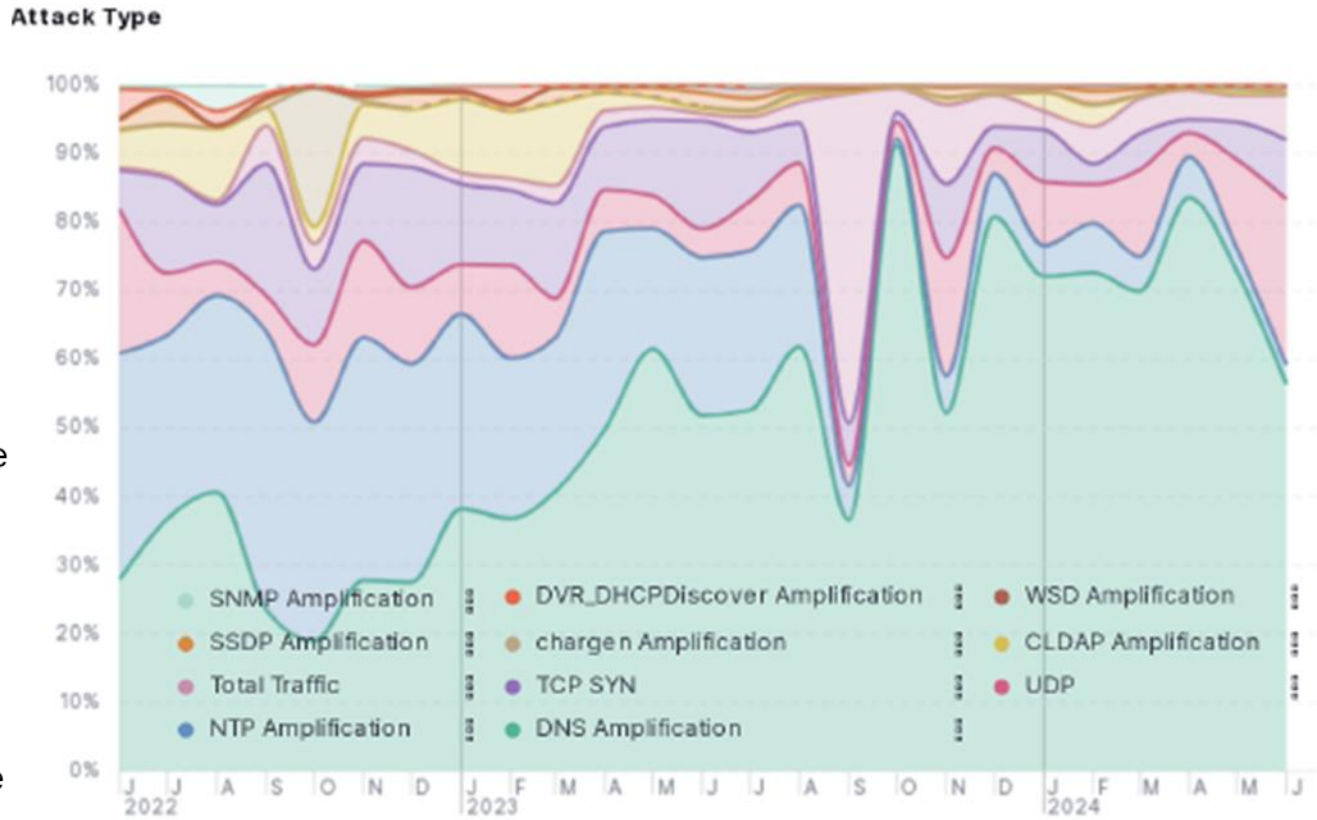


TYPE OF DDoS ATTACKS AS SEEN BY AS1299

- DDoS attacks are usually divided in two categories

1. Volume or size attacks where you measure the attack in bits per second (bps)
   - You flood the target with as much traffic as possible to overwhelm its bandwidth
   - A common use case today is to use botnets to generate the traffic

2. Network Protocol attacks where you measure the attack in packets per second (pps)
   - You manipulate packets to cause a memory overflow in the targets buffer



