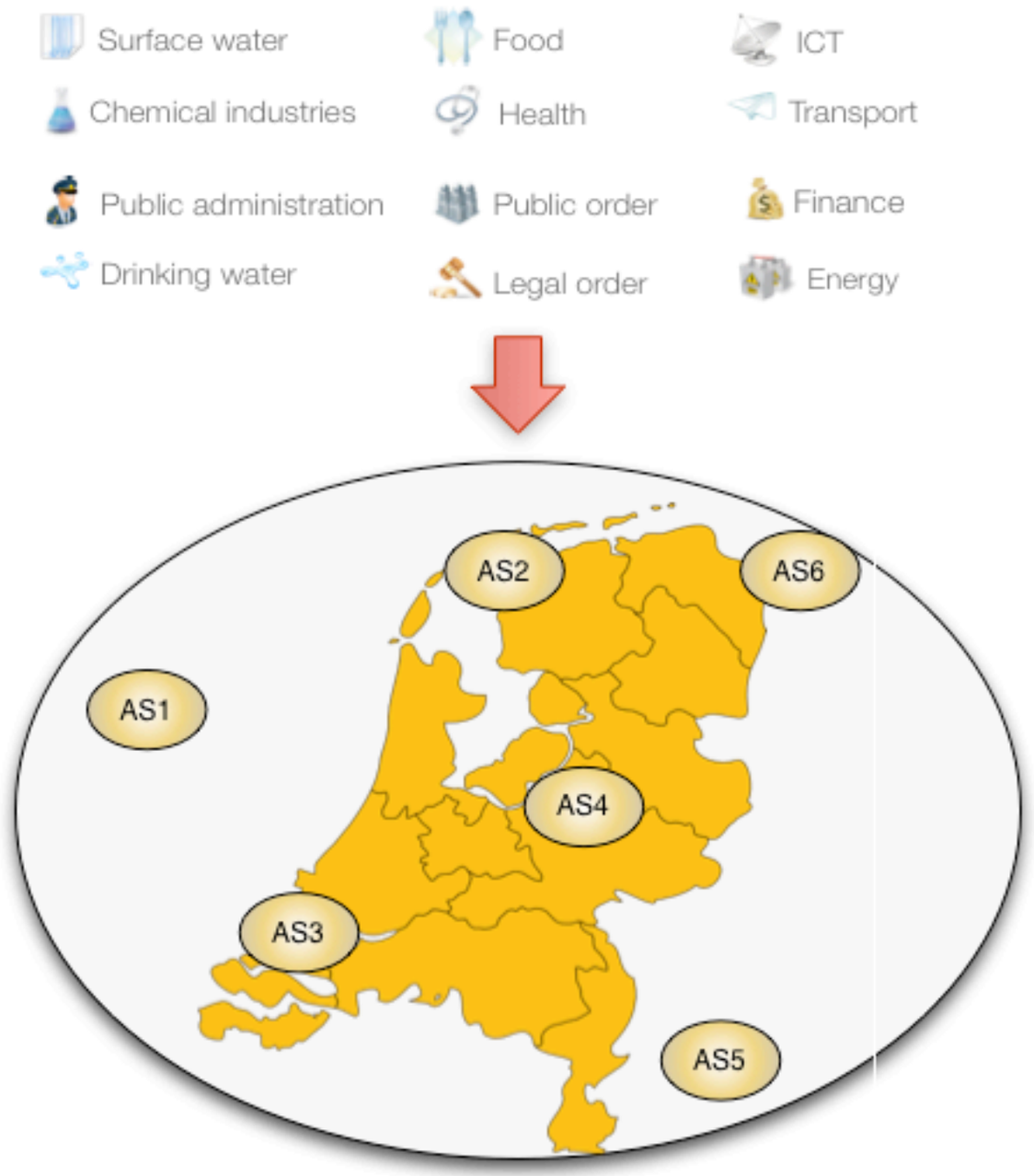
# Mapping the Dutch Critical Infrastructure

