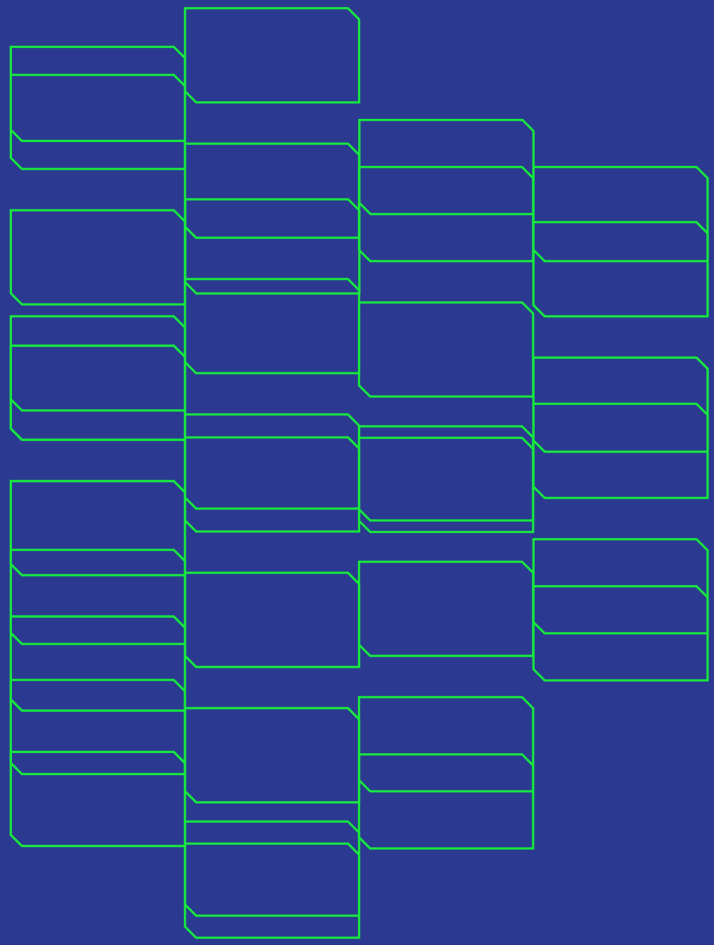
Security .Days

<Utrecht.NL>
<7-9 April 2026>

GÉANT

Examining Attack Data to Evaluate DDoS Traffic Assumptions

Scott Campbell



Co-funded by
the European Union

The path forward …

In most DDoS mitigation plans and strategies, there are some assumptions made about how traffic transits your network. While there is considerable variation in NREN architecture, there are some commonalities which can be expanded on a bit.

Discussion points:

- Basic networking terms and ideas
- Cautions about tooling
- A DDoS example to illustrate data ingress
- Takeaways and lessons

Some Core Networking Terms and Ideas

Three fundamental types of (non-naïve) connectivity:

- Commodity Transit
- Internet Exchanges
- Private Peering

I will describe and expand on where you might see them, and what they mean.

Some Core Networking Terms and Ideas (I)

Commodity Transit: Upstream network provider gives access to global routing tables.

Good: Well defined behavior, someone to contact for help, simple, sometimes upstream blocking

Bad: Expensive, less control, typical lower bandwidth

You can buy anything you want from the store, but you have to pay for everything.

Some Core Networking Terms and Ideas (II)

Internet Exchange: Physical location where different organizations connect to one another at L2, and exchange data after agreeing to terms and conditions.

Good: Convenient, cost effective, well understood

Bad: Humans. Other organizations differing/conflicting interests. Can be expensive

Membership club where you can swap stuff with other people if they are interested in playing along.

Some Core Networking Terms and Ideas (III)

Private Peering: Two organizations share physical connectivity directly between routers.

Good: Super cheap, good control

Bad: Physical proximity, Humans, potential Business and Legal conflicts.

Two people decide to exchange stuff without payment on a pre-determined corner.

Unfortunate Reality Effects

While individual parts of this taxonomy are simple, when combined they can create complex and hard to understand behaviors.

For example, you may see traffic from a particular large partner in several different paths and locations. Organizations normally pick the cheapest path *from their perspective* unless there is a very strong reason not to.