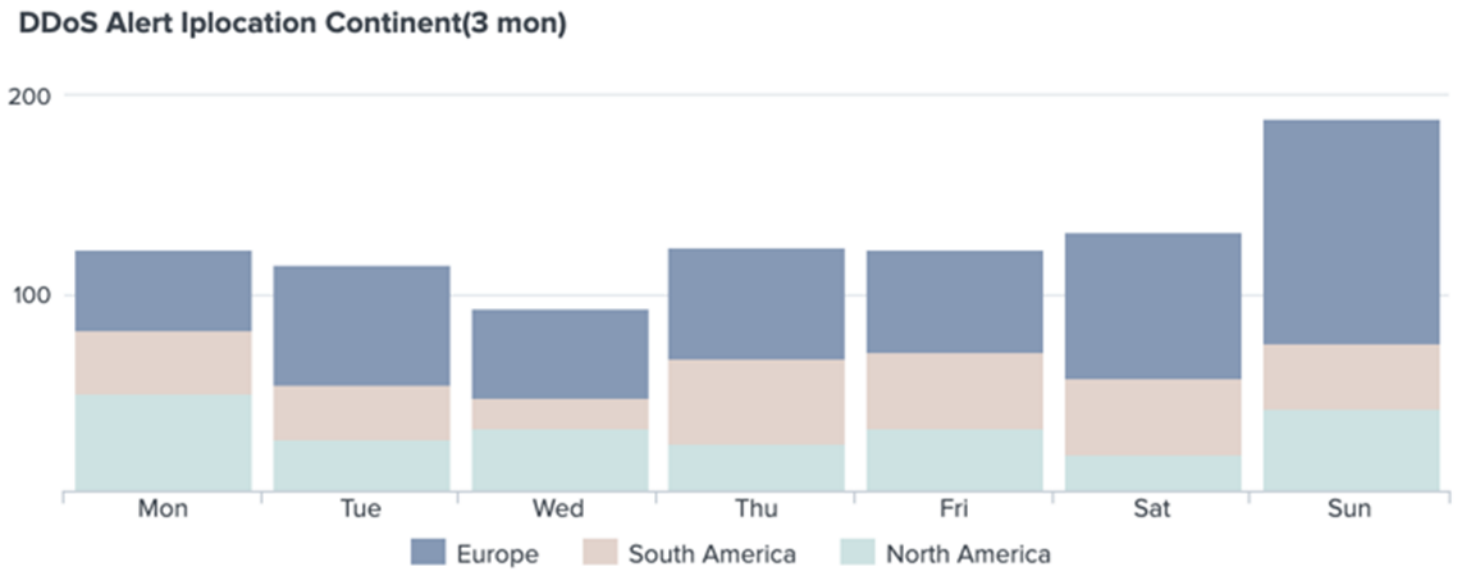
Almost **80%** of the attacks are DNS amplification attacks

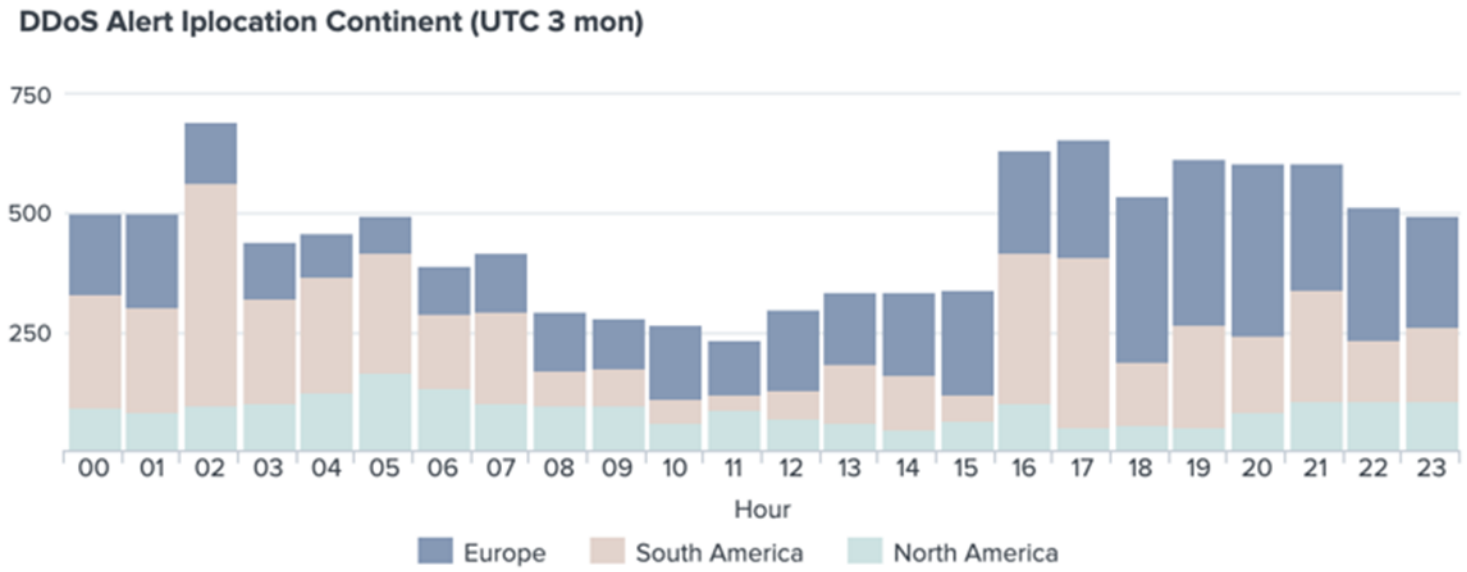
THE MOST COMMON CUSTOMER ATTACK

- DNS amplification is by far the most popular type of attack
- The most common DNS amplification attack vector is **UDP over HTTP** (port 80) and **HTTPS** (port 443)
- We see a quite big shift to exploiting compromised or acquired virtual machines (VMs) and virtual private servers (VPSs) from using IoT based botnets.
  - Servers offer much more bandwidth and computational resources
  - People are in general better at protecting IoT devices with passwords