**Razvan C. Oprea**
**Fahime Alizade**

***Supervisors:***
**Benno Overeinder**
**Marco Davids**

# The Question



# Methodology

We have no idea on organizations' physical connections to the Internet, but we are interested in the logical IP topology:

- we work at an **AS level**
- we use two methods for discovering relevant ASNs

**1 Bottom-up discovery approach**

We discover the "Dutch" ASNs, then we identify organizations in critical sectors

**2 Top-down approach**

Starting from organizations in critical sectors, we identify the corresponding ASNs

**3 Analysis and visualization**

We combine the results of the two approaches, find interconnections and build graphs

# Bottom-up Approach

We use the ASN allocation list published by the RIPE NCC

We select the ASNs allocated to organizations registered in NL or EU

Every EU ASN is queried in the RIPE WHOIS database to select NL registrations (address or description fields)

We select the organizations in the critical infrastructure sectors (domain name, KvK)

```
ripencc|*|asn|*|28184|summary
ripencc|EU|asn|1196|1|19930901|allocated
ripencc|IE|asn|1197|1|20101118|allocated
ripencc|EU|asn|1198|1|19930901|allocated
ripencc|EU|asn|1199|1|19930901|allocated
ripencc|NL|asn|1200|1|19930901|allocated
ripencc|EU|asn|1203|1|19930901|allocated
ripencc|AT|asn|1205|1|19930901|allocated
ripencc|IE|asn|1213|1|19920617|allocated
ripencc|EU|asn|1234|1|19930901|allocated
ripencc|EU|asn|1235|1|19930901|allocated
ripencc|EU|asn|1241|1|19930901|allocated
ripencc||asn|48198|1||reserved
ripencc||asn|48204|1||reserved
ripencc||asn|48253|1||reserved
ripencc||asn|12410|1||available
ripencc||asn|15449|1||available
ripencc||asn|15907|1||available
ripencc||asn|16078|1||available
```

# Bottom-up Approach (contd.)

## Limitations

We do not know if all the ASNs of an organization relate to critical infrastructure

We have limited information on organization structure and ownership (Virtual ASNs)

The number of “Dutch” ASNs in the Internet sector is disproportionately high (~80%)

## Observations

727 ASNs allocated to Dutch organizations

335 ASNs relate to the critical infrastructure sectors

265 ASNs relate to the Internet infrastructure sector

# Top-Down Approach

We search for well-known entities in each critical sector

We find the organization name (KvK) and their domain

We search for the IP addresses corresponding to their A, AAAA and MX records

We use RIPEstat to find the prefix it is part of and the originating ASN (the “proxy” AS)

# Top-Down Approach (contd.)

## Limitations

Public information only

Complete mapping of critical sector industries requires specialized knowledge (think food chain supply)

Backup and private links are not visible

## Observations

We tried to have at least few samples from every sector

In total, we hand-picked 147 organizations part of the Dutch critical infrastructure

# Data analysis

We combine the result of the two approaches and obtain a “master” ASNs list.

The inter-AS relationships is visible in BGP dumps, but it’s better to have multiple viewpoints for accuracy

RIPE RIS, RouteViews, Route Servers, Looking Glasses all offer multi-views on the BGP links

traceroute is not a viable option since the IP address space used by organizations is privileged information

We considered the aggregated data offered by UCLA IRL, CAIDA and University of Washington and we ultimately chose UCLA

