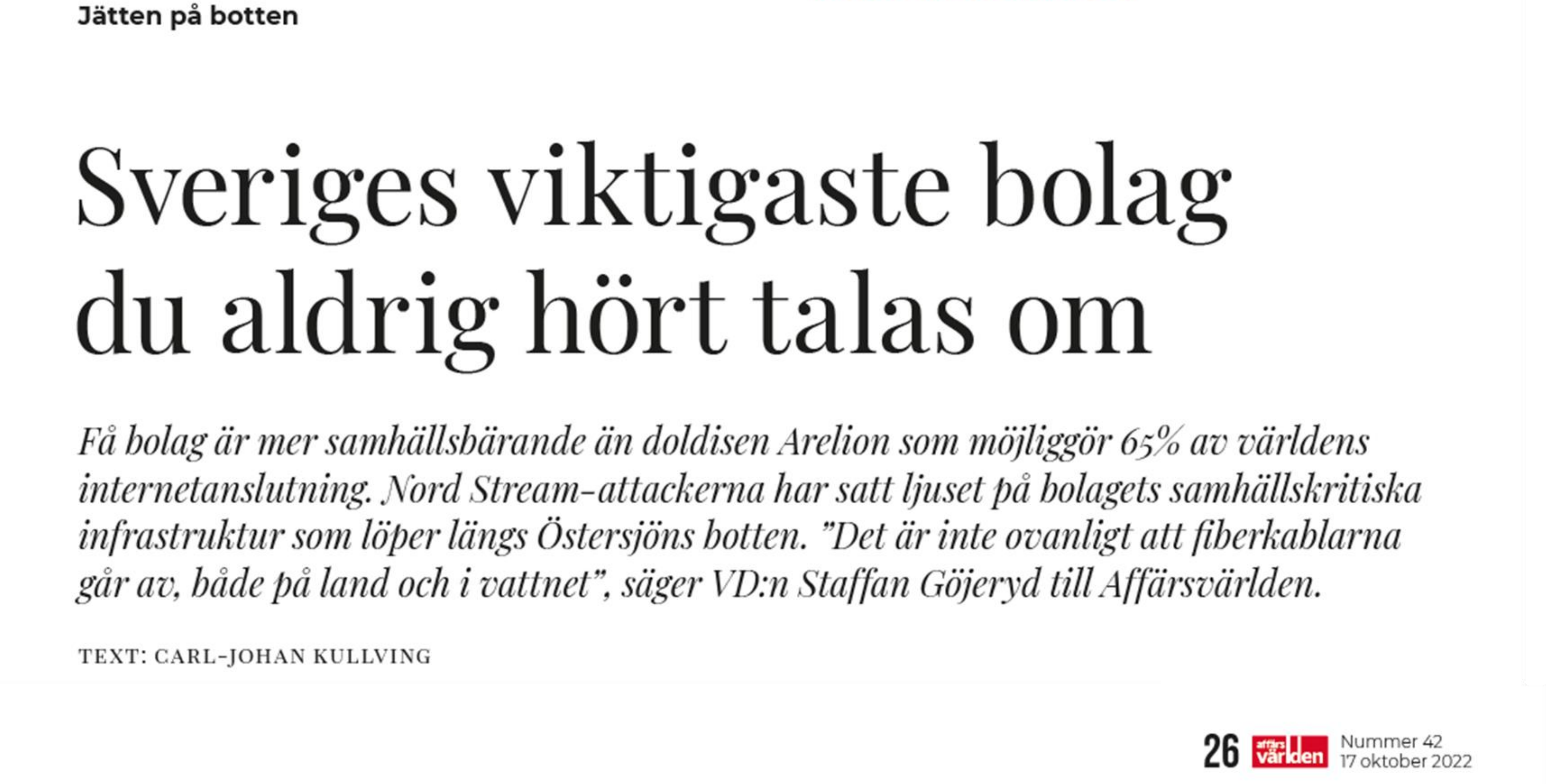
Arelion and our security work

Mattias Fridström

Vice President & Chief Evangelist

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



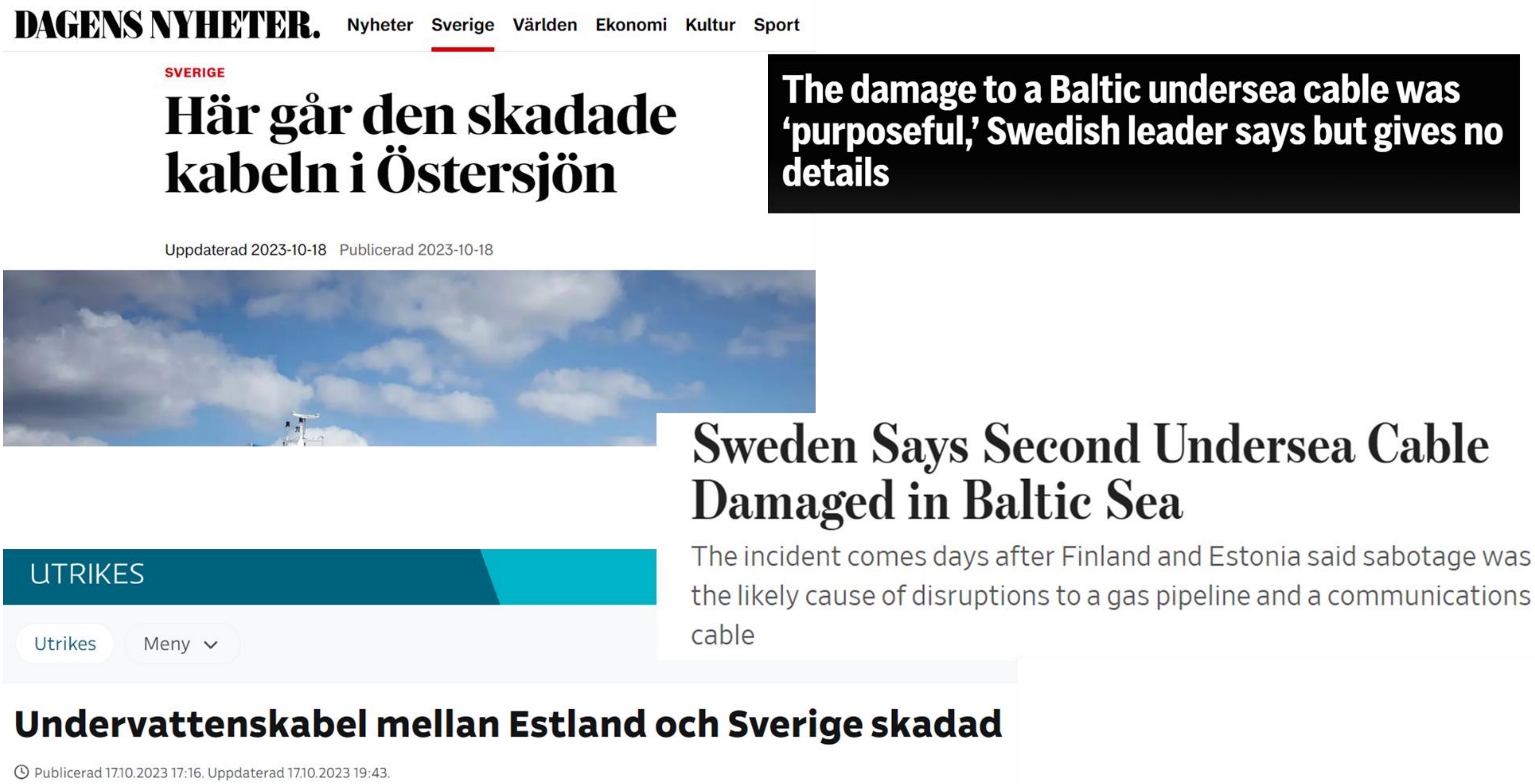
Jätten på botten

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

26 affärs världen Nummer 42
17 oktober 2022



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

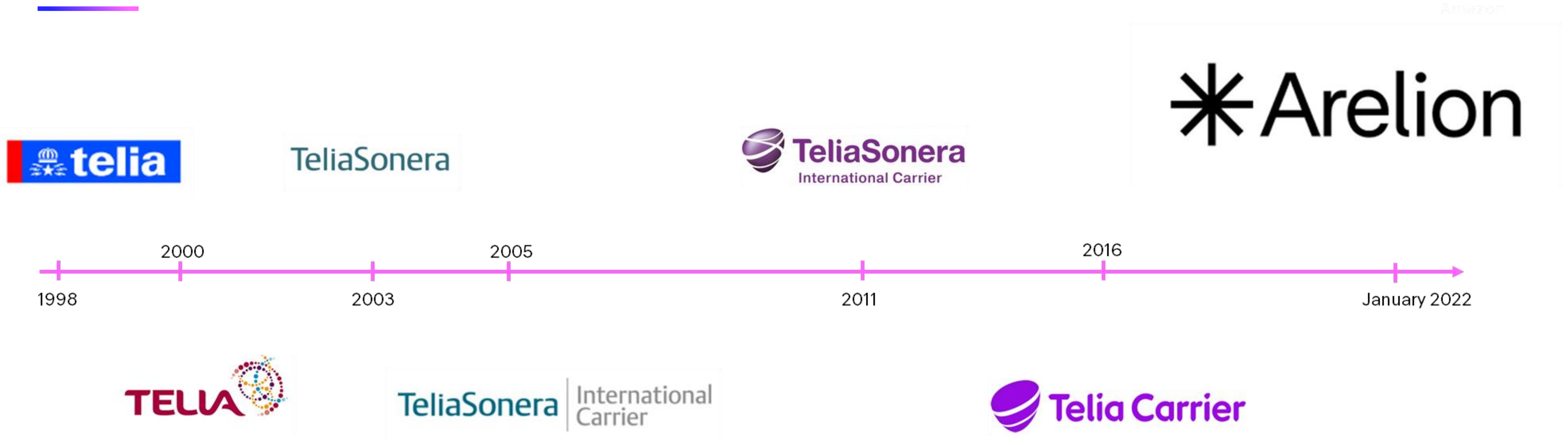
UTRIKES

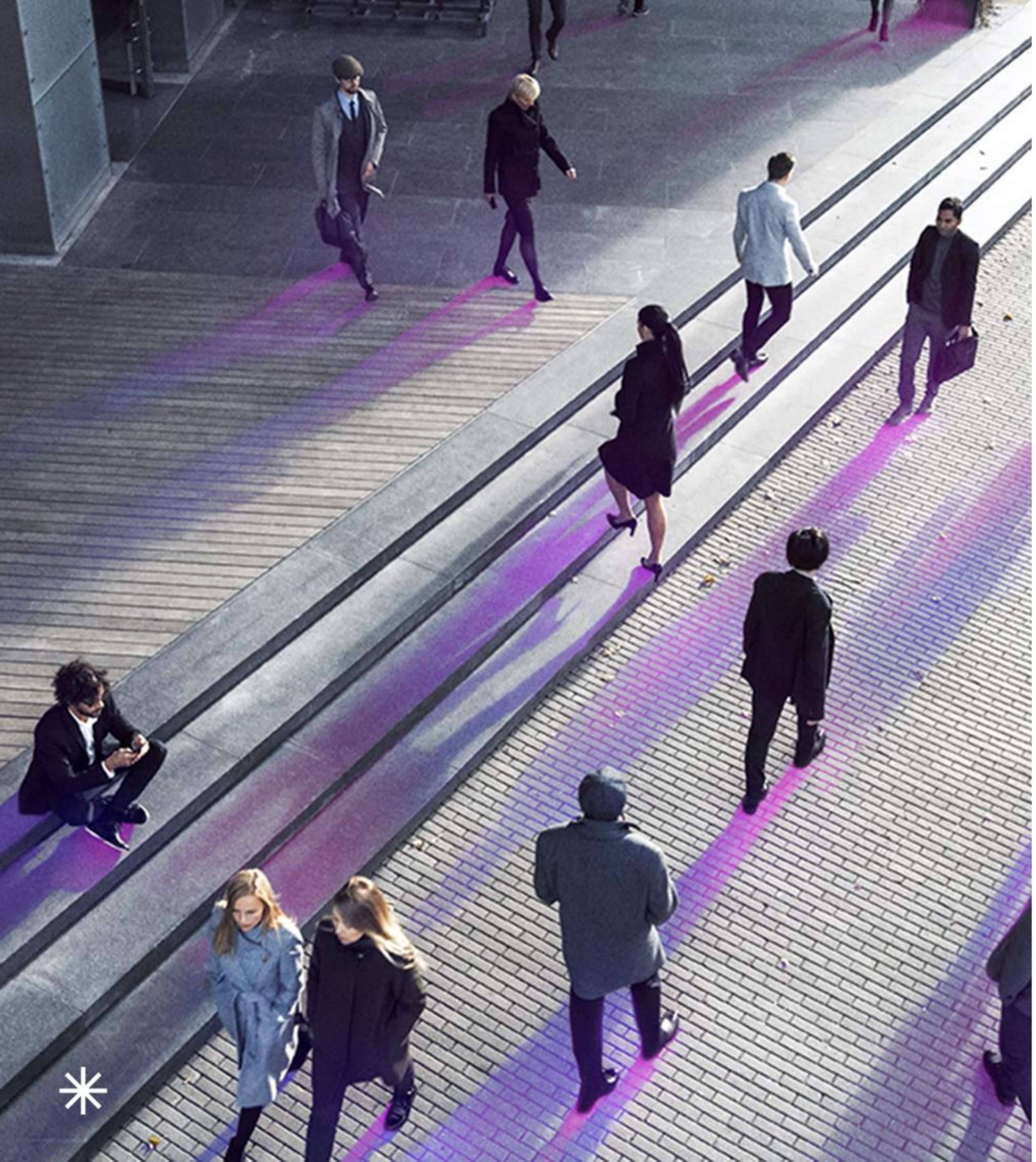
Utrikes Meny ⌄

Undervattenskabel mellan Estland och Sverige skadad

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

ARELION – SAME COMPANY BUT MANY DIFFERENT NAMES





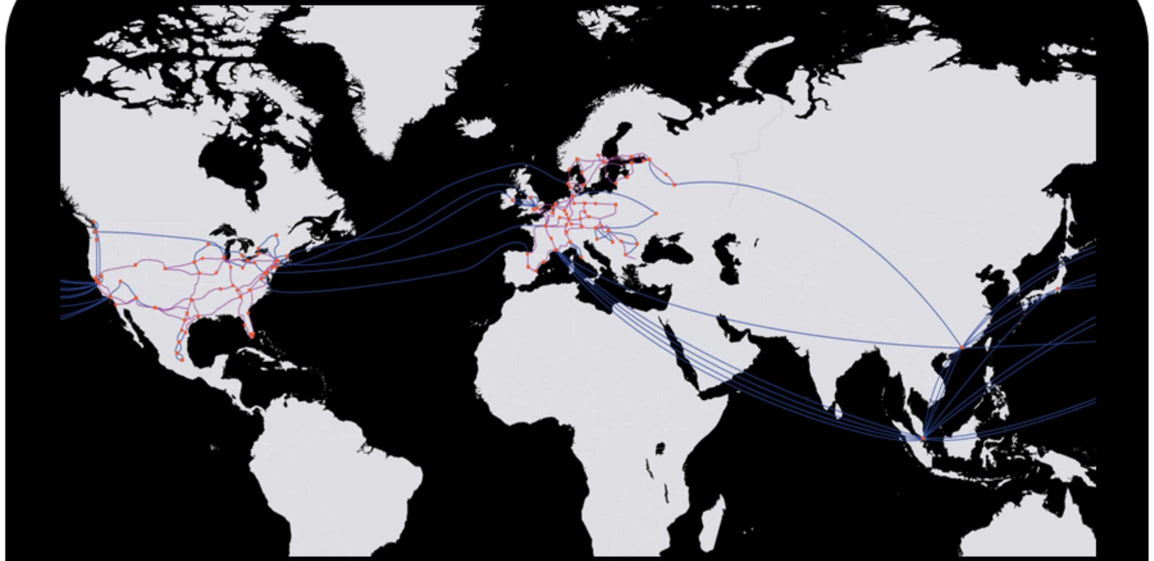
STRONG FOUNDATION FOR GLOBAL EXPANSION

As of June 1, 2021 Telia Carrier, now rebranded as Arelion, is fully owned by Polhem Infra.

- Owned by some of the largest public Swedish pension funds, Polhem Infra is a responsible and financially strong company which focuses on infrastructure assets crucial to society, including energy, transport, renewables and digital infrastructure.
- With extensive experience of investing in, and building up, profitable unlisted companies, Polhem Infra's goal is to be a stable, responsible and long-term owner.
- Following divestment, Arelion continues to be Telia Company's provider of wholesale connectivity and partner for global enterprise networking.

ARELION TODAY

ARELION IS THE BACKBONE OF YOUR BUSINESS



75,000 km of optical fiber

Customers in 125+ countries

69% Global Internet routes