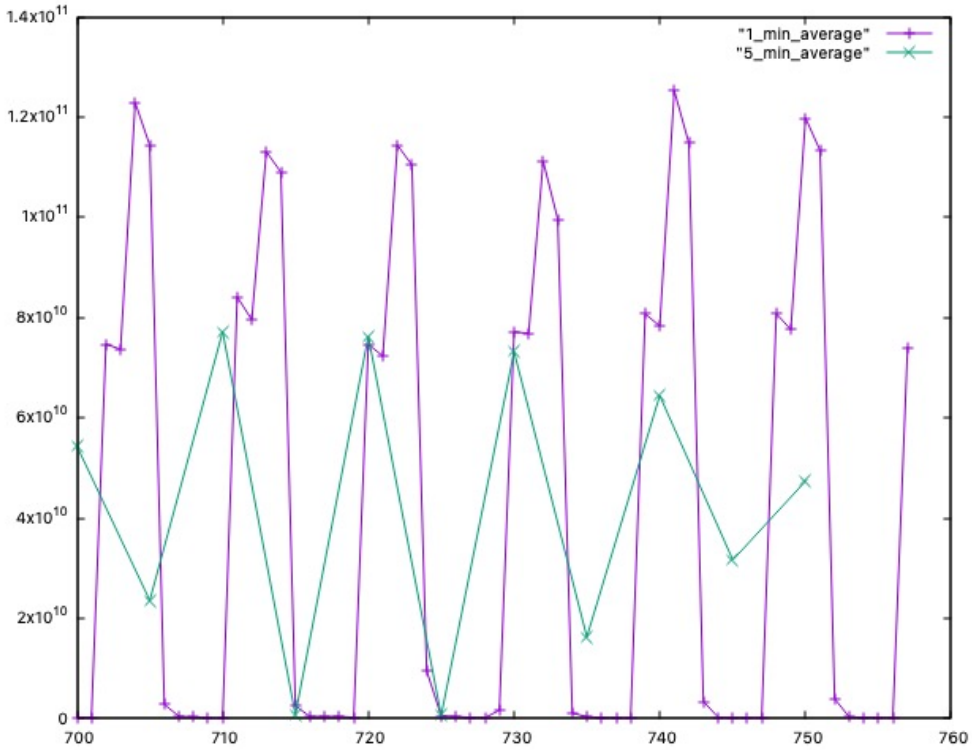
This will come into play specifically in terms of cloud providers and their related data centers.

Some Notes on Tooling

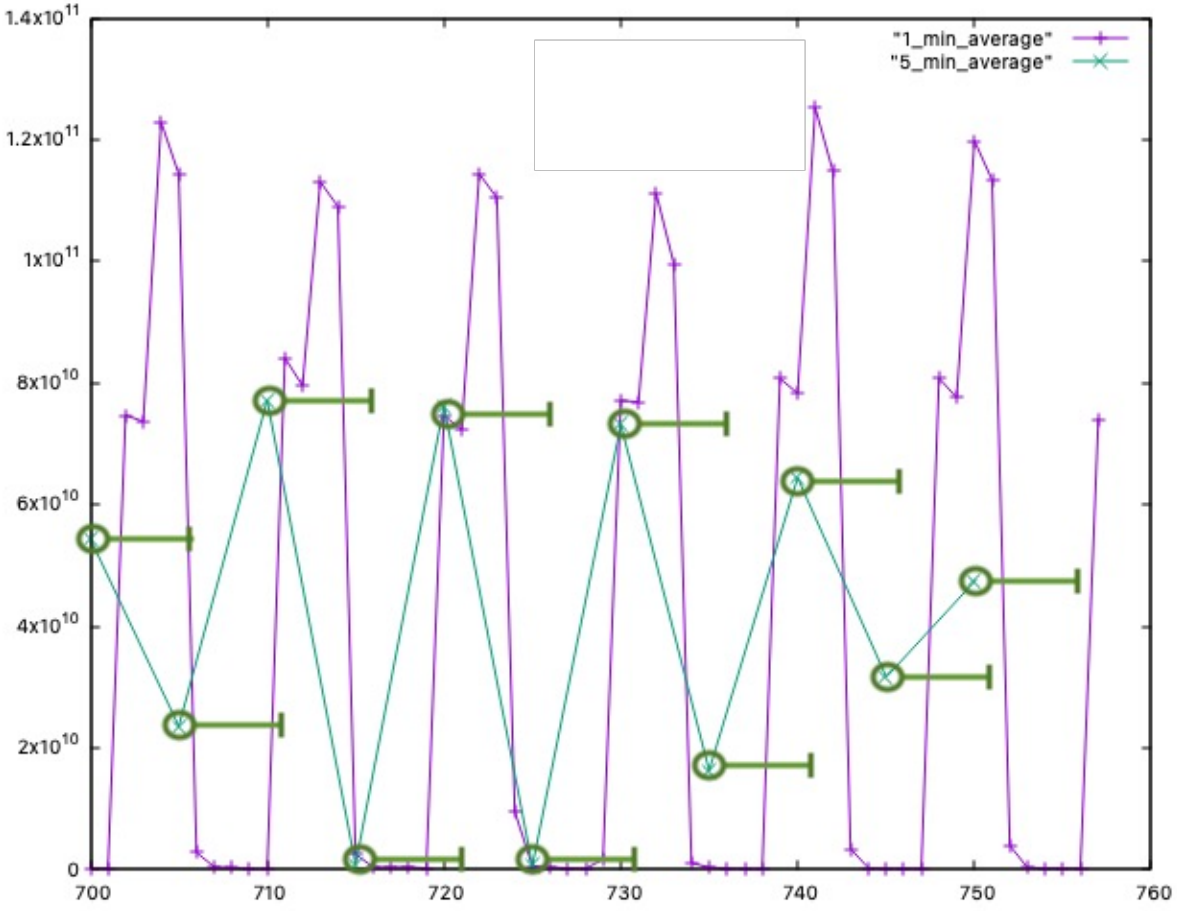
Our primary consumer flow analysis tool has adjustable “Flow Aggregation Windows” which defines the size of a unit of time.