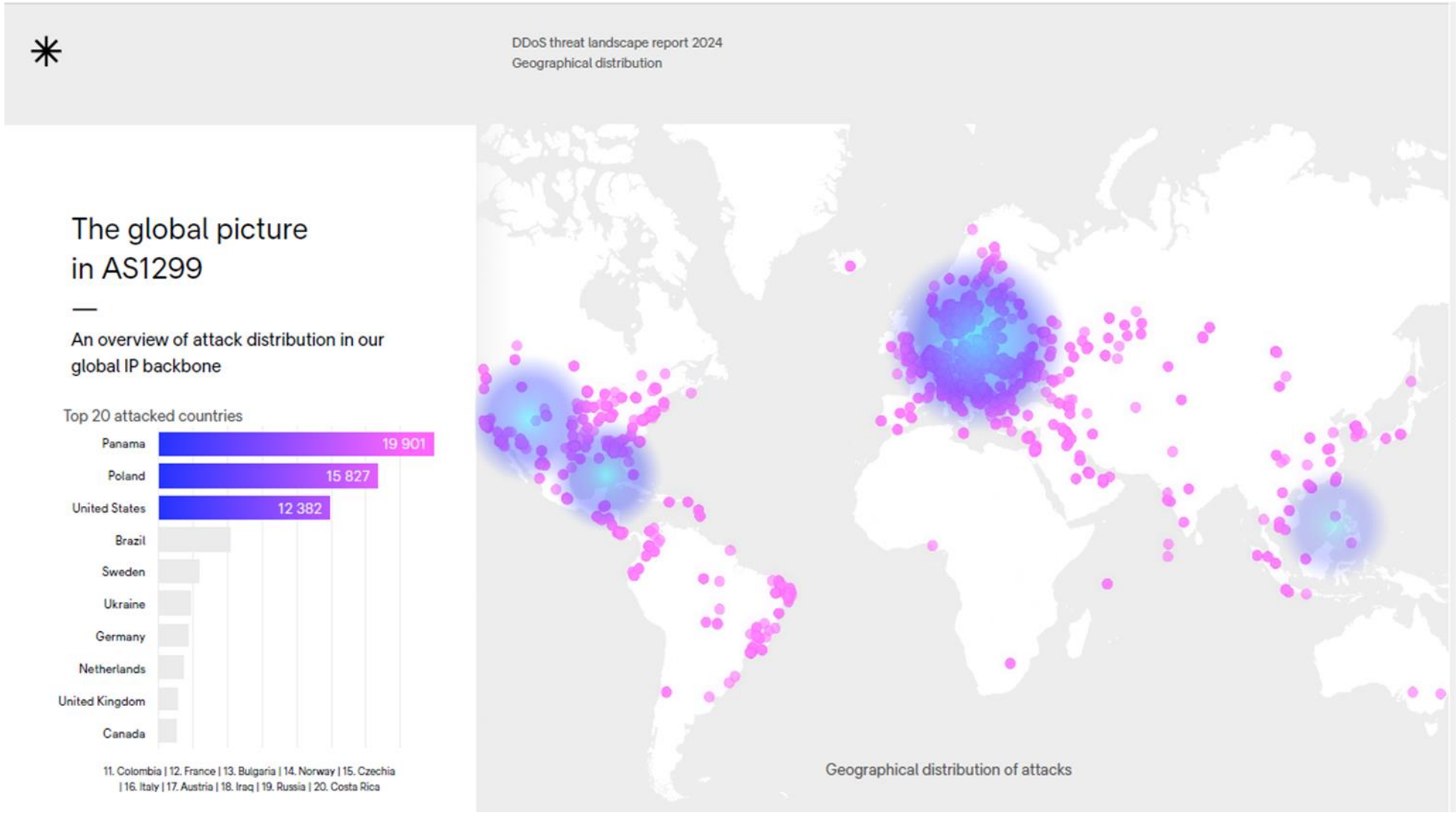
WHEN DO THE DDoS ATTACKS OCCUR

- Attacks over the weekend are still most popular and most attacks are done after office hours
- From an Arelion view more attacks are seen in Europe than in North America
- South America has un unproportional number of attacks in our network