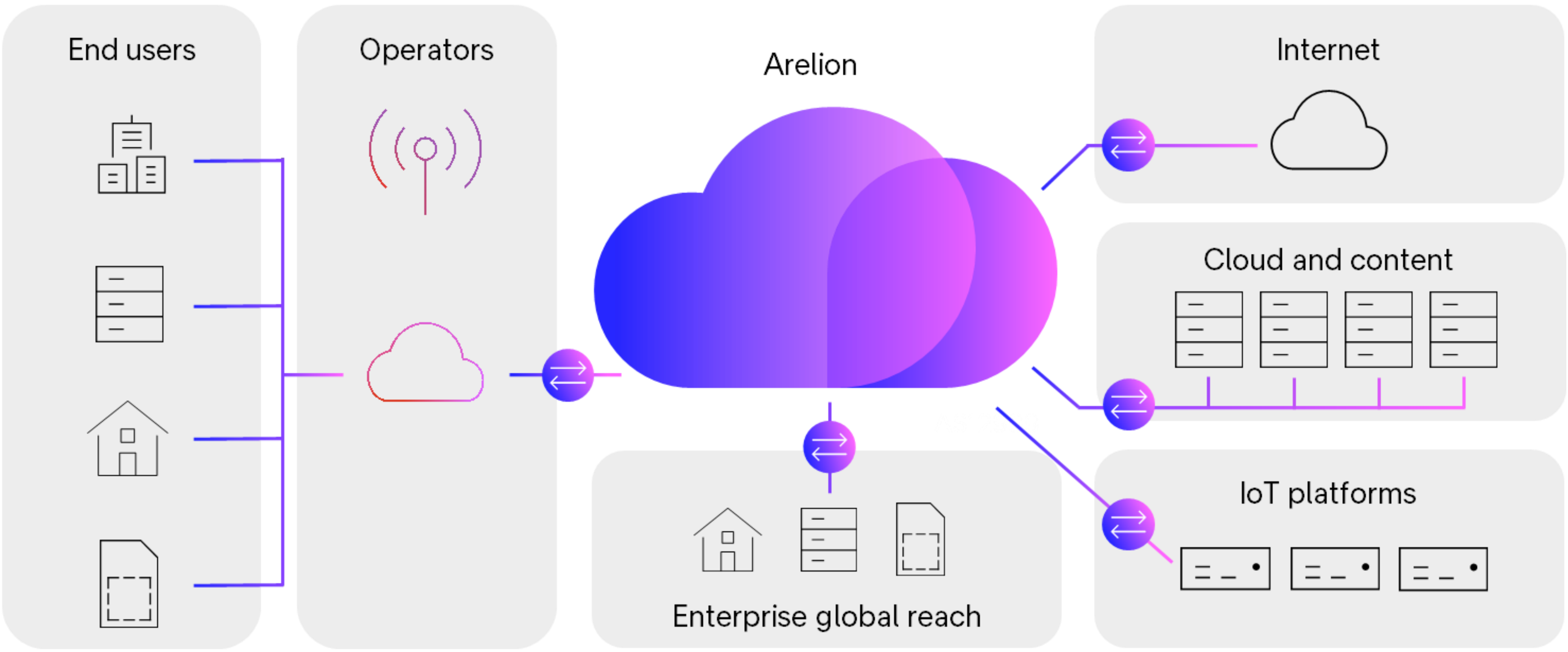
AS1299 est. 1993

2,750 Customers

72 Net Promotor Score

World's #1 Internet Backbone

CONNECTING OPERATORS, CONTENT PROVIDERS AND GLOBAL ENTERPRISES



EARNING THE TRUST OF THE MOST DEMANDING CUSTOMERS IN THE WORLD

Examples of potential customers

CLOUD & CONTENT PROVIDERS

f VALVE Google

Microsoft Tencent 腾讯 Alibaba Group 阿里巴巴集团

OVH.com amazon ACTIVISION BLIZZARD

fastly SAMSUNG Akamai in X

✳Arelion

OPERATORS

vodafone BT TELECOM ITALIA Rostelecom

LIBERTY GLOBAL PLDT TDC

gtt TELMEX altice Telia

Türk Telekom telenor HE

Telefonica orange™ T Deutsche Telekom

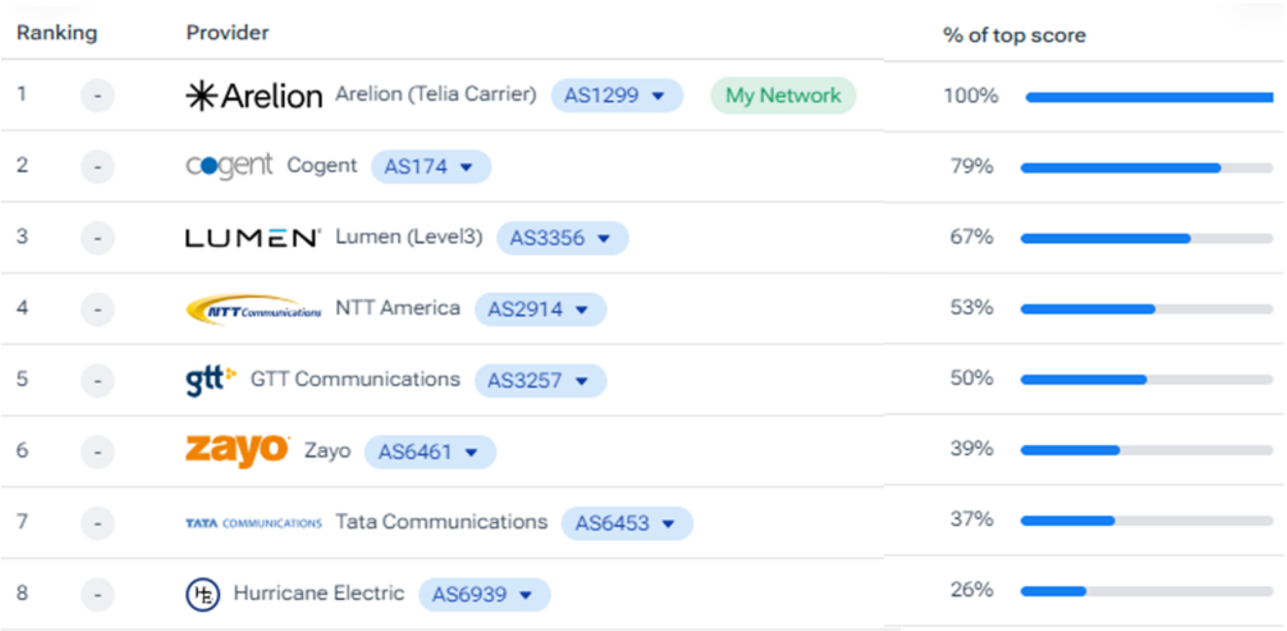
- Connectivity is business critical
- Traffic constantly increasing
- Both global and local

- Connectivity is business critical
- Ease of doing business is key
- Stable, more predictable environment

CURRENT INTERNET BACKBONE RANKING

- Kentik is currently providing a ranking (KMI rankings) of all networks forming the Internet (ca 70,000 active networks). This ranks all networks in terms of their “importance” for Internet to work
  - Amount of traffic
  - # of connected networks
  - The importance of connected networks (# prefixes)
  - How networks are connected (transit or peering)
- The higher you're ranking the more direct connects (shorter path) you can offer to important locations on the Internet (e.g. SFDC, Akamai, Workday, Zscaler, FB, YouTube, etc.)
- The percentage on the right shows how important a network is compared to the Top ranked network (Arelion in this case)