# Data analysis (contd.)

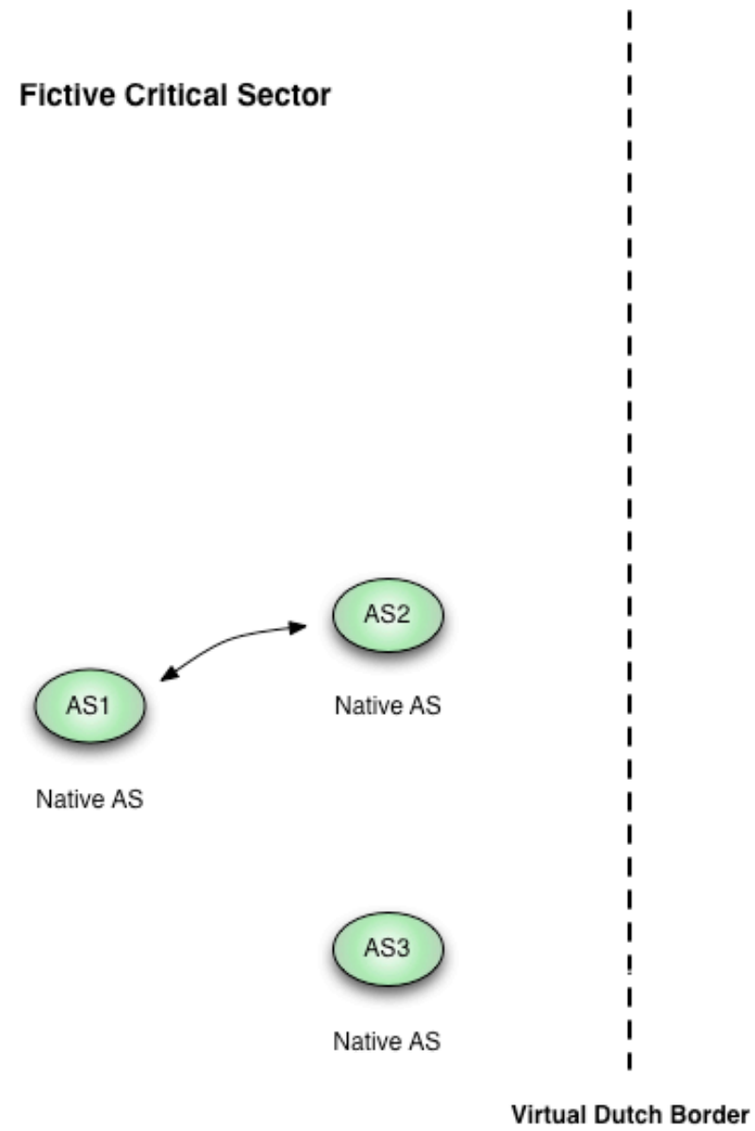
Many nodes (ASNs) are abroad

The initial graphs show many disconnected nodes

Which ASNs to include to show relevant links?

