Fachhochschule Gelsenkirchen

European Internet Situation Awareness → The Global View

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Content

- Structure of the Internet
- Internet Analysis System (IAS)
  (Idea, Targets, Approach, Results)
- Global view
- Summary

Content

- **Structure of the Internet**

- Internet Analysis System (IAS)
  (Idea, Targets, Approach, Results)
- Global view
- Summary

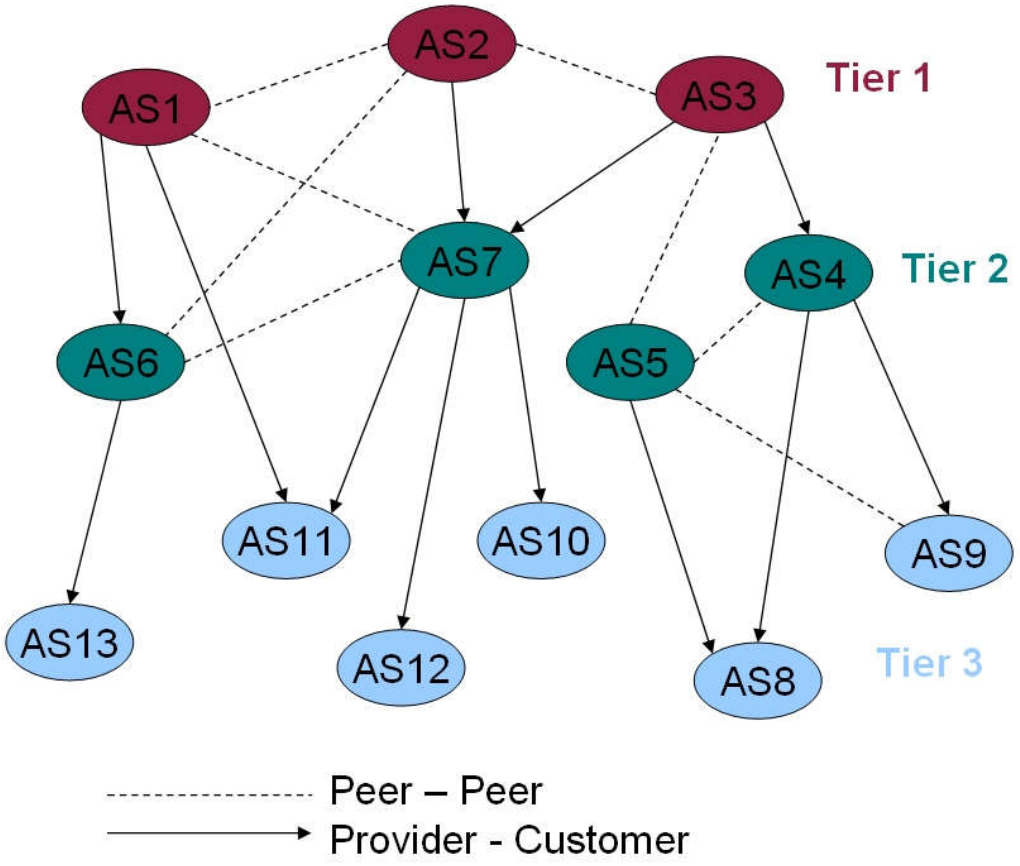
Structure of the Internet
→Autonomous Player

- **Autonomous Systems (AS)**
  - The global Internet consists of thousands of independent networks, the Autonomous Systems (AS)
  - Currently there are about 27.000 different ASs advertised in the global Routing table
  - The AS operators have different policies for the size and expansion of their network
  - An AS needs a strategy to connect with other ASs using upstreams, private or public peerings
  - There are more than 60.000 logical connections between ASs at the moment

- **Different types of Autonomous Systems**
  - Large Companies, e.g. business consumer (41 %)
  - Internet Service Providers, e.g. IP-carrier (35 %)
  - Universities (11 %)
  - Internet Exchange Points, e.g. public data exchange nodes (2 %)
  - …