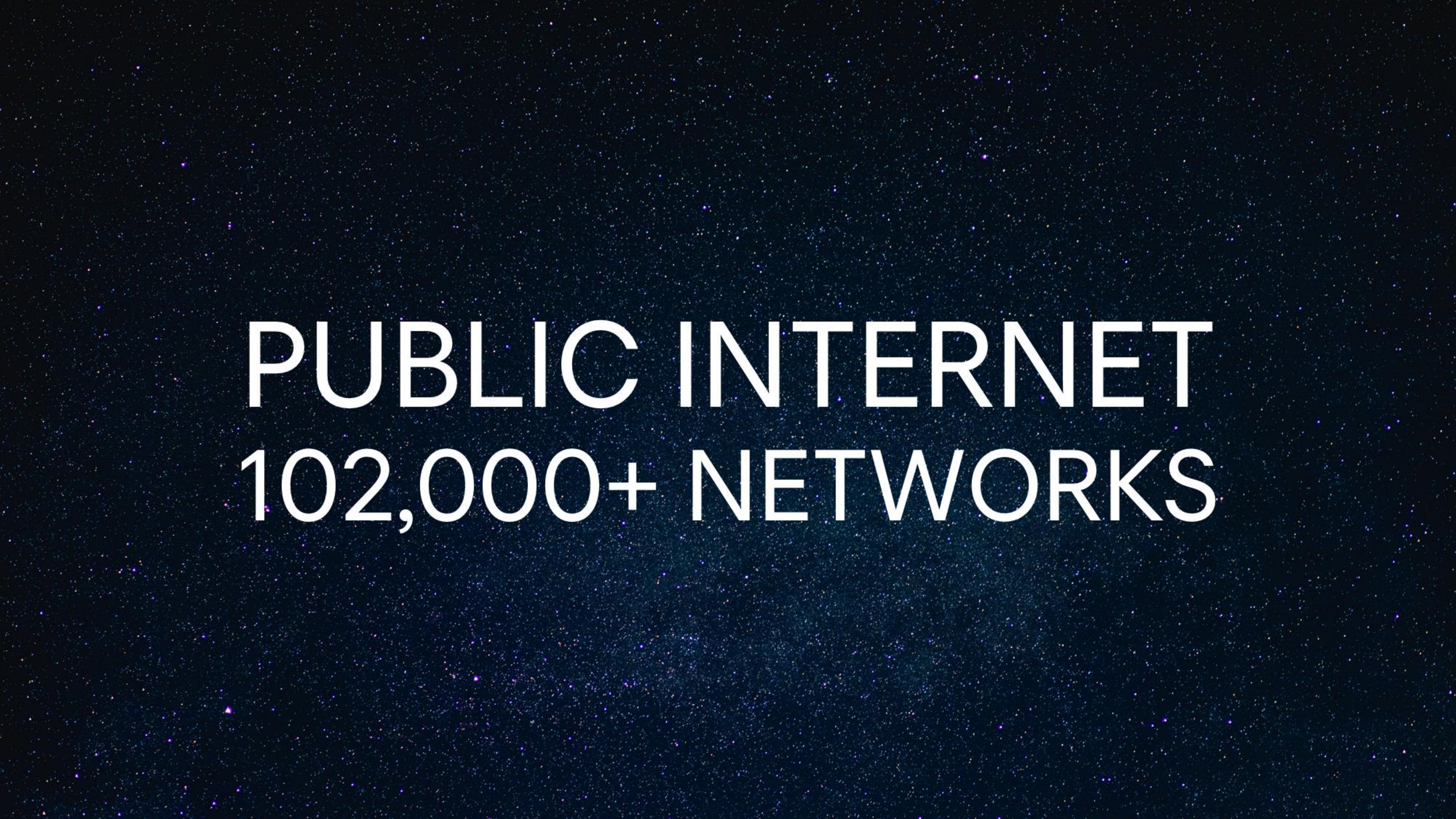
Global Networks



Ranking		Provider	% of top score
1	-	Arelion (Telia Carrier) AS1299 ▾ My Network	100%
2	-	Cogent AS174 ▾	79%
3	-	Lumen (Level3) AS3356 ▾	67%
4	-	NTT America AS2914 ▾	53%
5	-	GTT Communications AS3257 ▾	50%
6	-	Zayo AS6461 ▾	39%
7	-	Tata Communications AS6453 ▾	37%
8	-	Hurricane Electric AS6939 ▾	26%