GEOGRAPHICAL DISTRIBUTION

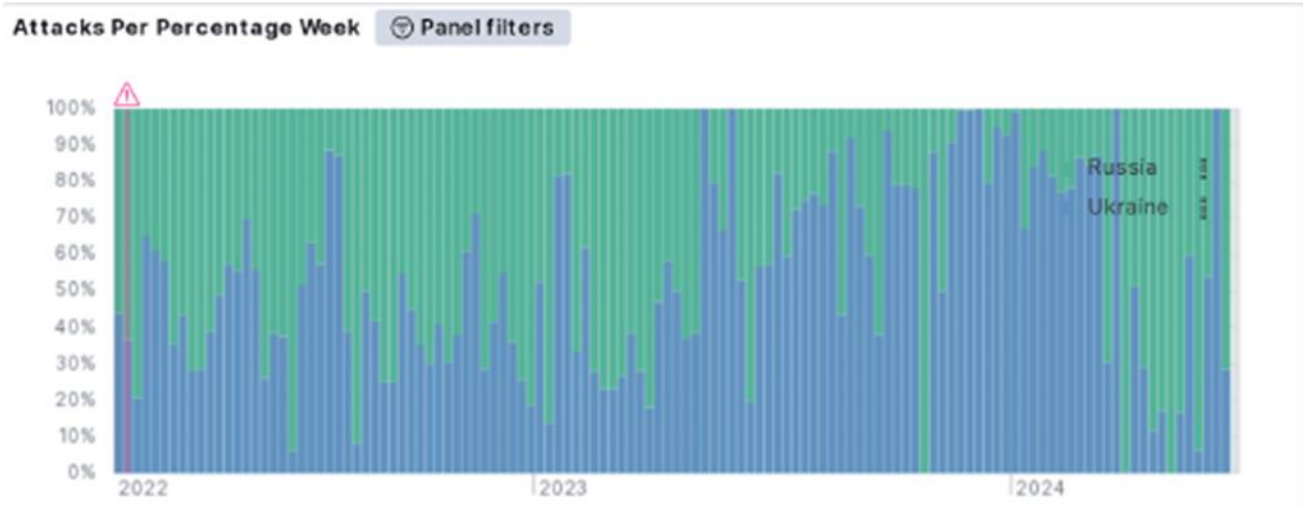


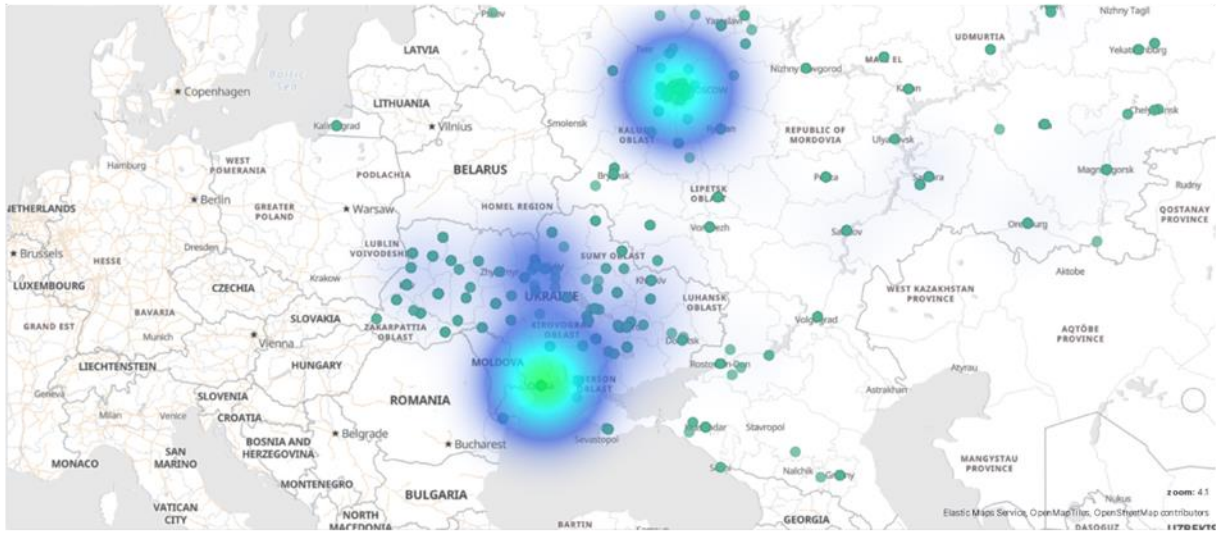
DDoS ATTACKS – RUSSIA AND UKRAINE INSIGHT

- Since Arelion run a significant amount of IP traffic towards and inside both Russia and Ukraine we have good insights in ongoing cyber attacks
- While attacks initially were targeted towards Ukraine we can now see more of a 50/50 spread
  - Largest attacks have clearly been towards Russia
  - It should be noted that lots of Ukrainian sites have been moved to outside of Ukraine and are now running from the cloud