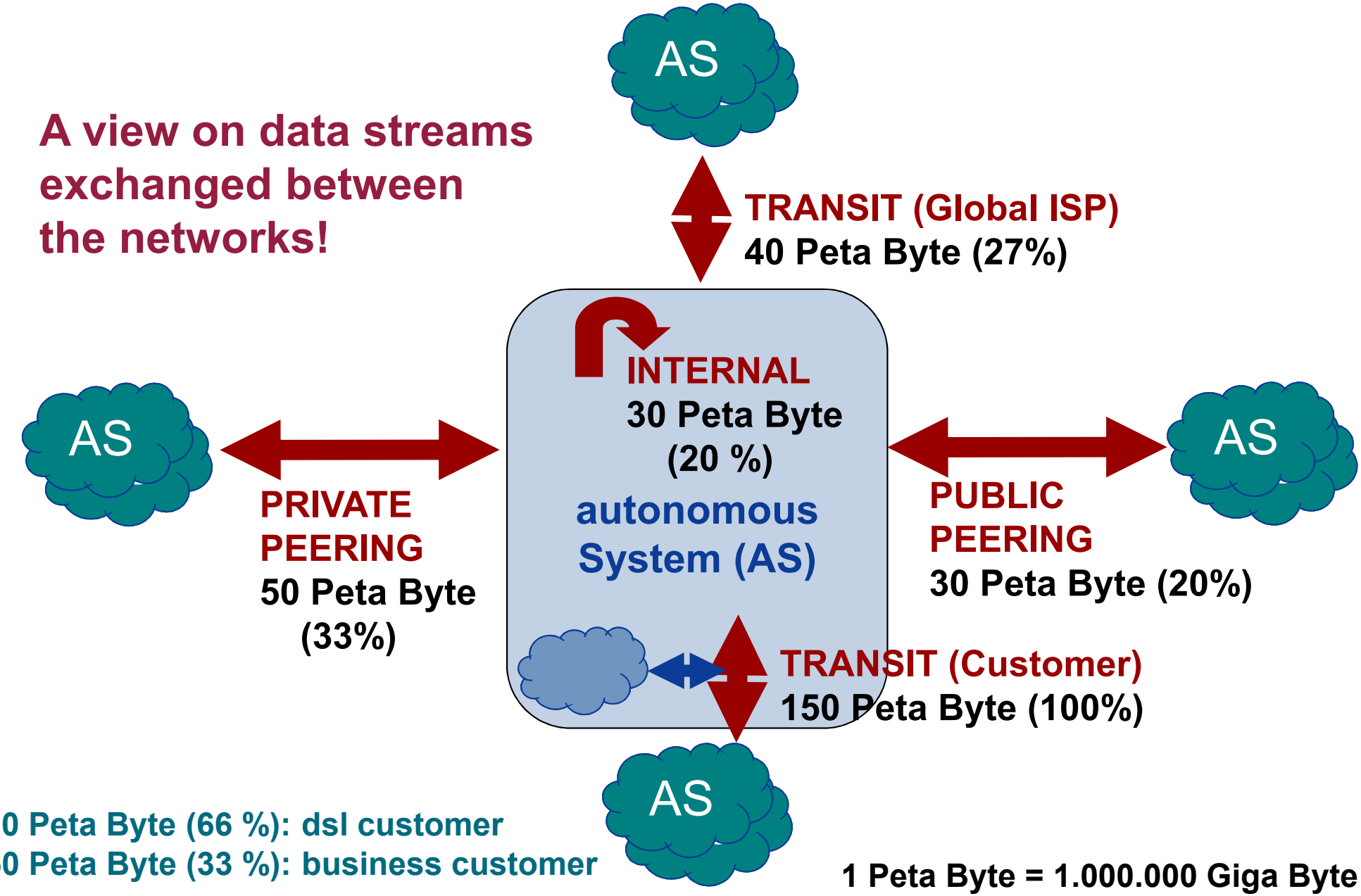
Structure of the Internet
→Connectivity of the Internet

- **Ongoing analysis on the Route Views Snapshot**
  - <= 2 = 63 %
    <=10 = 94 %
    >10 = 6 %
    >100 = 0,4 %
    >300 = 0,1 %
  - Economical necessities affect the carrier‘s proceeding
  - This yields to a destabilization of the internet infrastructure