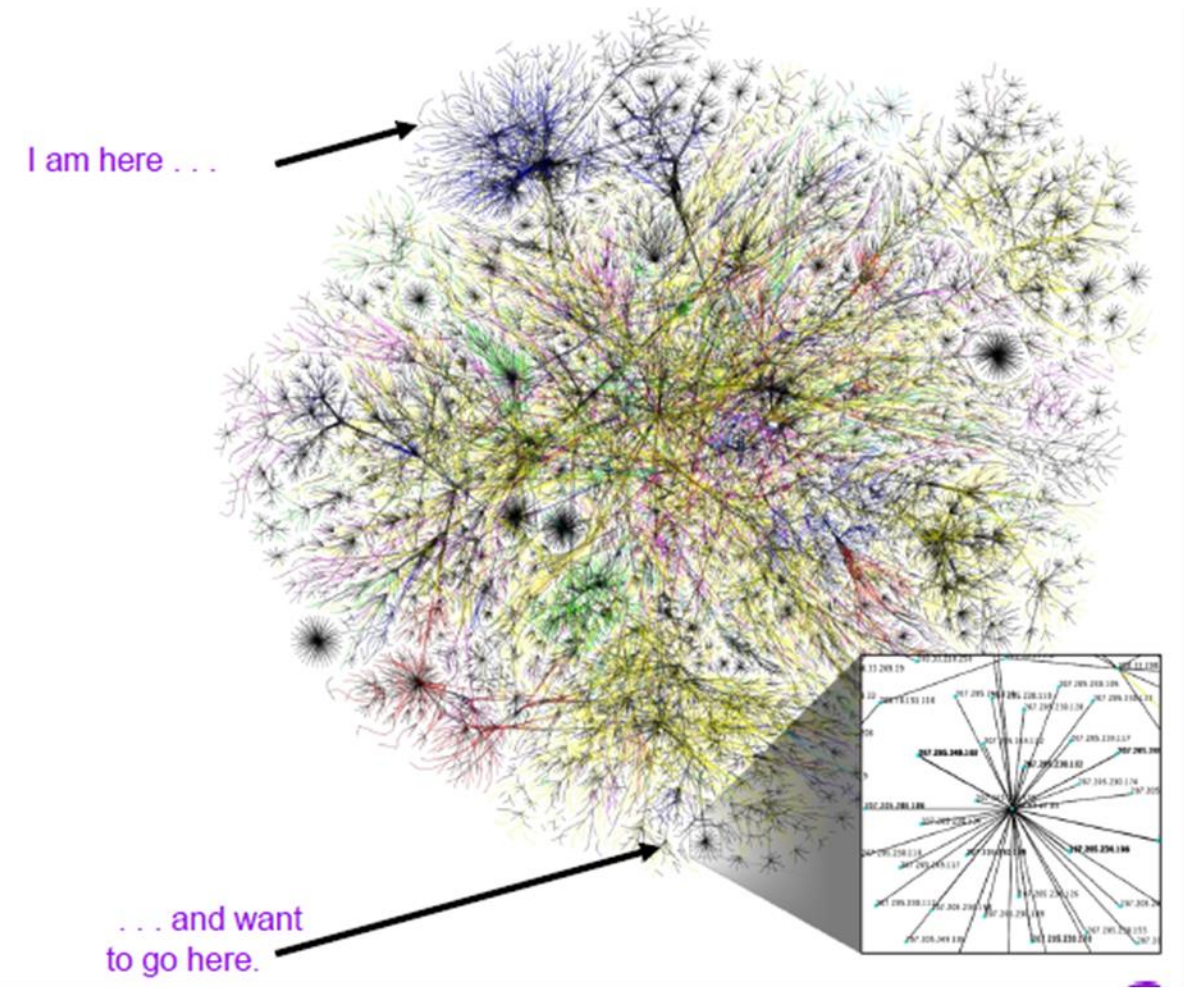
August 8, 2024

THE PUBLIC INTERNET



PUBLIC INTERNET
102,000+ NETWORKS

A BIG “TRUST BASED” NETWORK OF NETWORKS



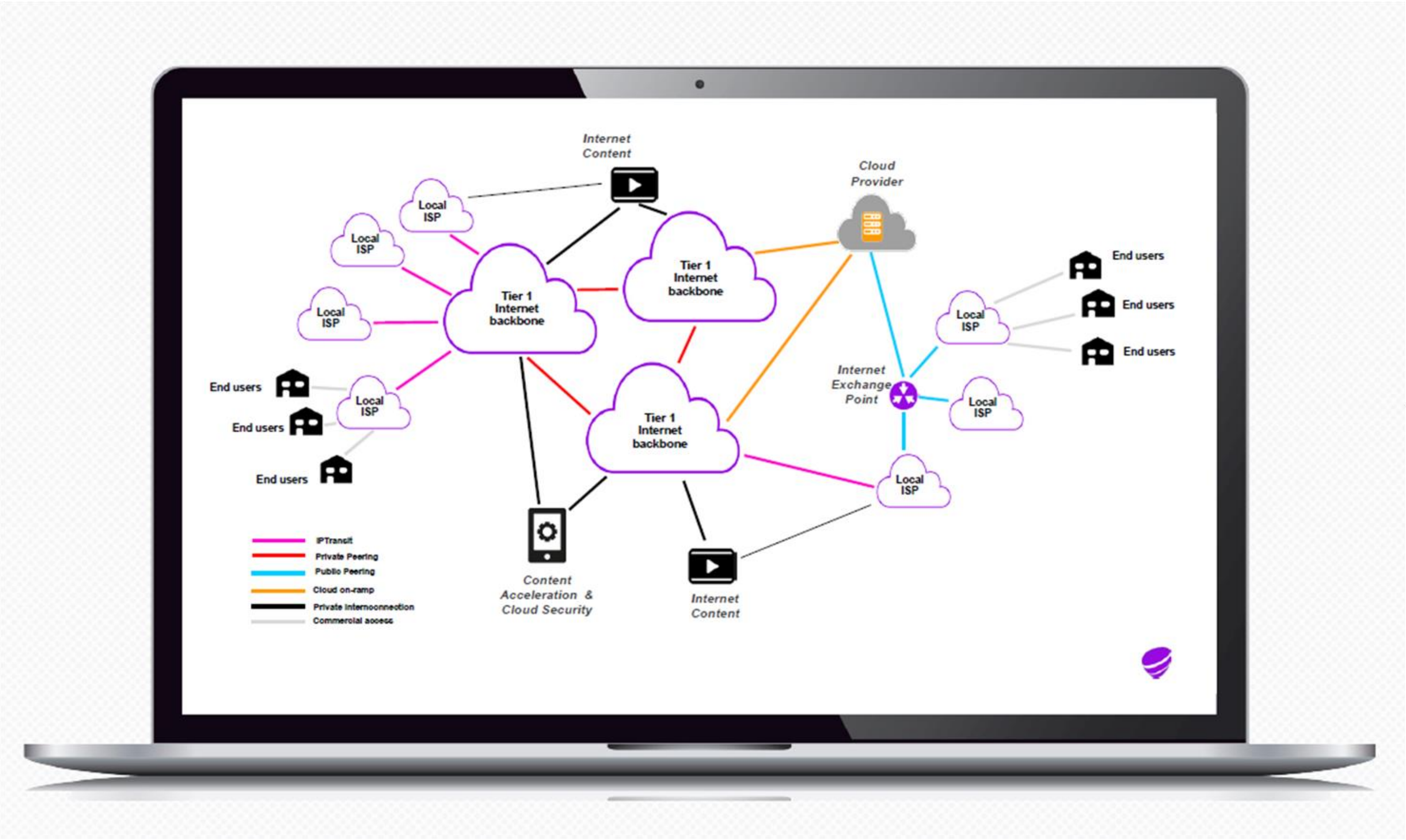
PROS

- Coverage – it's everywhere
- Price
- Supports ”cloud first” traffic patterns

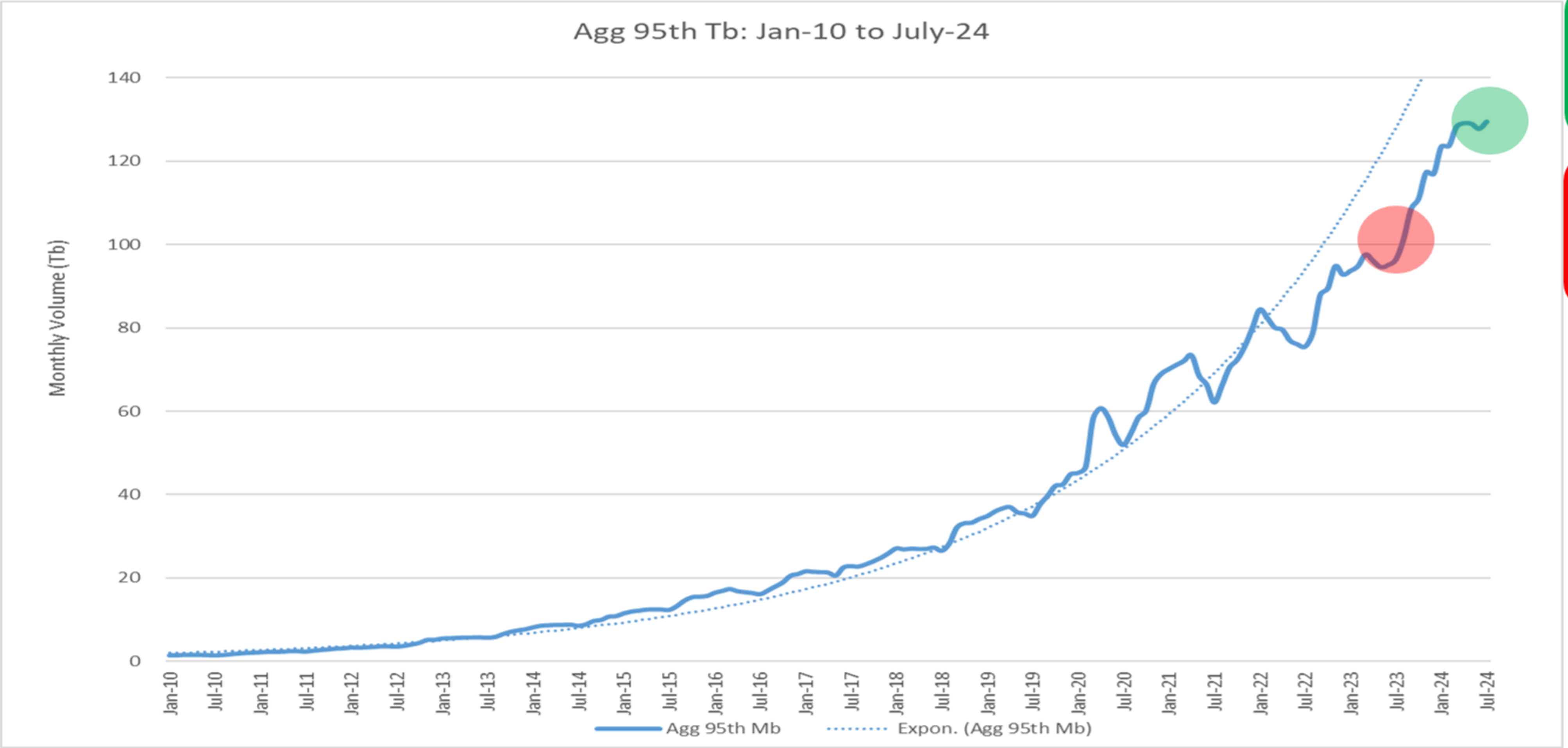
CONS

- Still best effort network
- Routing exchange based on economics not performance
- Politics, Regulations and Protectionism

WHAT FORMS THE INTERNET TODAY



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

DDoS Security
-your first line of defense

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

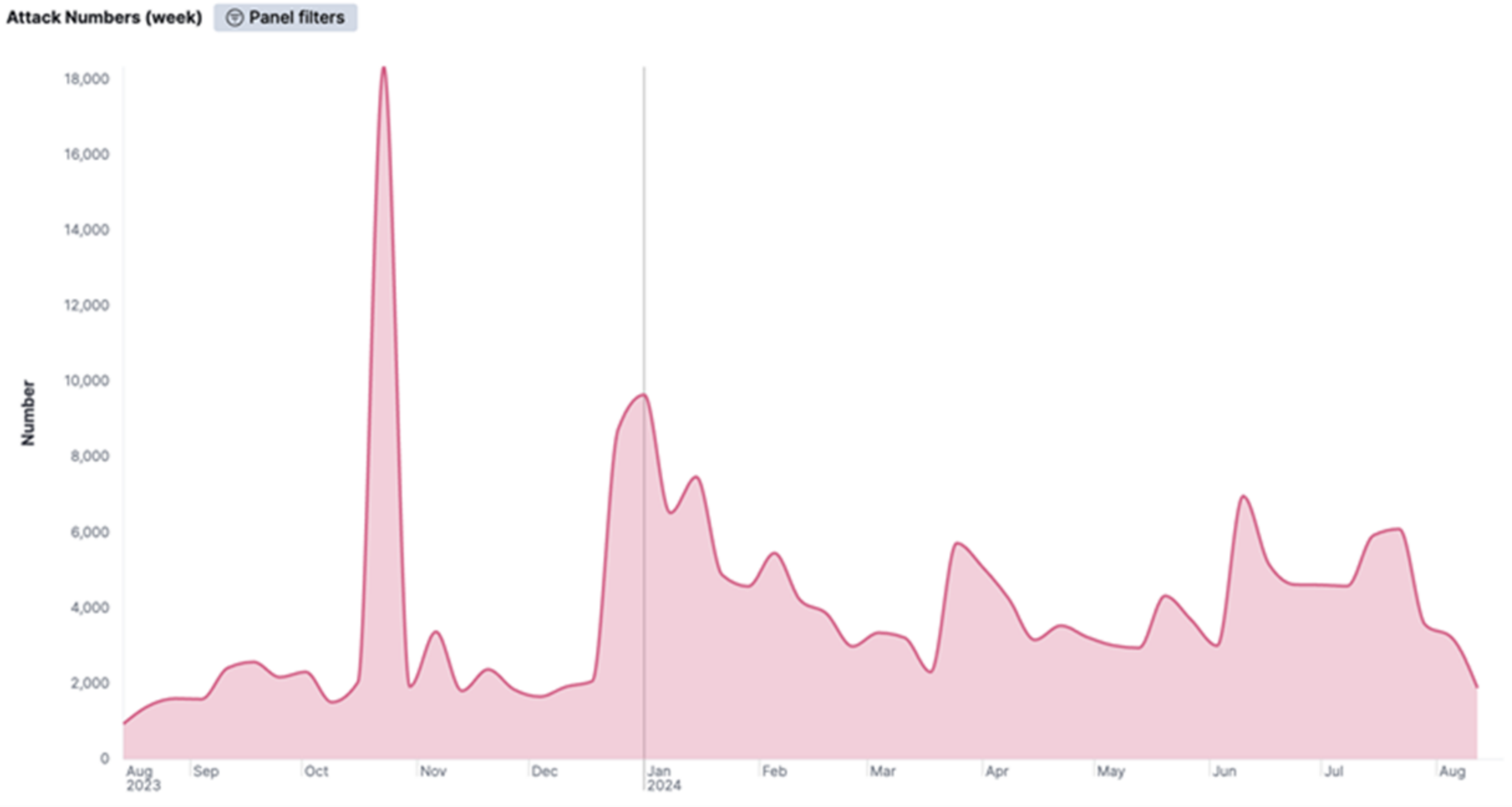
- Hackers work “smarter not harder”

Attack duration is down

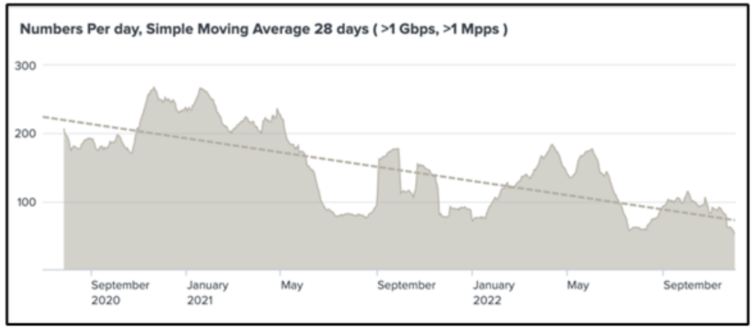
- Most likely due to that unsuccessful attacks are called off quicker