Green = Attack on Russia

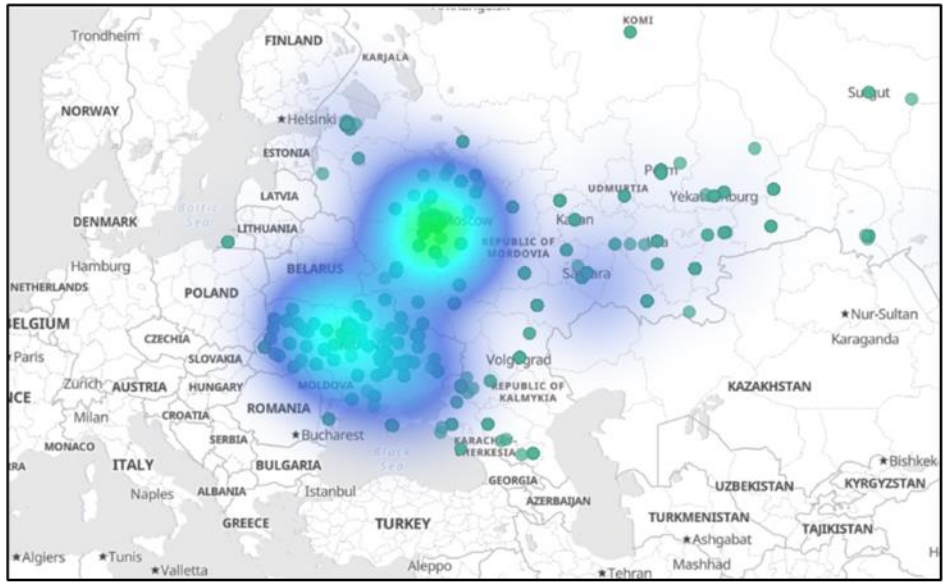
Blue = Attack on Ukraine



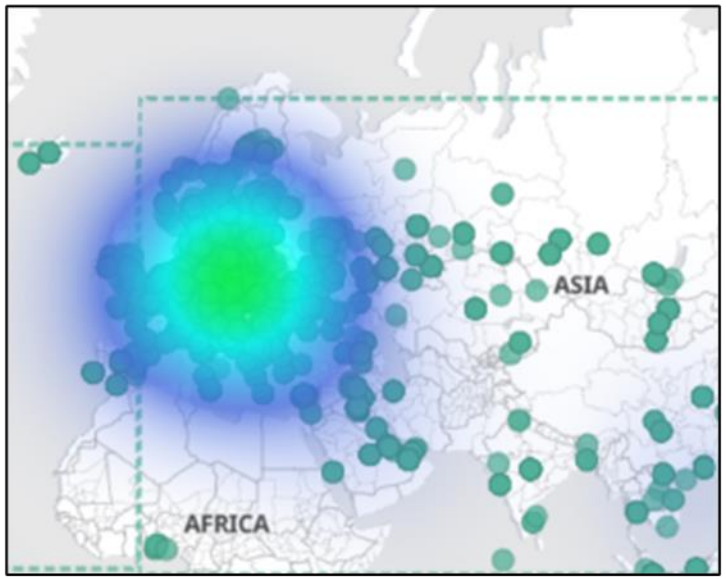


RUSSIA AND UKRAINE – CHANGE OF ATTACK PATTERNS

- After the initial attacks at the start of the war the attacks are now much more to neighboring countries with Poland taking the largest hit