- **What is imported in this field?**
  - We need an entity which keeps an eye on the level of connection and the reliability of all ASs in the Internet

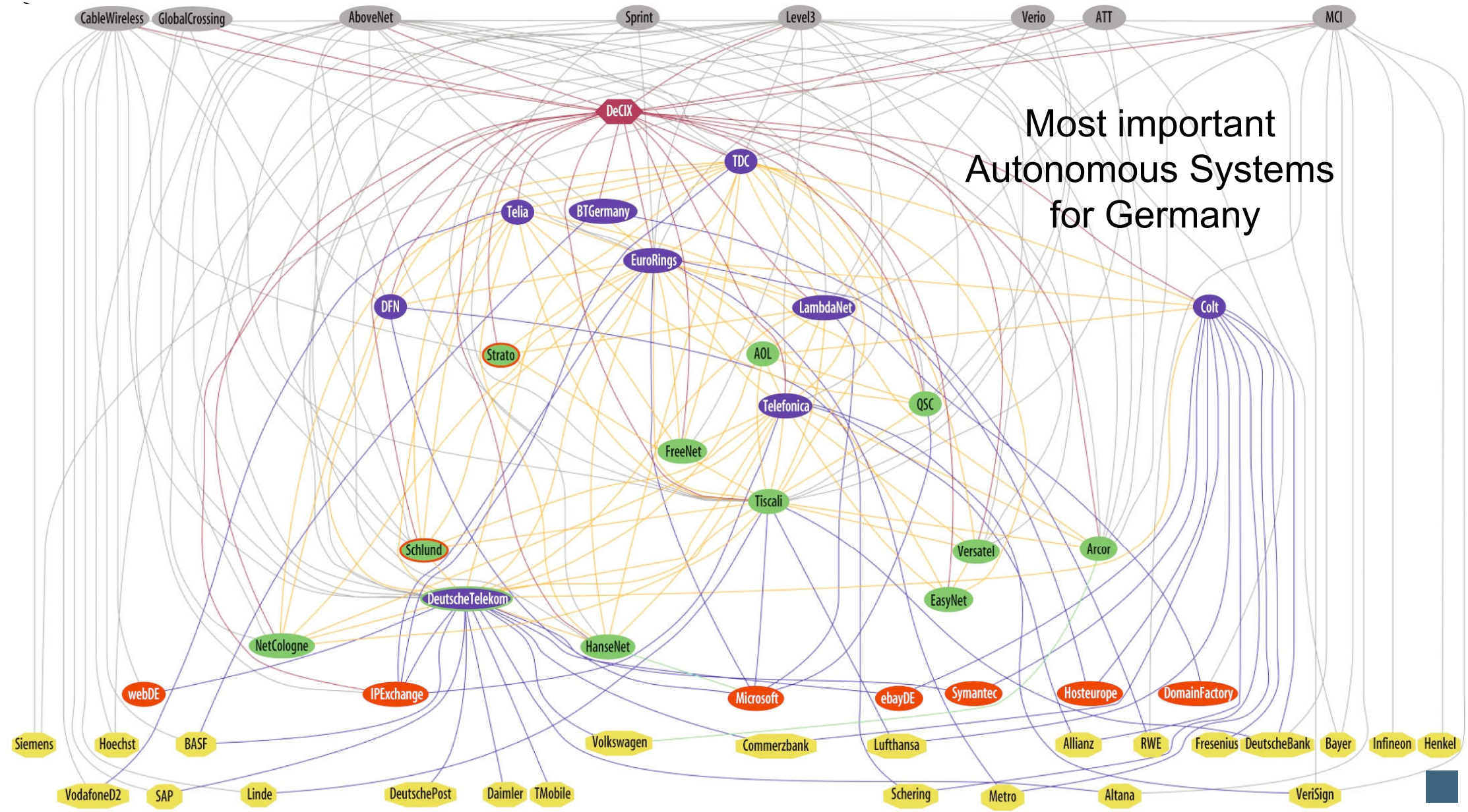
Data volume / month in Germany
→ Estimation