We choose to include the providers of the native and proxy ASNs

We then built the full mash of the AS and provider list based on UCLA data

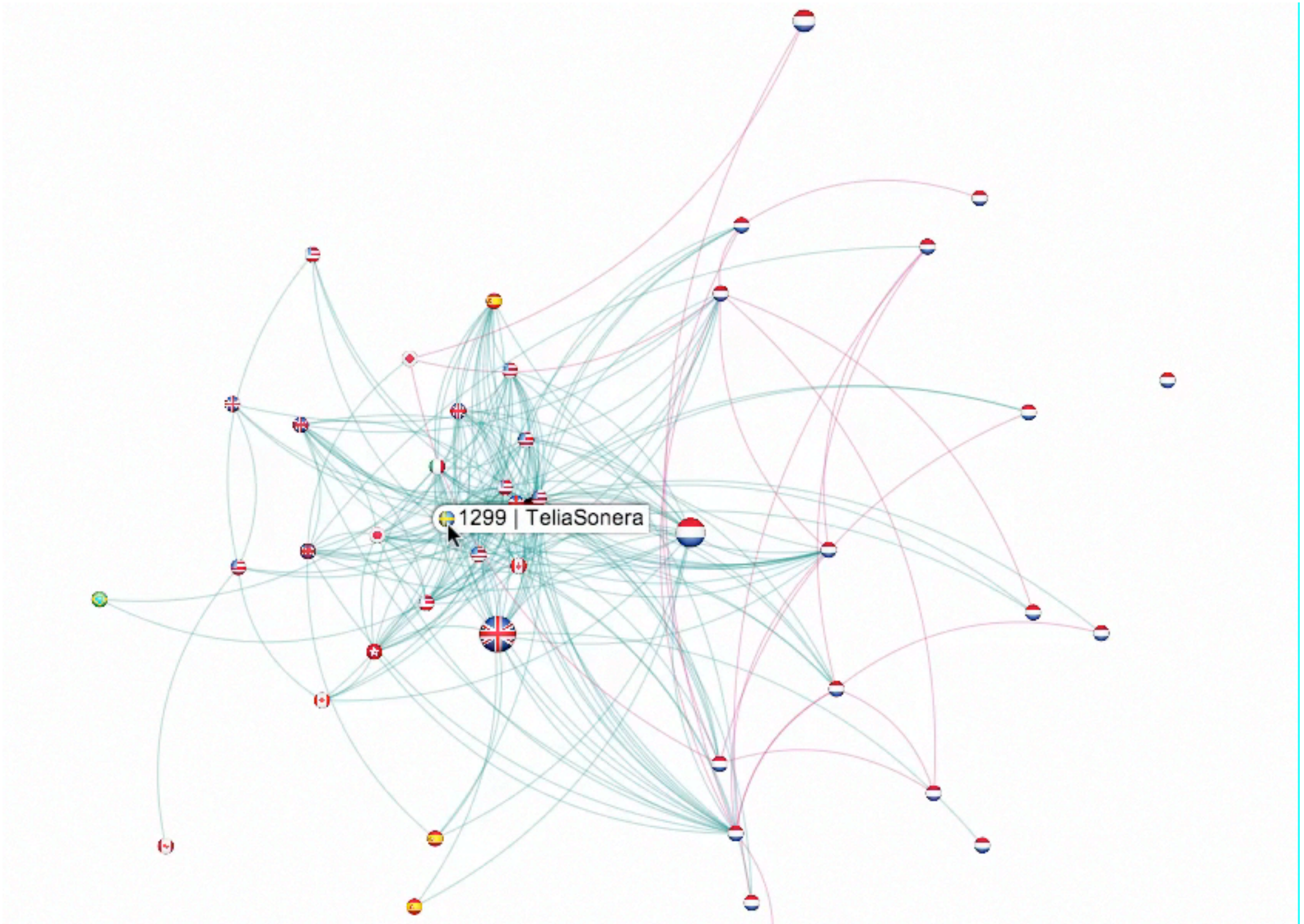


# Visualization Methods

To display and present high number of AS numbers and their relations, we chose **Sigma.js**, which is an open source Javascript visualization library.