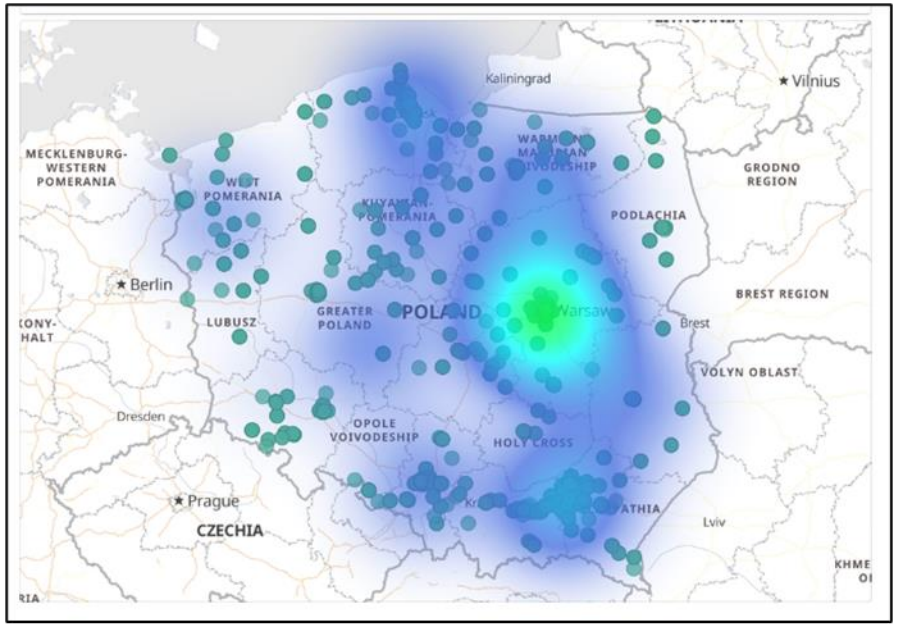
Summer 2022



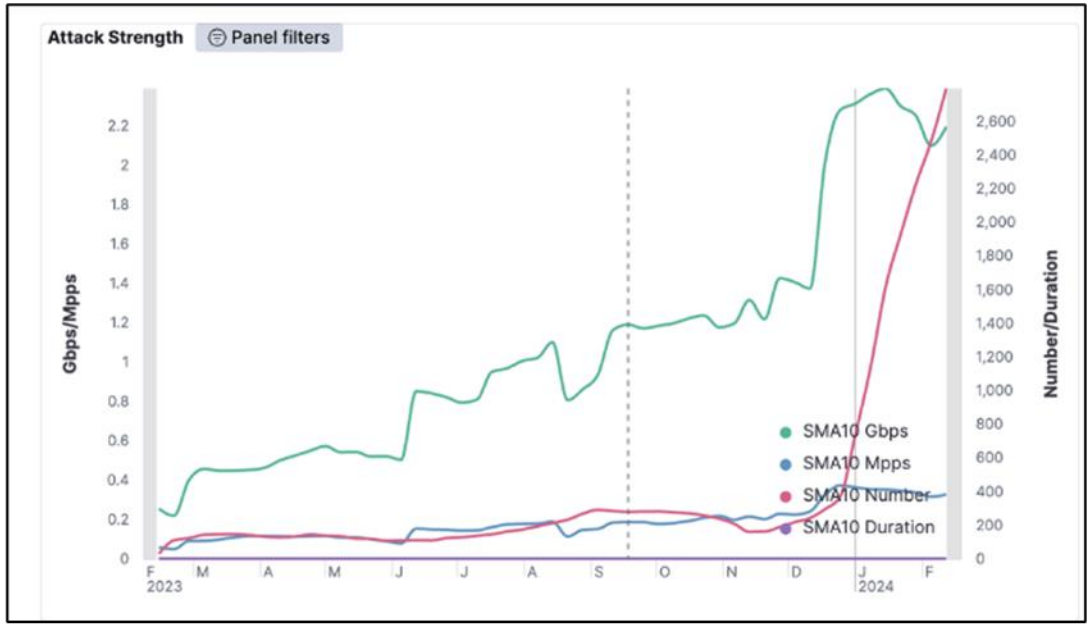
Summer 2024

POLAND IS CURRENTLY SINGLED OUT BY MANY HACKING GROUPS

- Most attacks use the DNS amplification vector and their target is both the data communication industry as well as infrastructure companies



Summer 2024



The start early in 2024

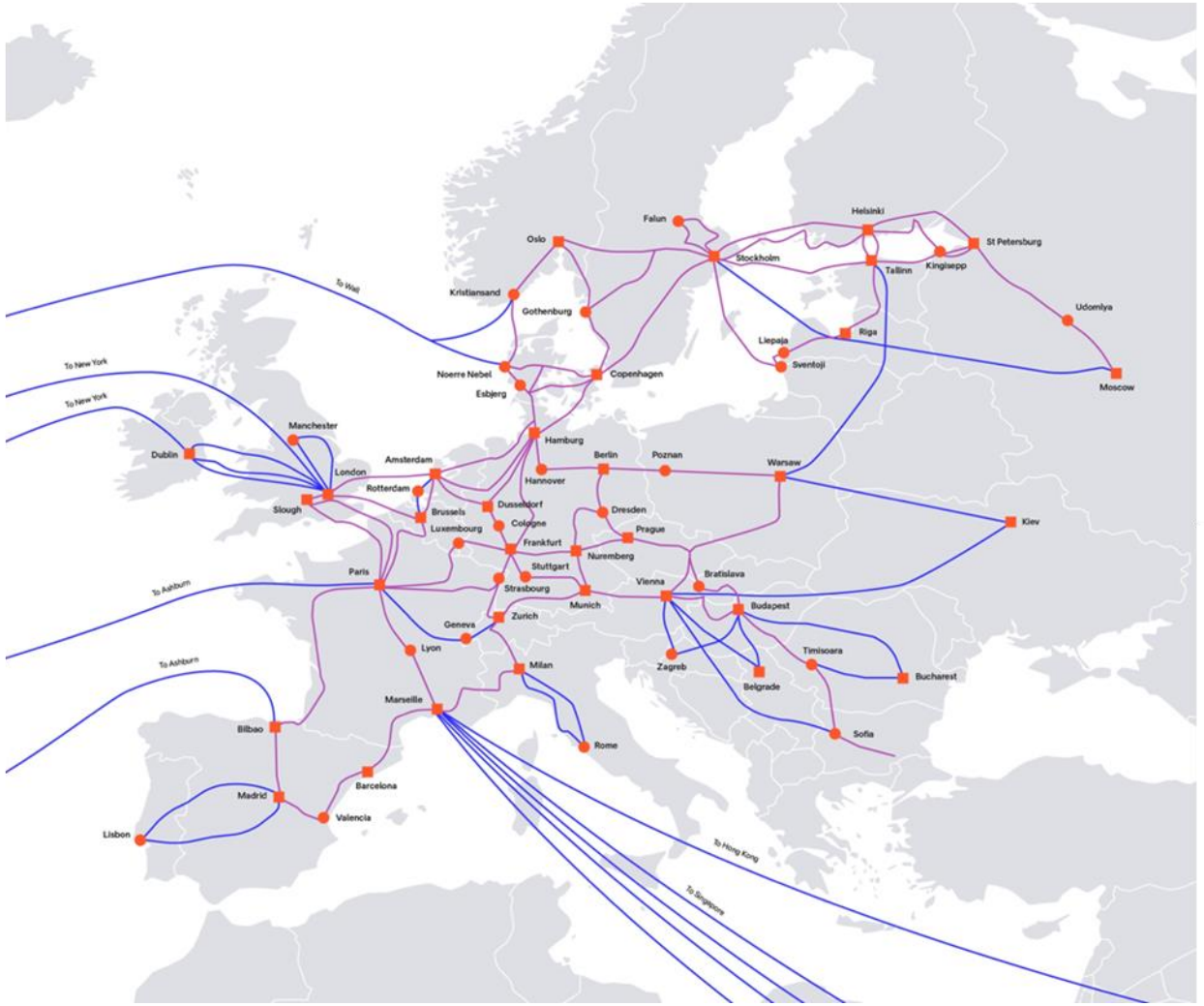
OUR YEARLY REPORT WILL GIVE YOU MORE...