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

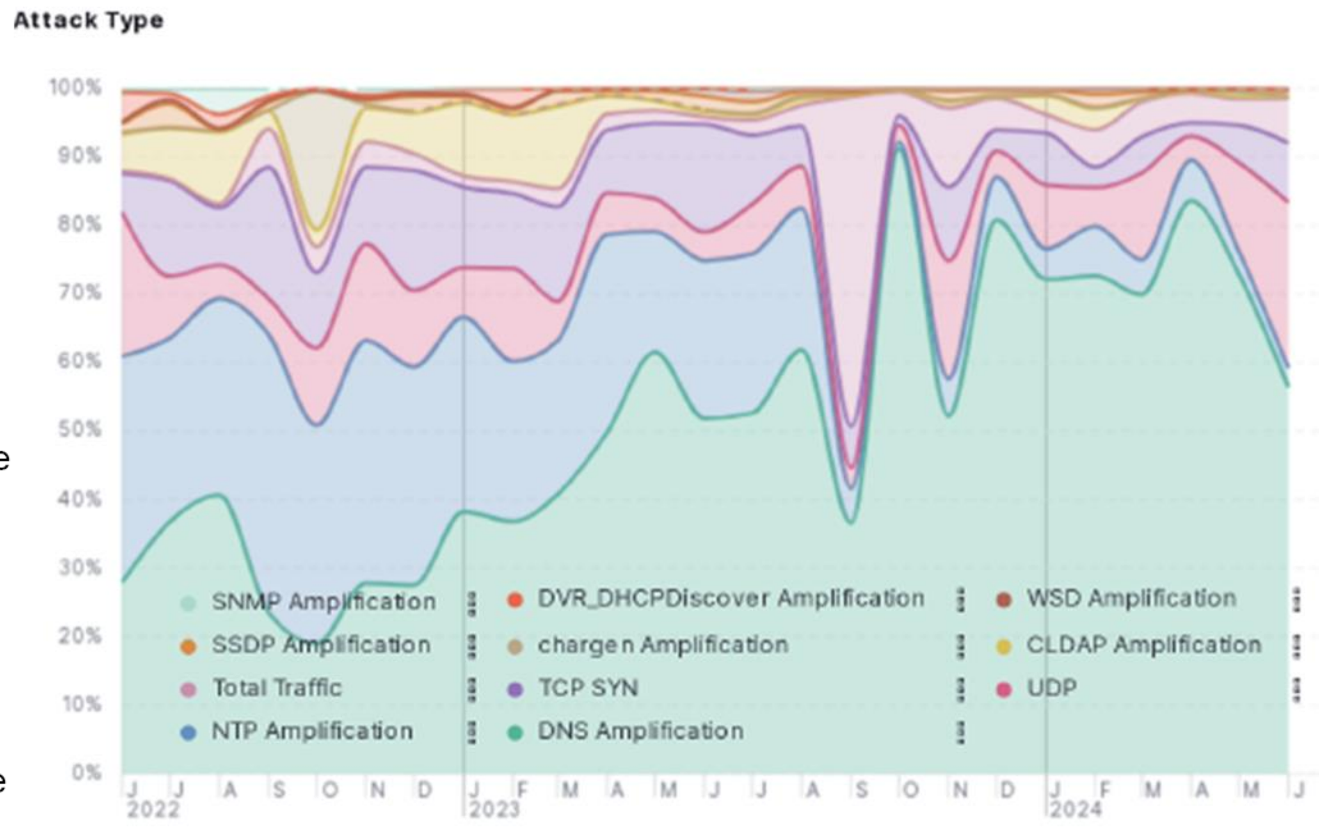


TYPE OF DDoS ATTACKS AS SEEN BY AS1299

- 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



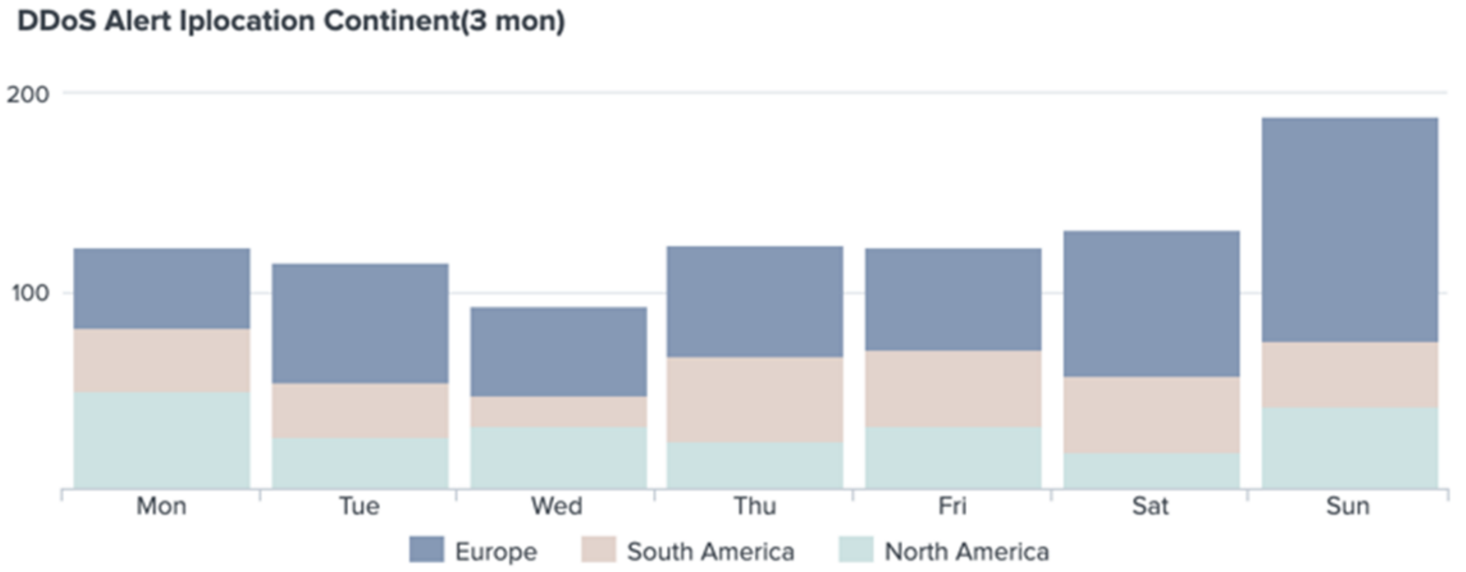
Almost **80%** of the attacks are DNS amplification attacks

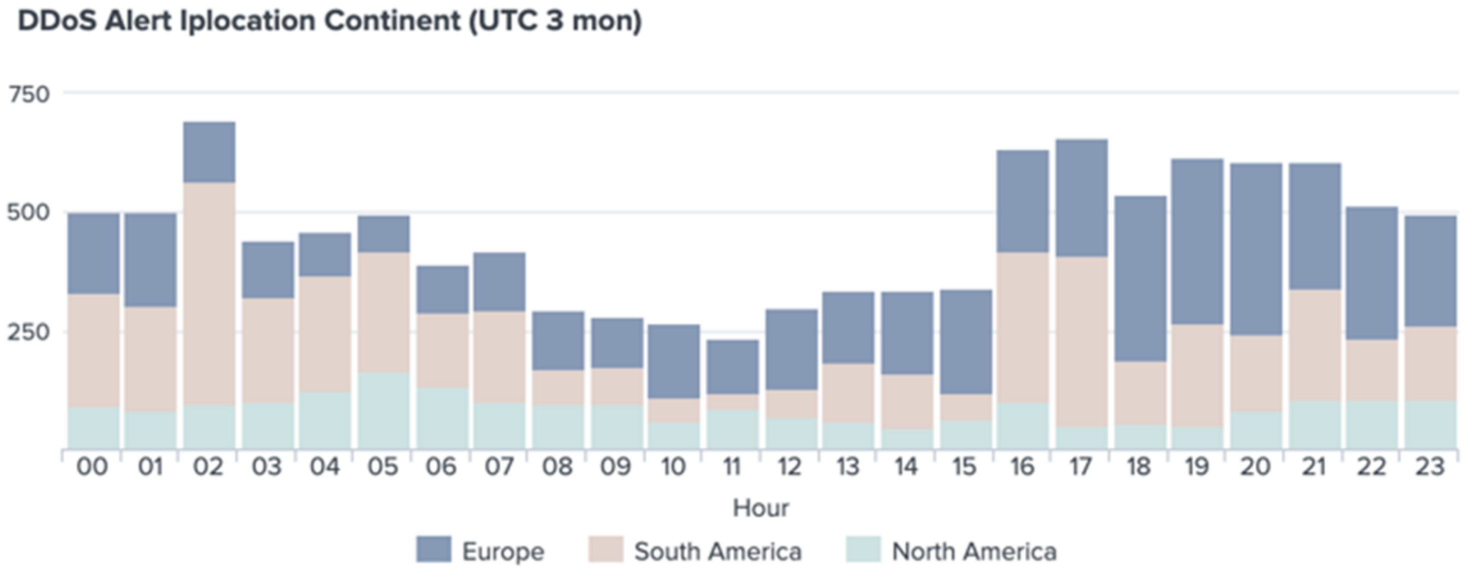
THE MOST COMMON CUSTOMER ATTACK

- 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

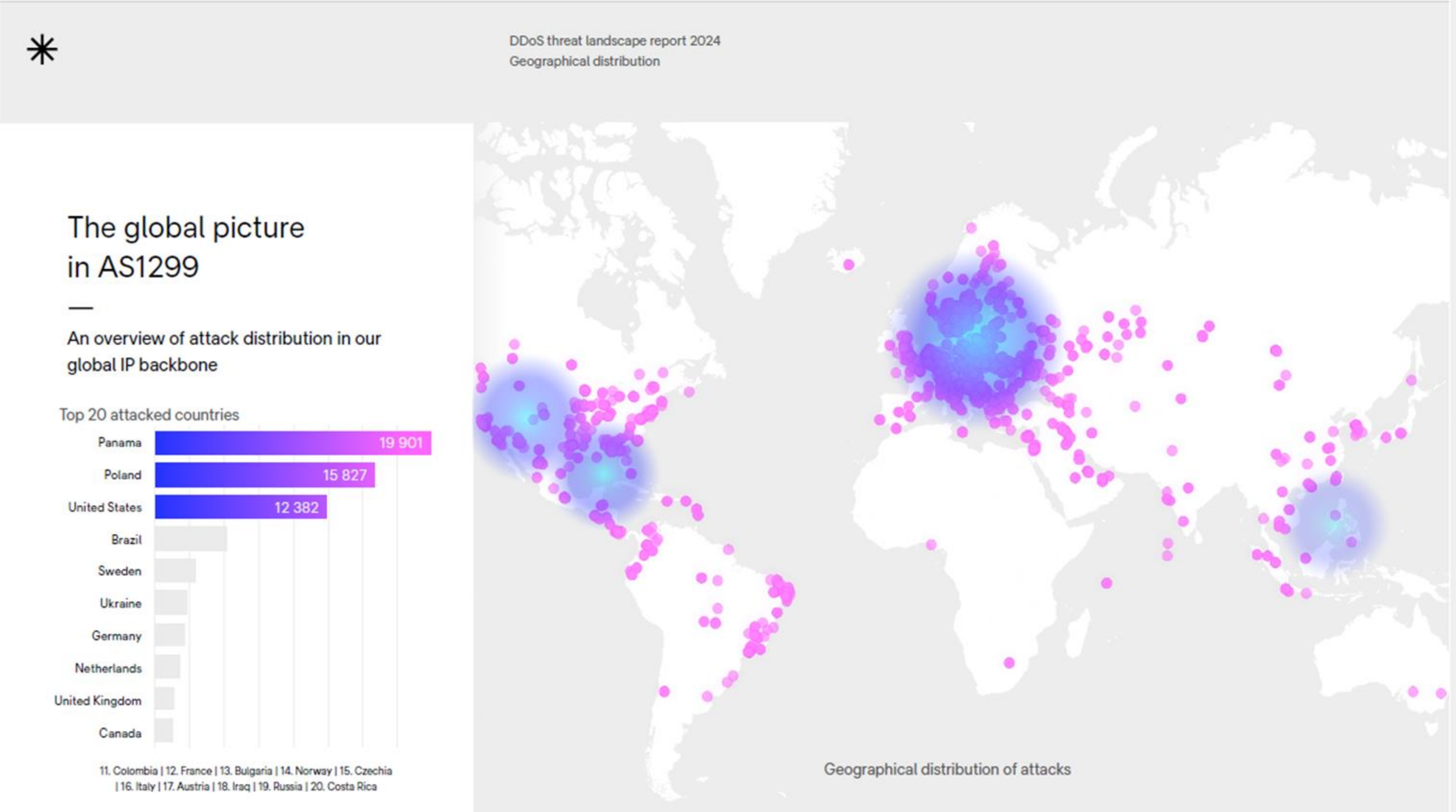
WHEN DO THE DDoS ATTACKS OCCUR

- 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 threat landscape report 2024
Geographical distribution

The global picture in AS1299

—

An overview of attack distribution in our global IP backbone

Top 20 attacked countries

Panama	19 901
Poland	15 827
United States	12 382
Brazil	
Sweden	
Ukraine	
Germany	
Netherlands	
United Kingdom	
Canada	

11. Colombia | 12. France | 13. Bulgaria | 14. Norway | 15. Czechia | 16. Italy | 17. Austria | 18. Iraq | 19. Russia | 20. Costa Rica

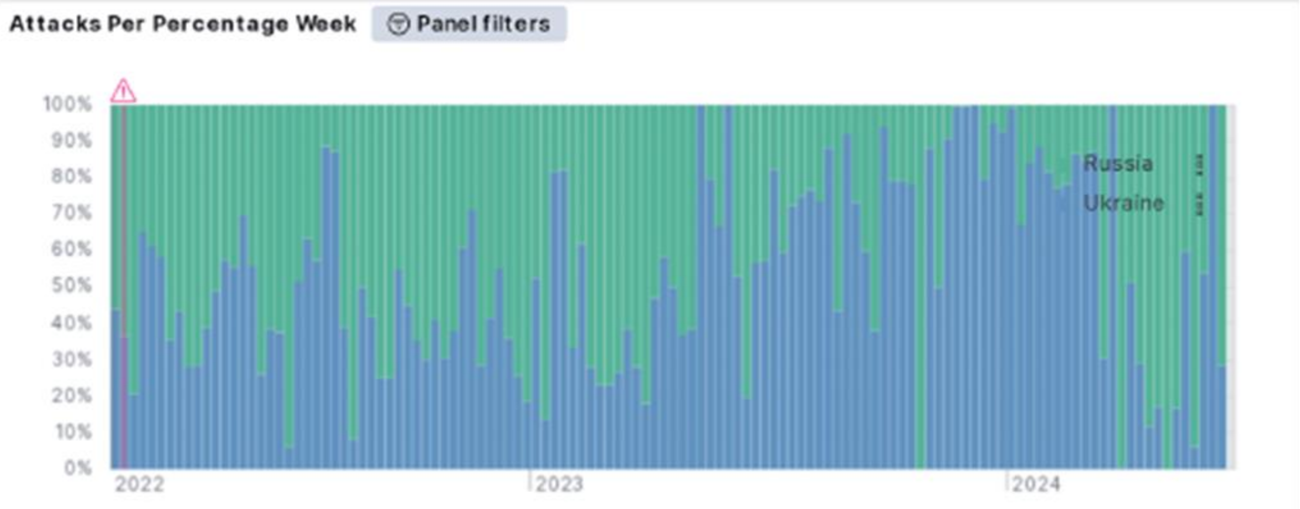
Geographical distribution of attacks

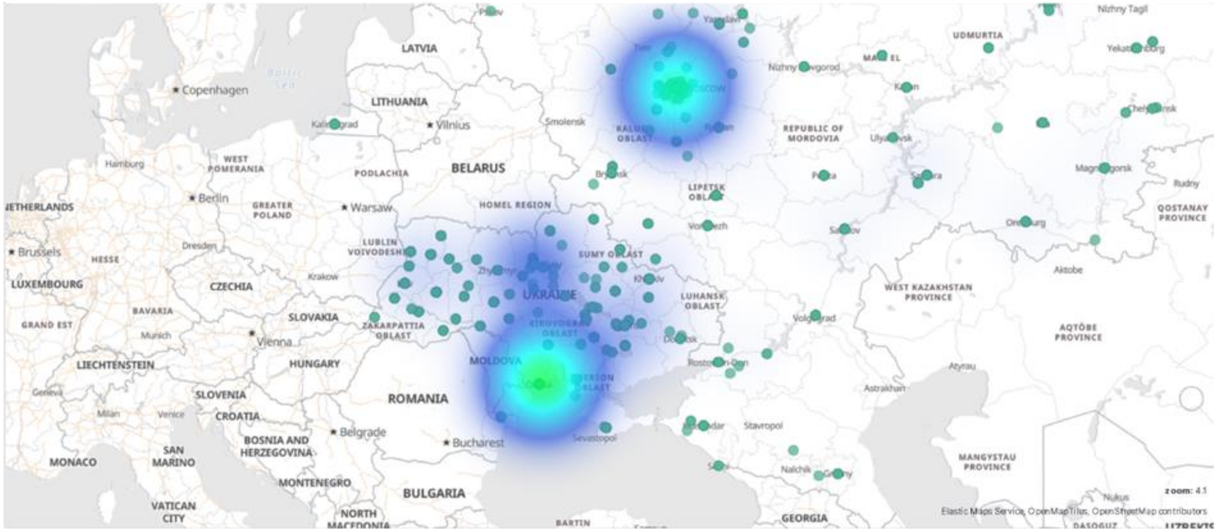
DDoS ATTACKS – RUSSIA AND UKRAINE INSIGHT