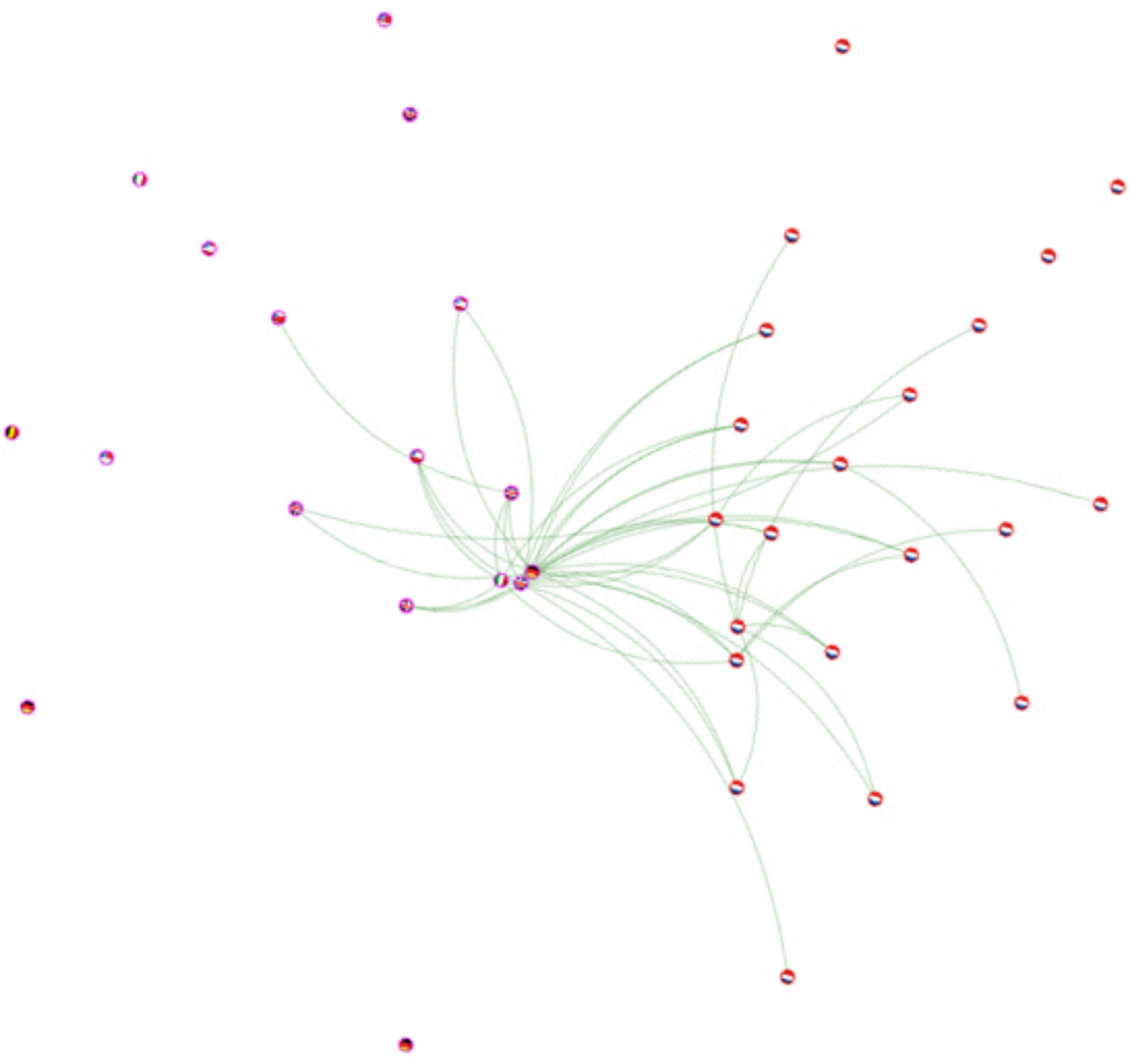
We achieved an interactive presentation of graph to zoom-in and to see labels.