PHYSICAL SECURITY

Arelion

ALMOST ALL GLOBAL TRAFFIC RUNS IN FIBER CABLES

- Ca 95% of the intercontinental traffic runs in sea cables crossing the world
- Almost all international and national traffic runs in fiber cables
  - Underground
  - Electrical power lines
- Our industry have historically been extremely transparent with where these cables are located
- Several incidents the last couple of years will definitely change this



THE BALTIC VIEW OF THE CHANGED GEOPOLITICAL SITUATION

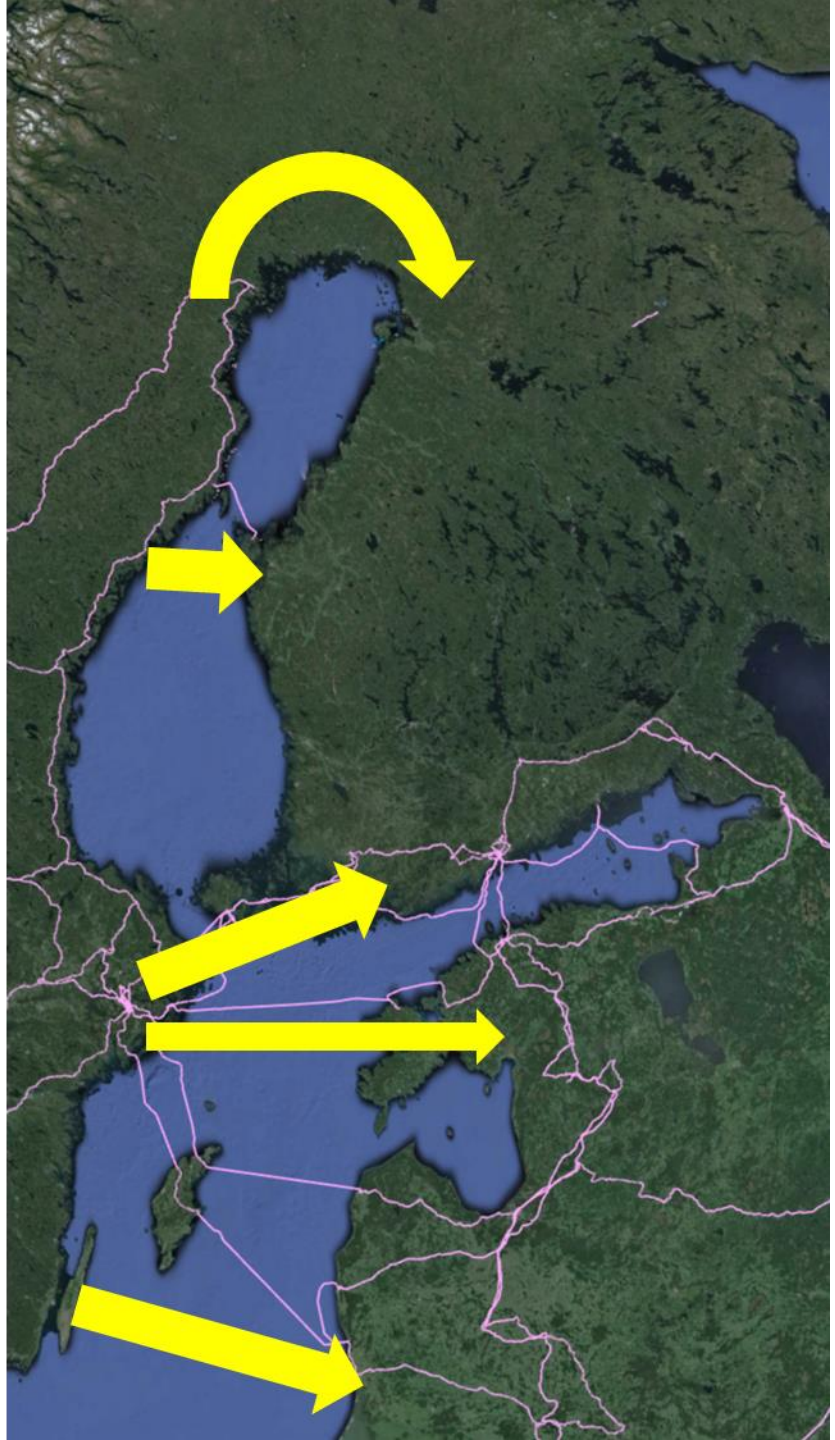
- With the war in Russia far to close there has been an increased interest among Nordic and Baltic Operators including Enterprises to increase network resilience