For the exact same set of flows, larger aggregation windows show *smaller byte/packet totals over the same time range.*

- 1 min = ~125G peaks
- 5 min = ~80G peaks



About Averages – What is Happening



The 5-minute average takes the average of 5 1-minute samples as the data value.

The value is just the average, and not 5x the average, so the reported value will always be less.

Averages – What is this teaching us??

This averaging behavior rests on a fundamental issue in time series analysis – given “bursty” data, smaller time windows create graphs with greater variability.

When looking at a graph or report, the results must be carefully examined in the context of the analysis. This is particularly important when looking at complex groupings of information (like flow records from a complex network).

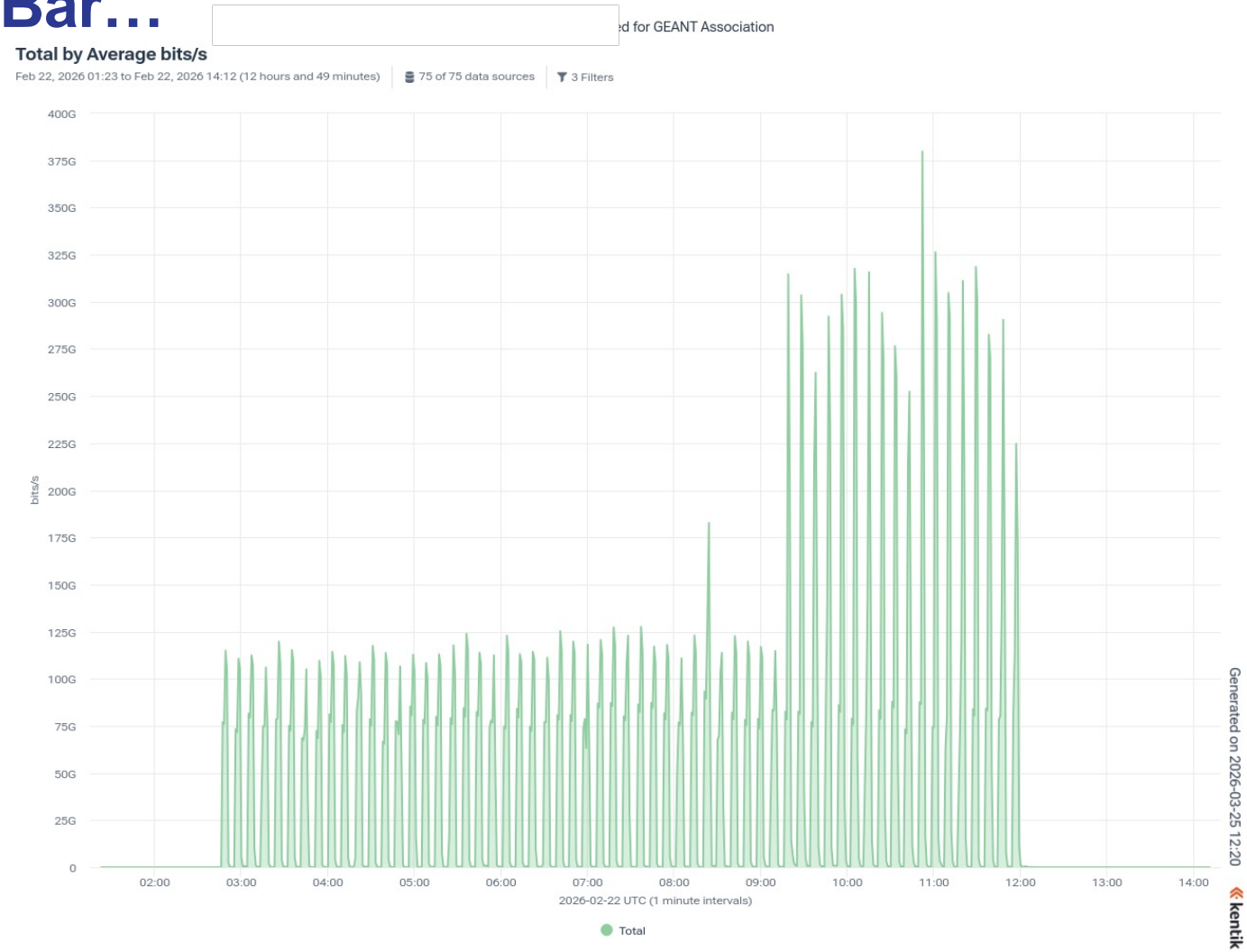
Full Disclosure: I looked at these graphs for *months* before the nagging irritation that things didn’t make complete sense overwhelmed my hope that the analysis was correct.