- 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

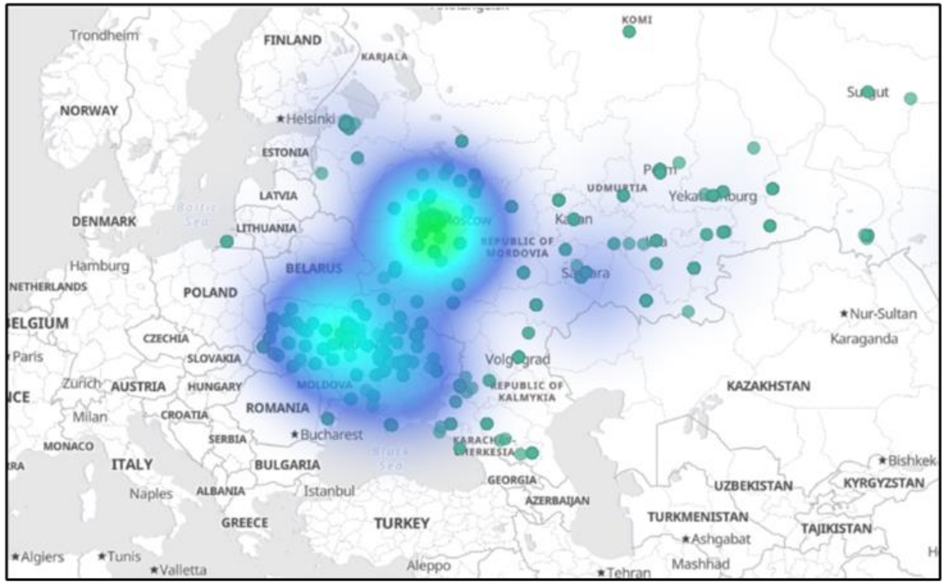
🟦 Blue = Attack on Ukraine



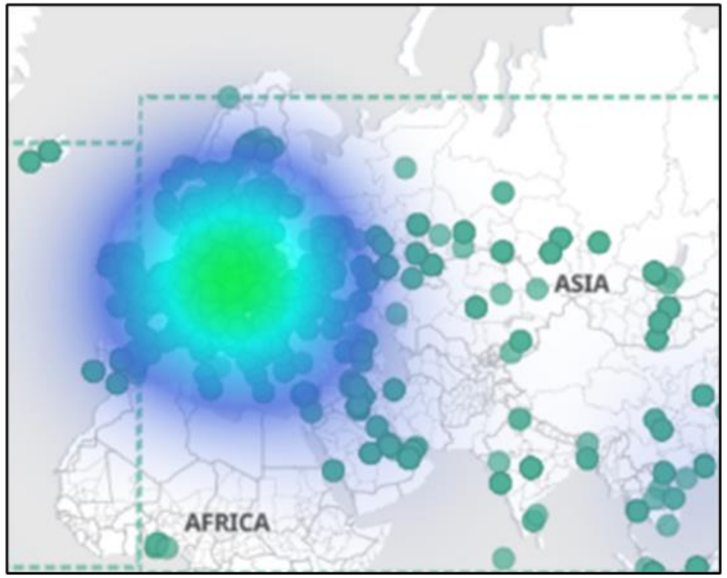


RUSSIA AND UKRAINE – CHANGE OF ATTACK PATTERNS

- 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



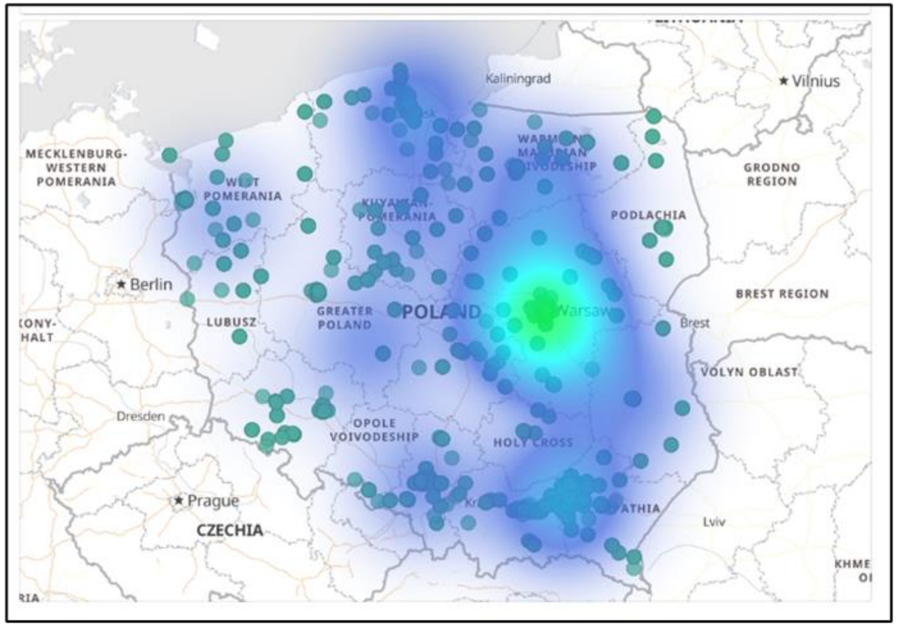
Summer 2022



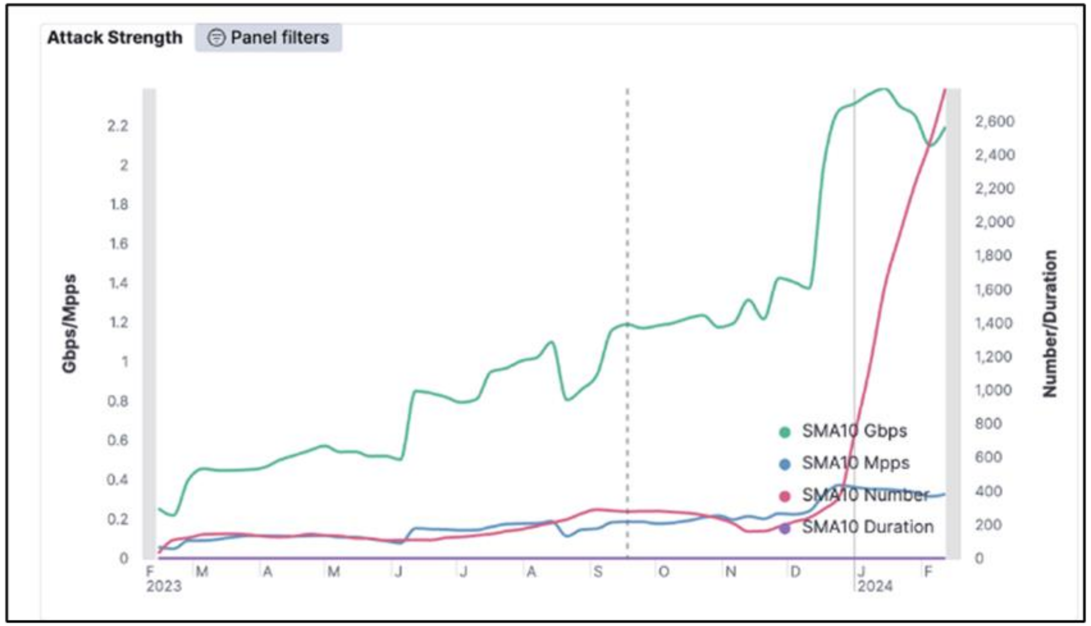
Summer 2024

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…

Key backbone security trends

DDoS threat landscape report 2024

Arelion

PHYSICAL SECURITY

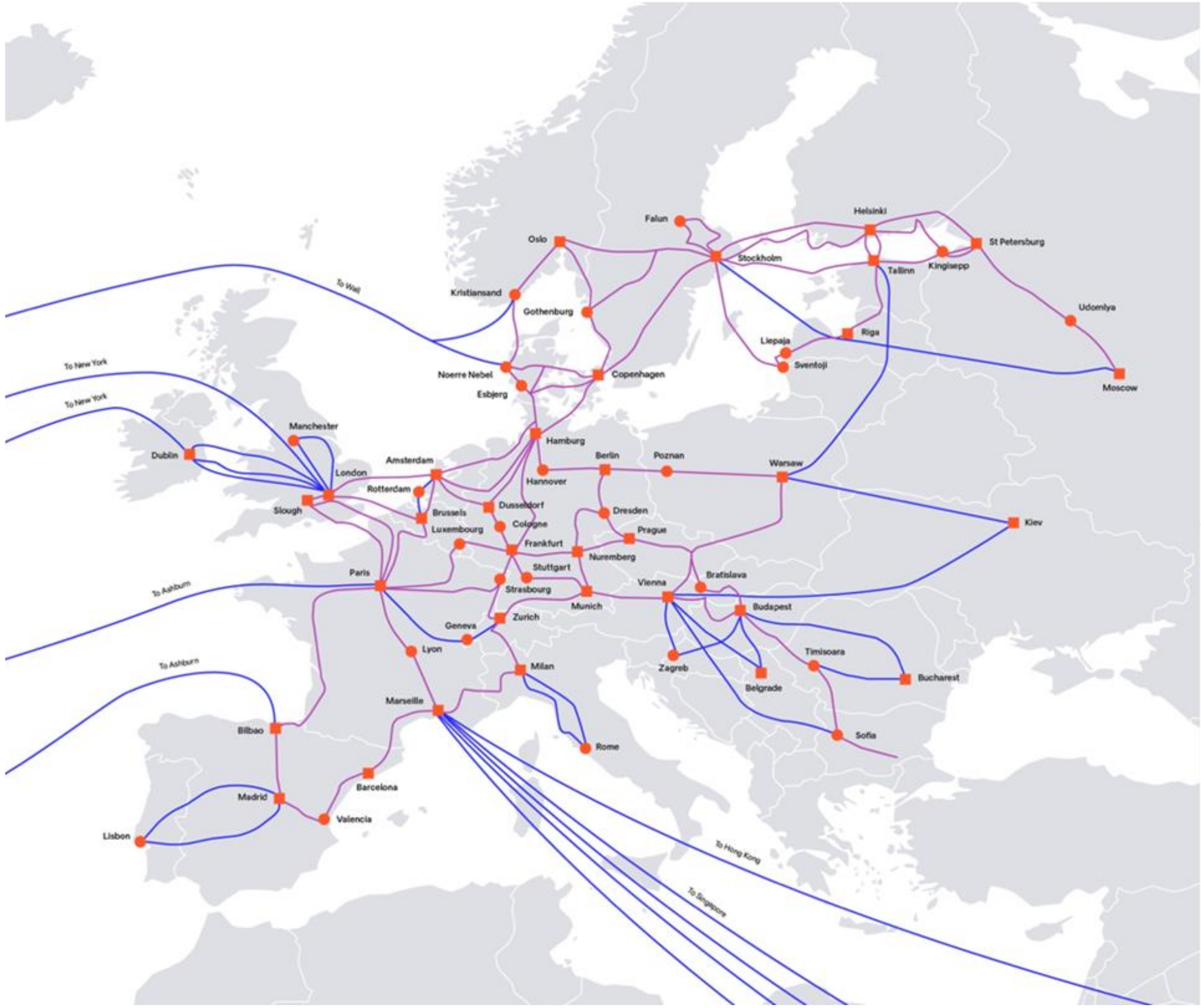
ALMOST ALL GLOBAL TRAFFIC RUNS IN FIBER CABLES

- 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