100 Peta Byte (66 %): dsl customer
50 Peta Byte (33 %): business customer

1 Peta Byte = 1.000.000 Giga Byte

Structure of the Internet
→ Analysis of „Internet Germany“



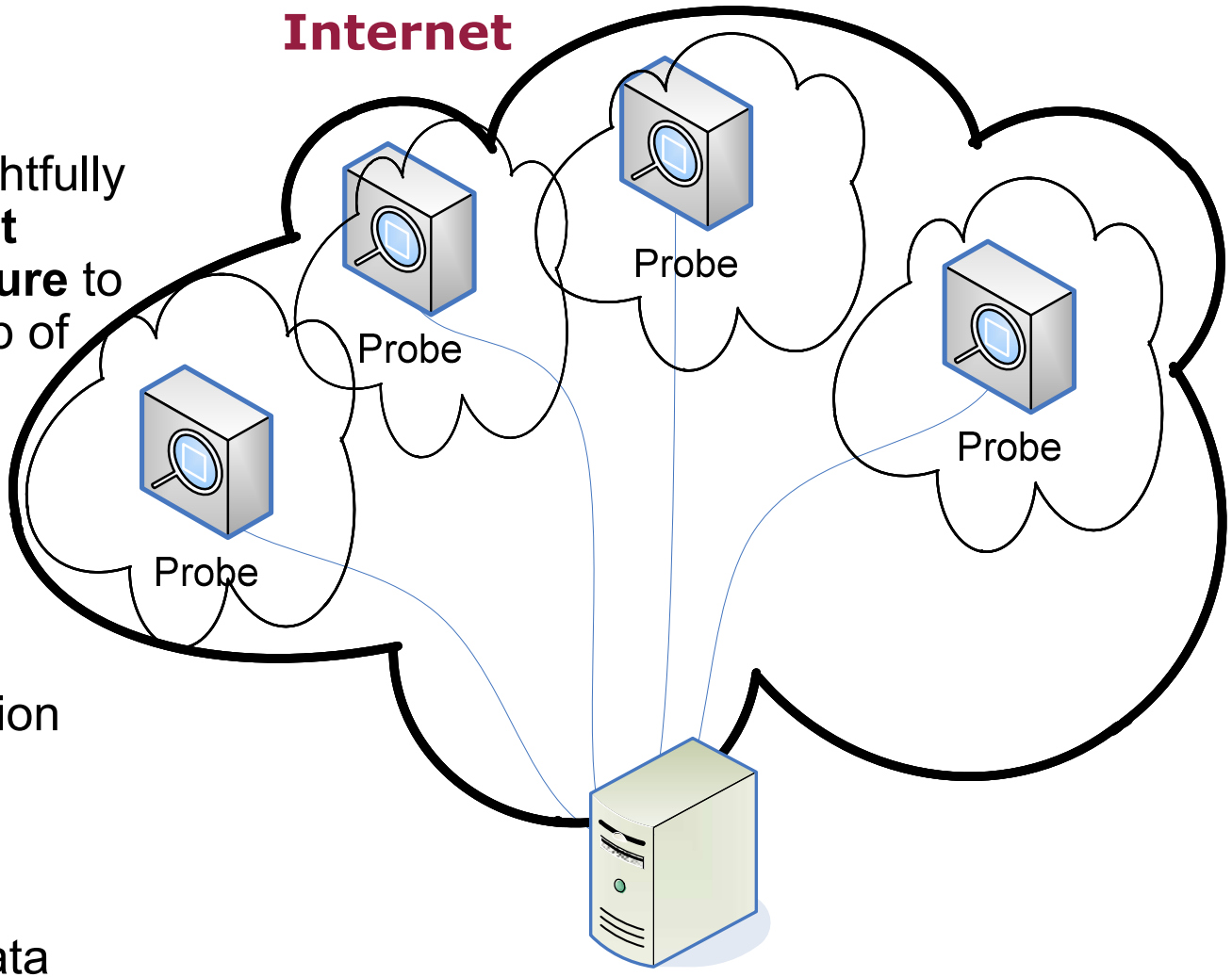
Most important Autonomous Systems for Germany