A DDoS Walks Into a Bar…

Some basic information:

Peak ~380 Gbit/sec
Duration ~9 Hours
3 Dest IPs at IX

All UDP
179/udp : 97%
0/udp : 3%



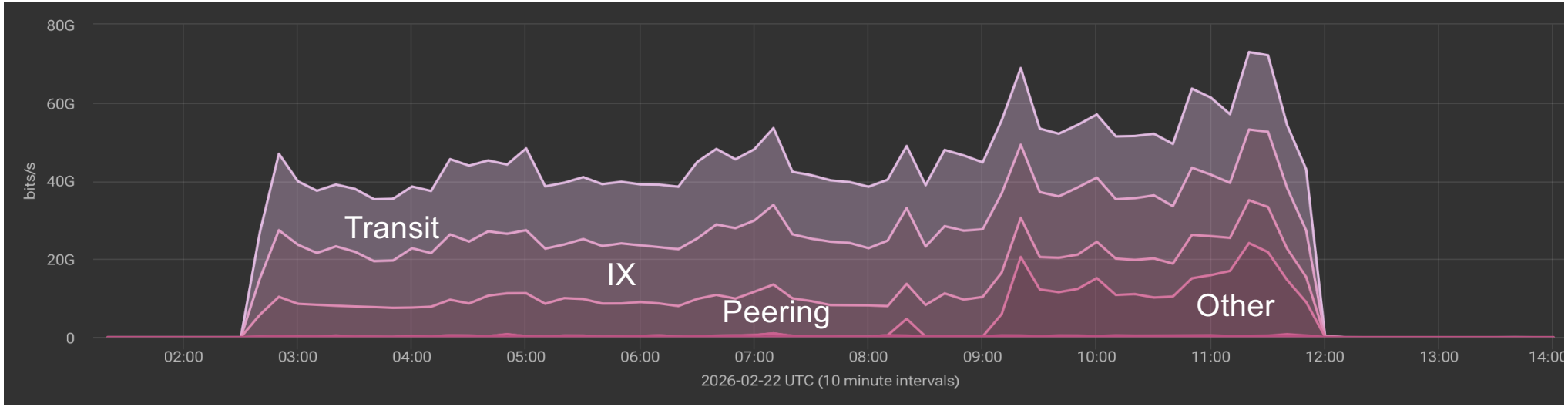
DDoS – Where is the traffic from??

At the most basic level, each router interface can be assigned a membership based on the interface description text.