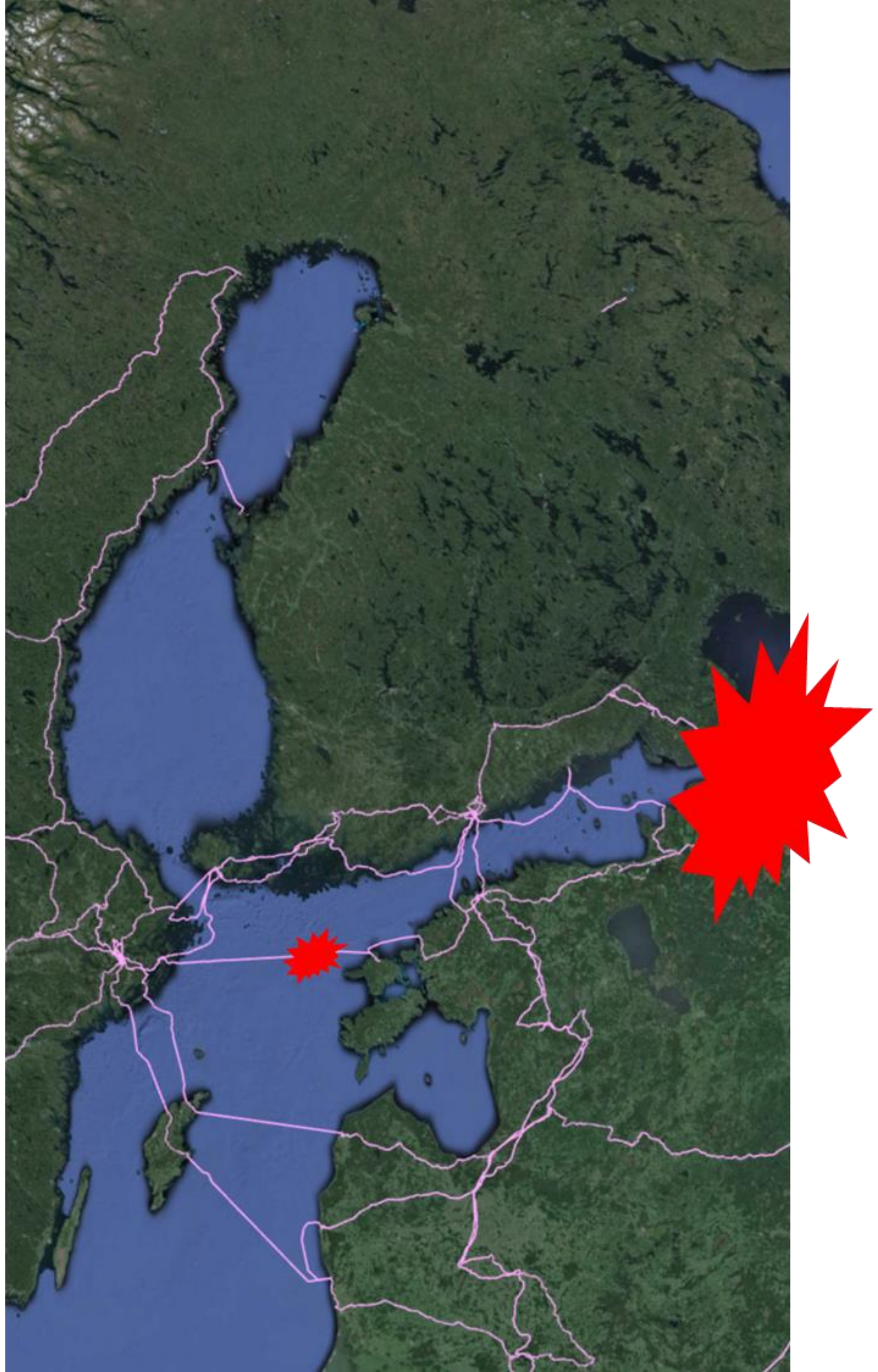


THE BALTIC VIEW OF THE CHANGED GEOPOLITICAL SITUATION

- 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



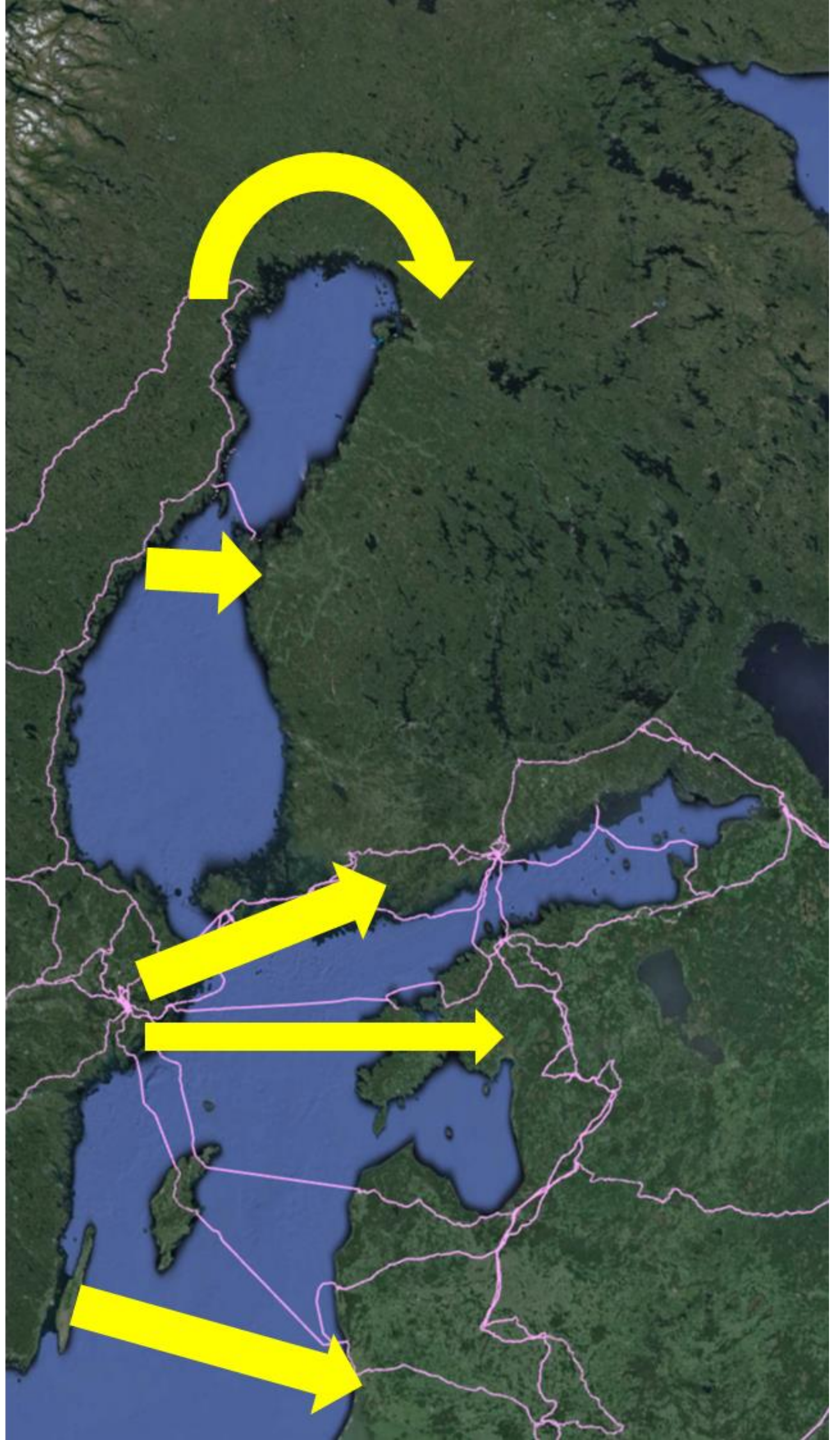
AND THEREFORE AN INCREASED INTEREST IN NEW TRAFFIC ROUTES

- 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



DDoS MITIGATION

THE IMPORTANCE OF WORKING TOGETHER

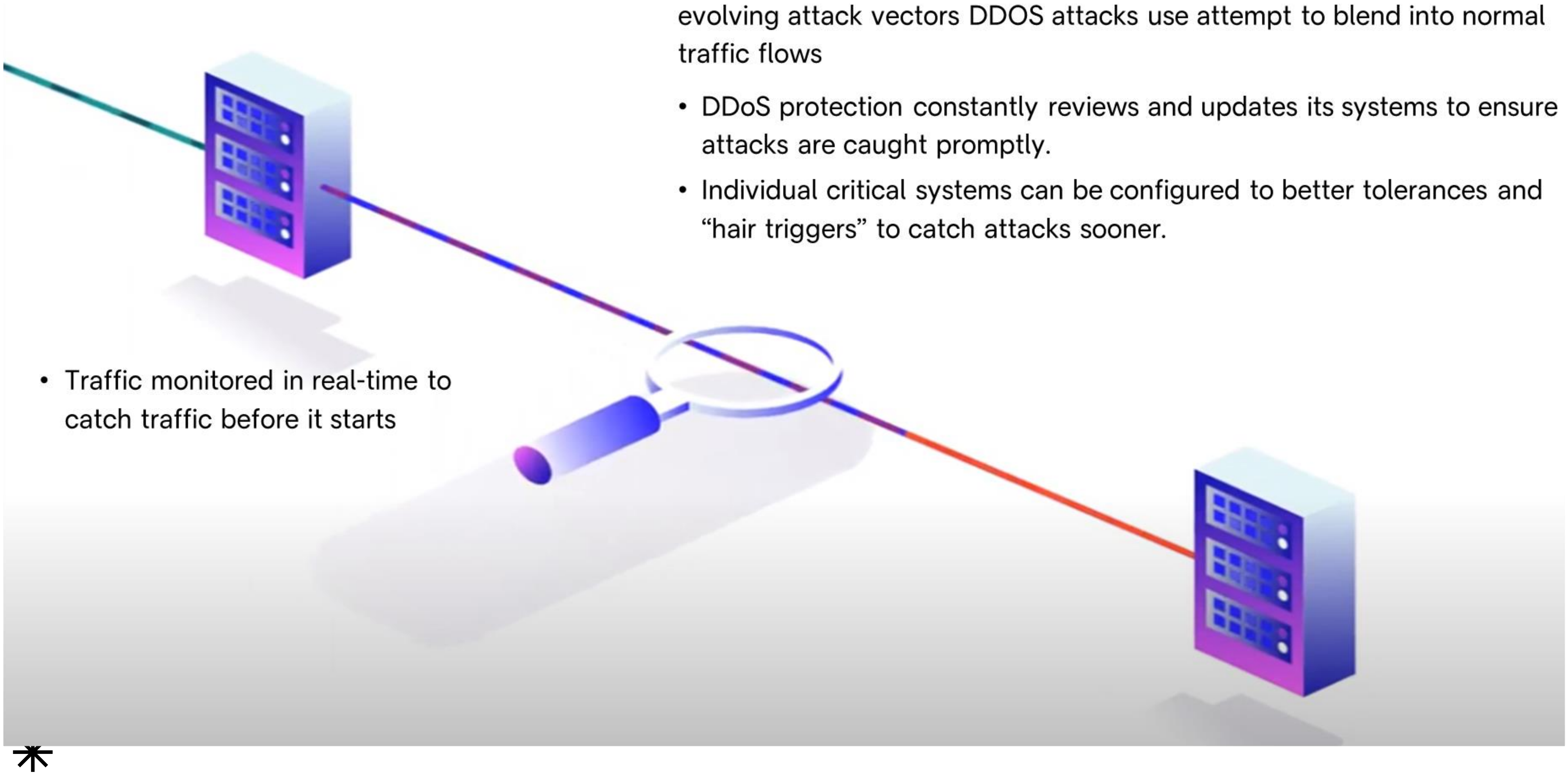
- The last few years the largest IP networks together with the largest content providers have joined what is referred to as **“the DDoS Traceback Working Group”** where spoofing friendly networks are hunted down and dealt with.