# Visualization Detail



# Visualization and conclusions

Energy Sector - no providers



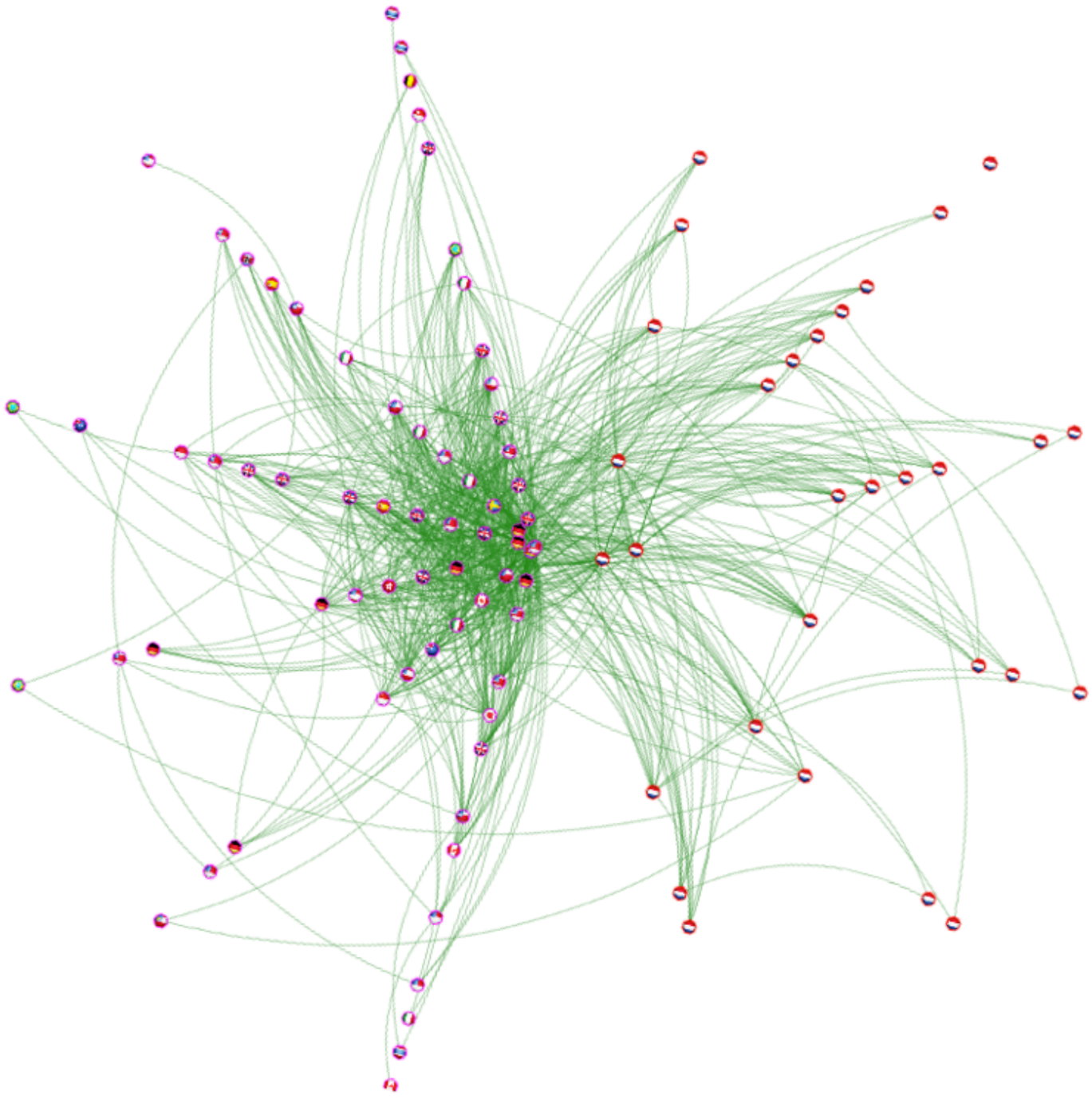
Foreign ASNs

Dutch ASNs

# Visualization and conclusions (contd.)

Energy Sector - with providers

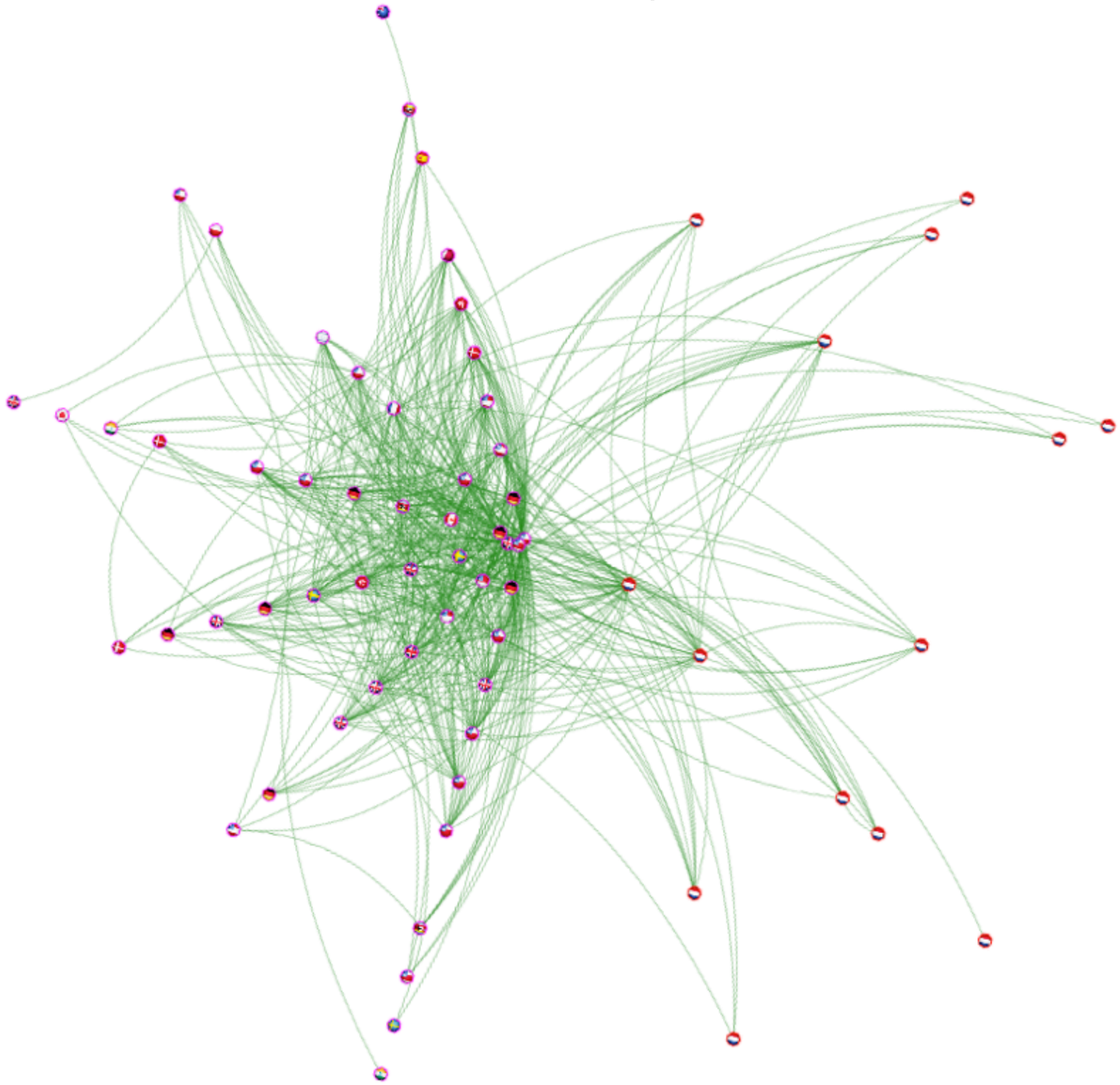
Foreign ASNs



Dutch ASNs

# Visualization and conclusions (contd.)

Food Sector - with providers



Foreign ASNs

Dutch ASNs

# Observations

1 Related companies/industries choose sometimes the same providers: **NS and ProRail (BT), Royal Dutch Shell, Gasunie** and **Argos Energies (Microsoft Corp.)**

2 Some organizations have their own ASN, but they still outsource their email and website hosting (**Alliander**).

3 The biggest providers (mail) are **MessageLabs** (UK & US), **KPN**, **Microsoft**, **Tele2 Nederland** and **Ziggo**.

# Observations (contd.)

4 What do **ABN AMRO**, **Triodos Bank**, **AkzoNobel**, **GGD** have in common: all their mails come through the same provider: MessageLabs Ltd., UK

Nine other companies in the critical sectors use the services of MessageLabs Inc., US