This is done via regular expressions applied to the interface description text which benefits you tremendously if you have standardized/automated methods for labeling.

Quite powerful, *except where it doesn't work* or when functionality does not align with the set of interface description types.

DDoS – Source Information



Name	Average (Gbit/sec)	Peak (Gbit/sec)
Transit	12.37	20.92
Internet Exchange	11.48	20.38
Direct Peering	6.57	12.51
Other	3.06	23.77
External R&E	0.13	0.81
Internal NREN	0.10	0.30

About the ‘Other’

As suggested in the Information Sourcing slide, not every flow and interface description neatly into a functional group.

Other stuff:

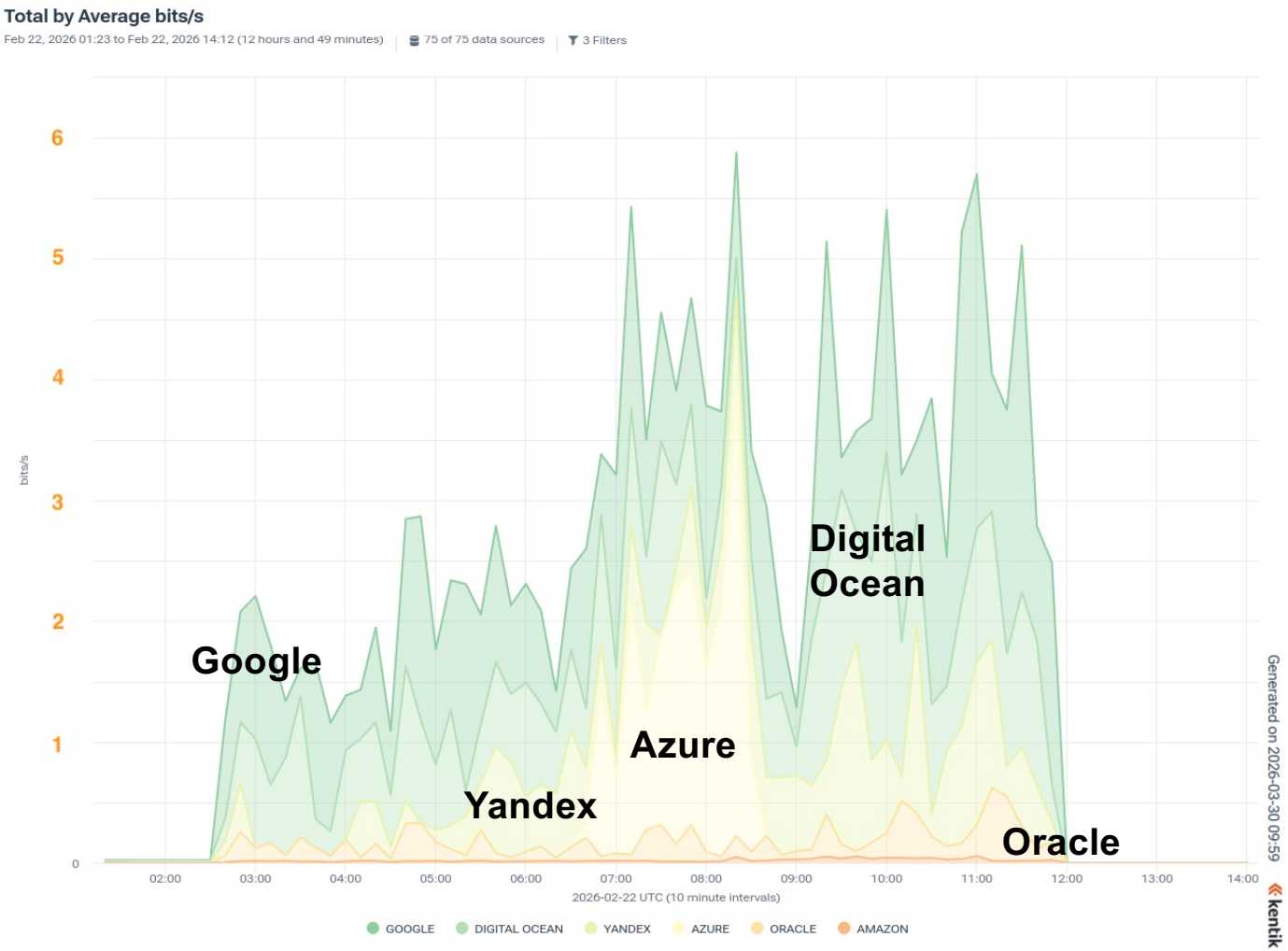
- DDoS Scrubber: Route injection to private AS
- Flowspec Rules: Forwarding to port zero …
- One-off descriptions