- RPKI (Resource Public Key Infrastructure) is now widely adopted among Tier 1 networks and future development is done together

- In general more info is shared among the Top Tier 1 providers

DDoS – EARLY DETECTION

- Although obvious to your organization that your systems are failing, the evolving attack vectors DDOS attacks use attempt to blend into normal traffic flows
  - DDoS protection constantly reviews and updates its systems to ensure attacks are caught promptly.
  - Individual critical systems can be configured to better tolerances and “hair triggers” to catch attacks sooner.



- Traffic monitored in real-time to catch traffic before it starts

WHAT DOES DDoS MITIGATION DO?

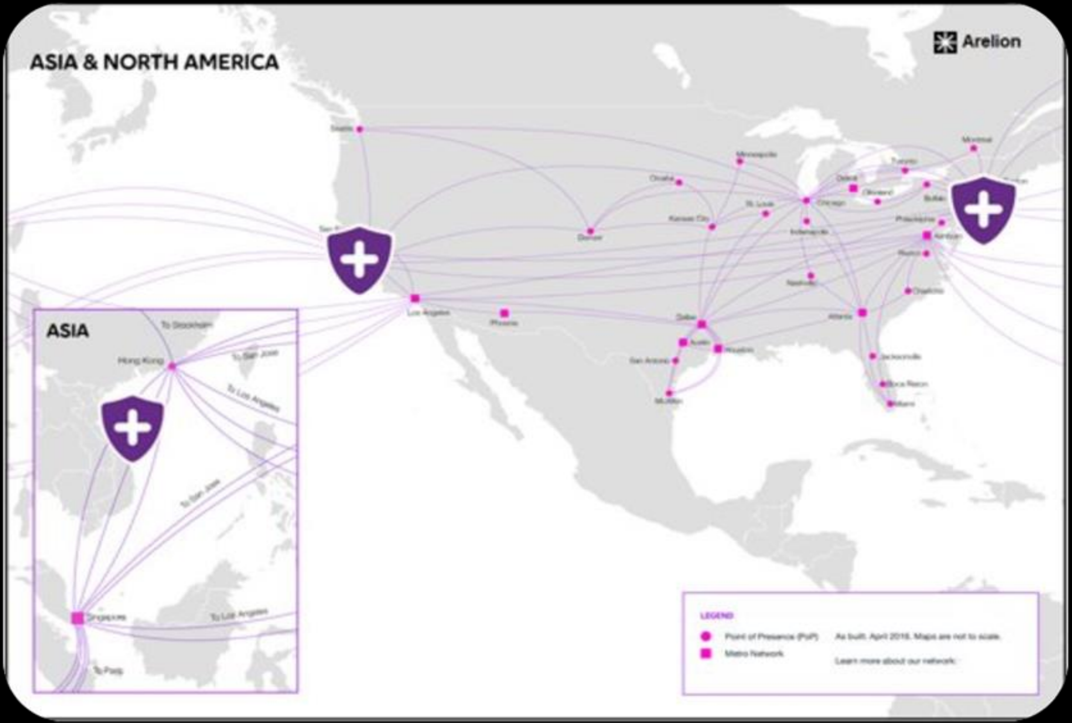
DDOS mitigation automatically detects when you are under attack

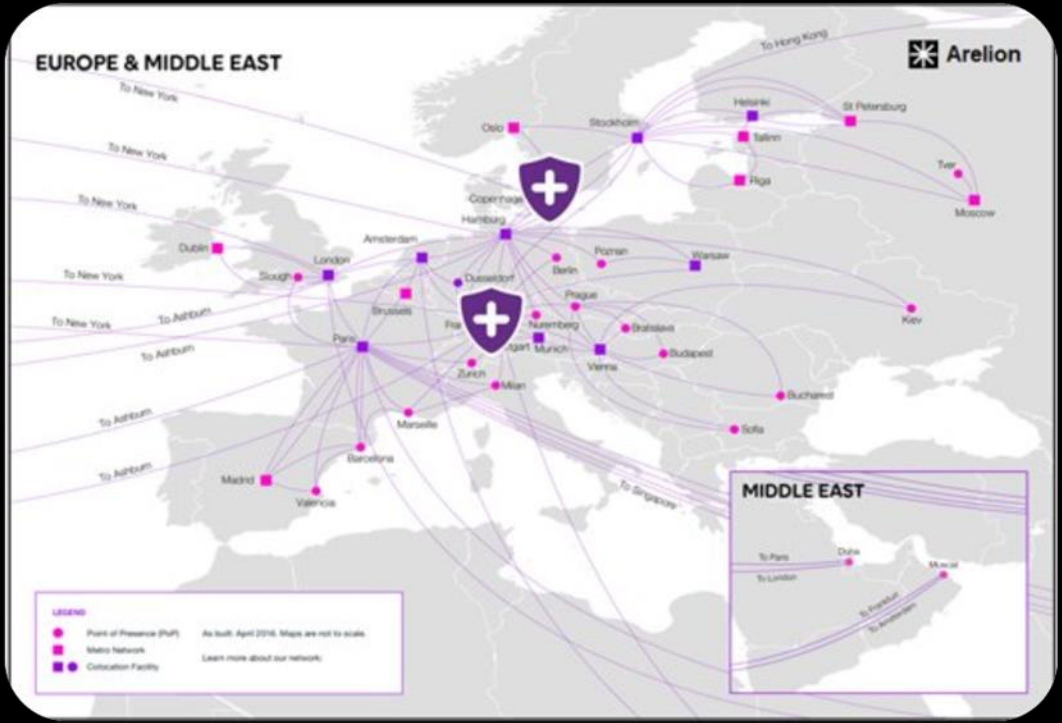
- This allows your organization to not dedicate resources to monitoring traffic
- Or worse still, stops your organization from only realizing you're under attack when your systems start to crash

DDOS Mitigation cleans or “scrubs” the Internet flow coming into your network and IT systems to remove the attack traffic

- This allows your organization to continue to function as normal during the attack
- Protection can start and stop as required, always ensuring your organizations coverage

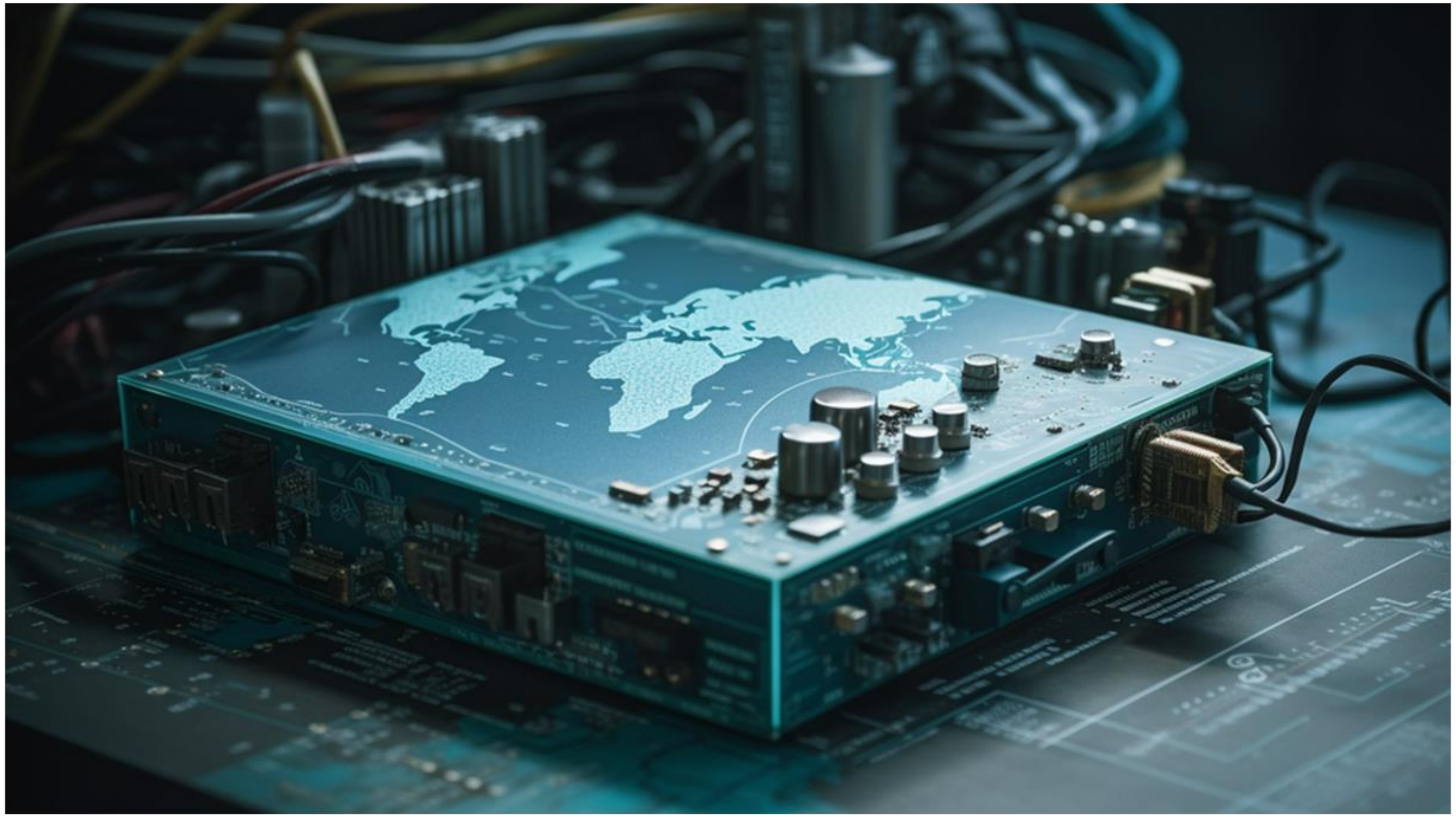
Distributed scrubbers coupled with ultra high-capacity network





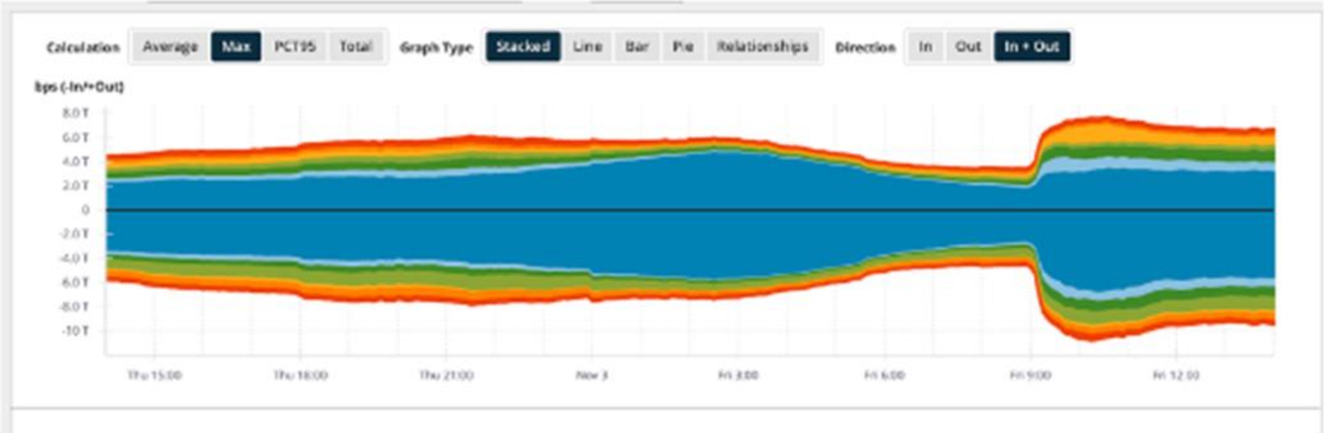
SUMMARY

- DDoS attacks are unfortunately still an issue in the Internet world
- The public awareness of the importance of IT security is increasing every month
- The Internet community that we are a big part of is increasingly working together to fight the cyber criminals
- DDoS protection is still just one of many protection mechanisms you need to be safe
- Physical security is the next focus area for all Operators



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



Calculation: Max

Graph Type: Stacked

Direction: In + Out

Thank you!

Arelion