5 In fact, **MessageLabs** (a division of Symantec Corp.) is the single biggest messaging provider in our list

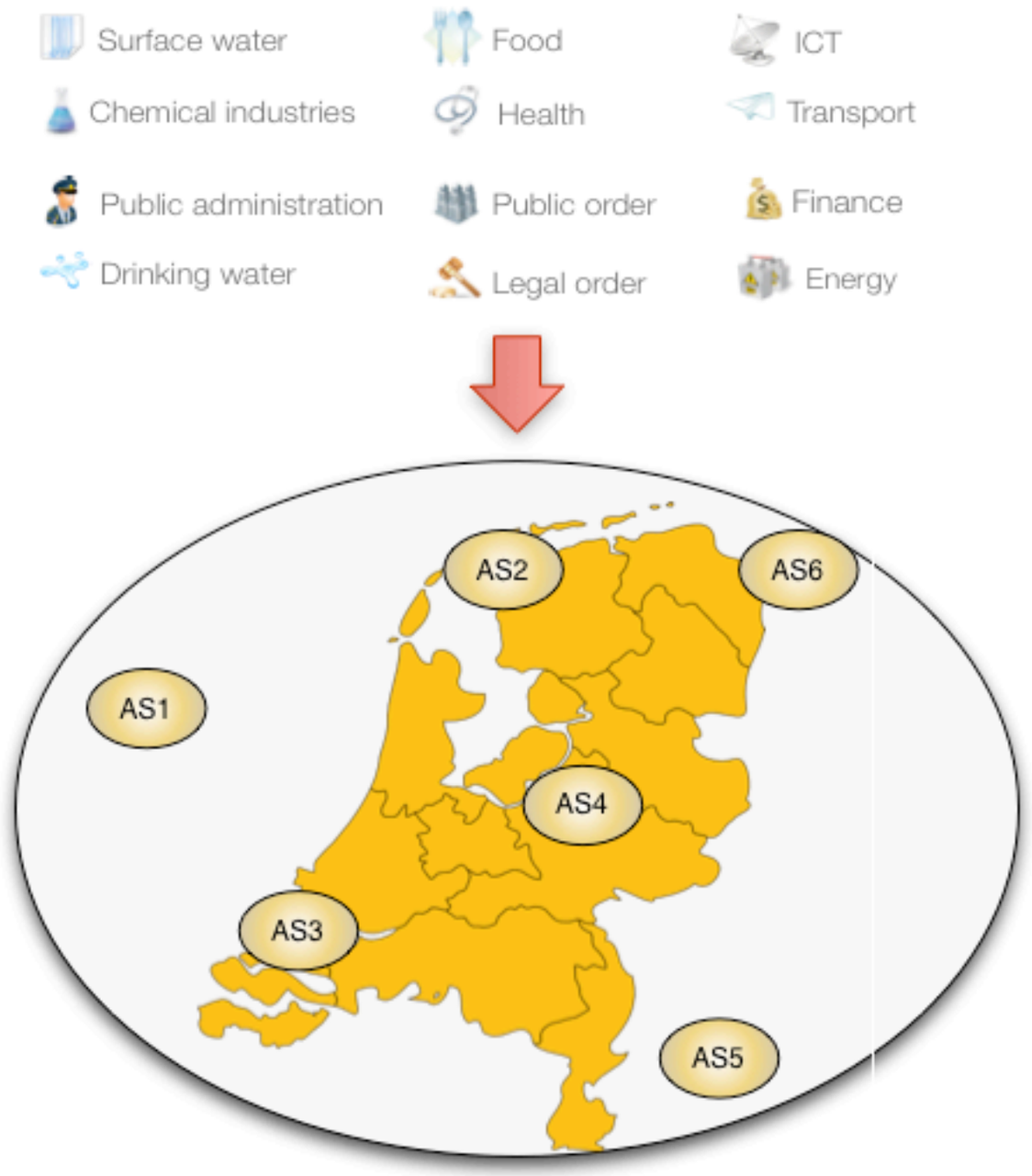
# Conclusions

Many critical infrastructure organizations have reliable connections to the Internet, but rely a lot on foreign providers for their communication needs

It is worth discussing the security and privacy implications of having email and websites hosted with entities from outside the EU

We do not see that critical infrastructure organizations regard their network infrastructure as being of national critical importance

# Q & A


Surface water
Food
ICT
Chemical industries
Health
Transport
Public administration
Public order
Finance
Drinking water
Legal order
Energy
AS1
AS2
AS3
AS4
AS5
AS6