The ‘other’ here tends to be all the corner cases and interesting things that make

Hyperscalars

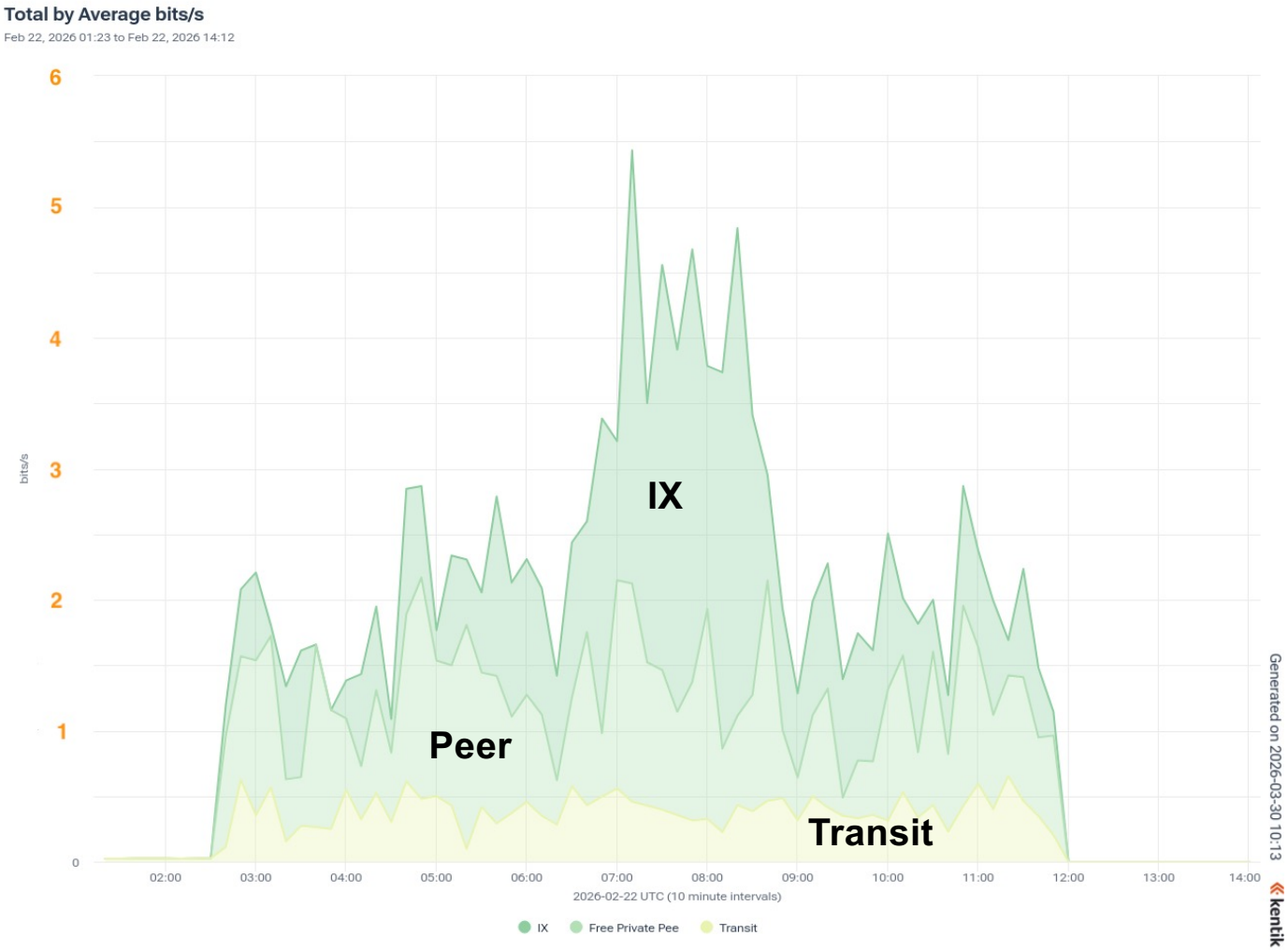
How did cloud services contribute to the DDoS attack?