- In October 2023 we experienced an outage to a sea cable that has been deemed as sabotaged by the media (one of 4 cables/pipelines damaged during 12 hours)

- The Swedish marine inform in public of increased underwater traffic in the entire Baltic sea

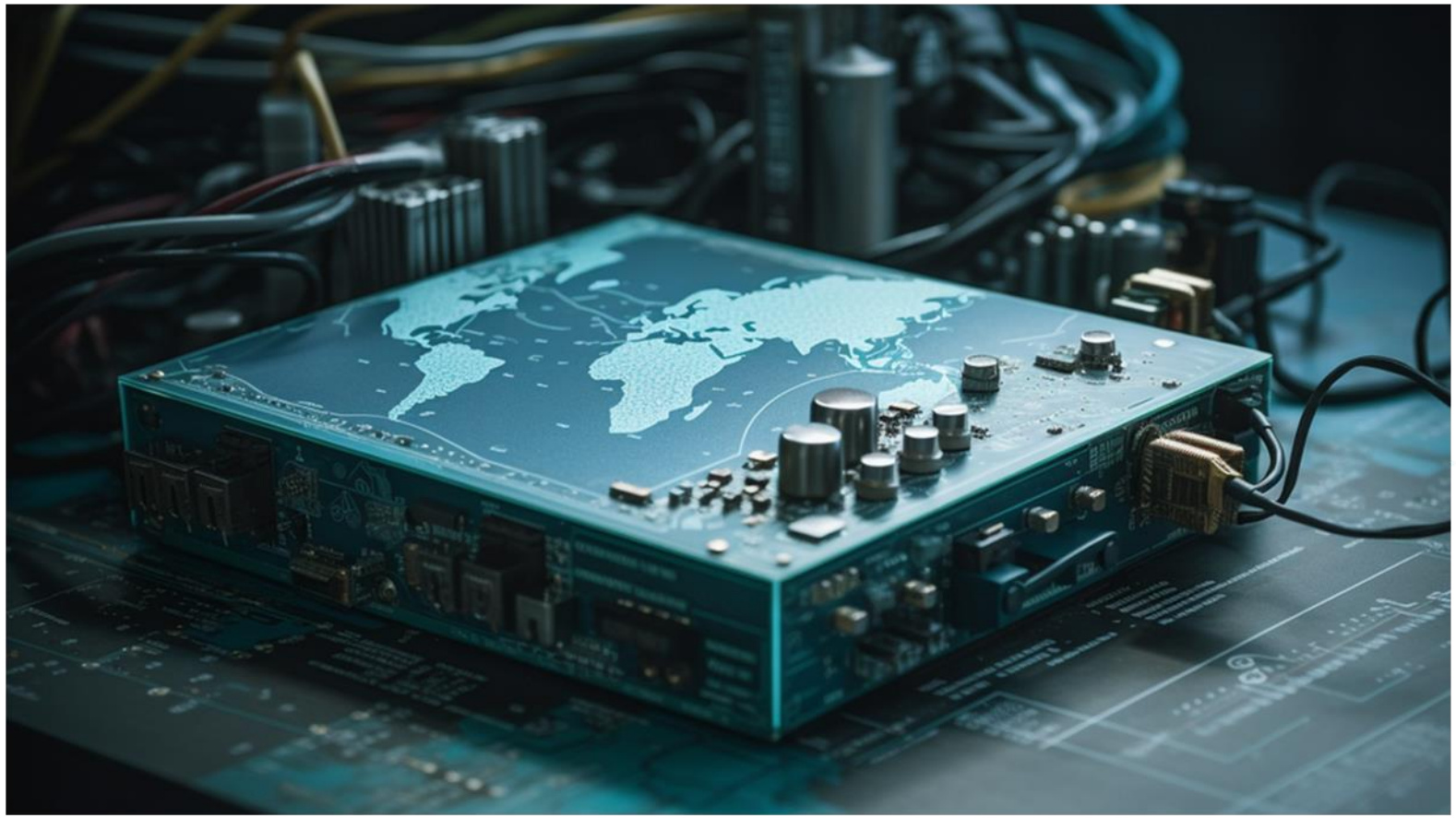
AND THEREFORE AN INCREASED INTEREST IN NEW TRAFFIC ROUTES

- A lot of new plans are under development to increase the number of cables thus also the resilience in this area
- Geographical diversity is more important than shortest route between key end points
- Having up to four routes between your end points do no longer seem unrealistic
- New funding may be available from new sources



SUMMARY

- Traffic is still growing
- New demand is hopefully around the corner
- DDoS attacks are unfortunately still an issue in the Internet world
- The Internet community that we are a big part of is increasingly working together to fight the cyber criminals
- Physical security is the next focus area for all Operators



Thank you!

Arelion