Can look at tagged interfaces and AS numbers to determine data volume.



Hyperscalars

Looking at how that traffic got to our network.



Additional Vectors

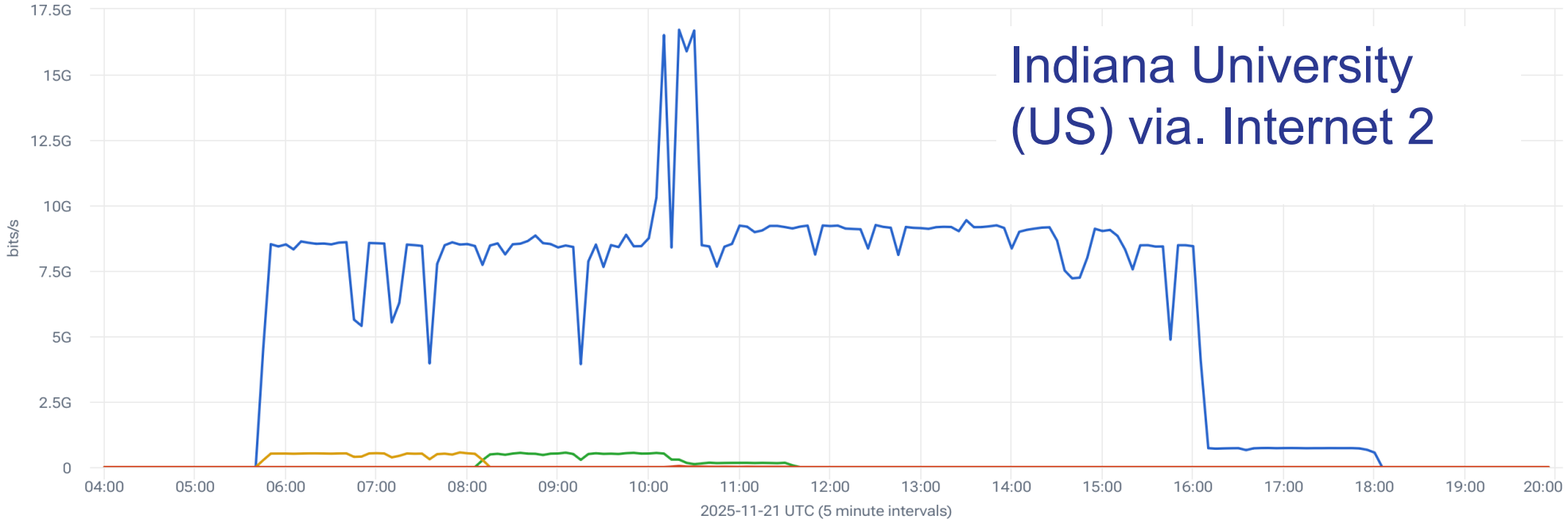
The last example is one example of DDoS activity. It is fairly typical, but there are other examples showing other data source types.

Looking at the table from a few slides back we see in addition to transit, Internet Exchange, Direct Peering and Other there is also External R&E and Internal NREN.

These types represent high-volume, non-commercial connectivity within the EU as well as globally. GEANT has dozens of these connections, many between 100-400G.

Example II

Example of such an incident.



State of Things …

The idea to take away is that most NREN networks have vastly more exposure than their available scrubbing capacity. This is particularly true when you take into consideration inter-NREN and R&E partners rather than just commodity transit.

Taking into account the shrinking attack duration, things are becoming more complex in terms of attack mitigation.

Remediation: Detection

IPFIX 315 – 1 second detection time (mechanically more like sFlow) dramatically increase detection granularity, router exports first (160+) bytes of the packet header.

Some complexities here in terms of flow record volume, field extraction from data, and header data as potential privacy issue if not addressed correctly.

Remediation: Example Responses

Path Mitigation: Classic BHR, sink destination outside “border” – not attractive, but minimize rollover effects from unwanted traffic

Source Mitigation: Like Nokia Deepfield, use (dynamic) list of known bad addresses and prefixes to block traffic on entrance to the network.

Traffic Mitigation: Do all packets need equal access across the network? Limit well defined traffic classes to rate limited policies.

In all cases, non-trivial complexity in terms of how to address support and error reports. New approaches – not all packets are equal.

Nothing is simple at scale.

GÉANT

Co-funded by
the European Union