Content

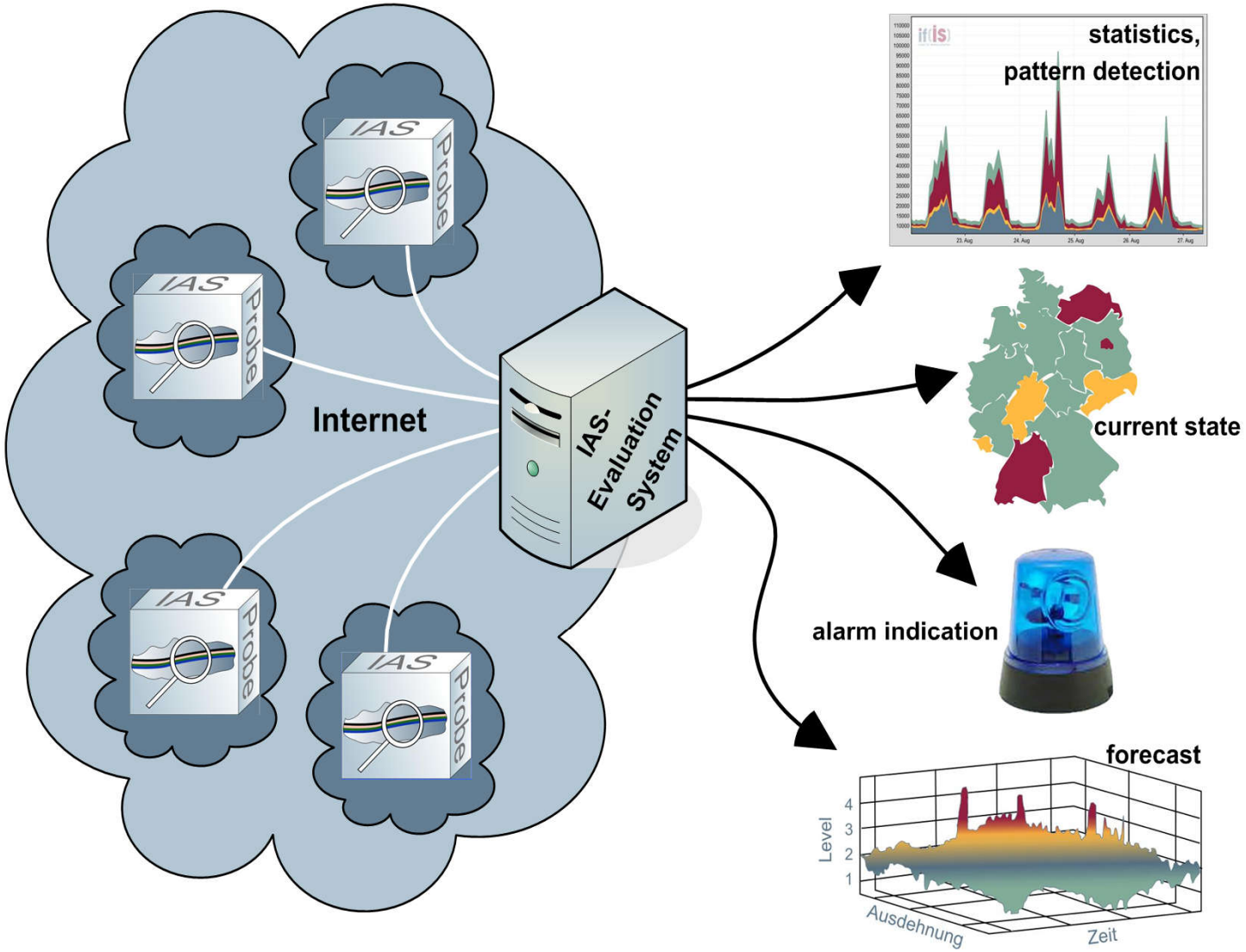
- Structure of the Internet
- **Internet Analysis System (IAS) (Idea, Targets, Approach, Results)**
- Global view
- Summary

Internet Analysis System (1/3)
→ Idea

- Observation of the critical infrastructure **„Internet".**
- **Probes** are placed in thoughtfully selected spots of the **internet communication infrastructure** to gather the raw data, made up of counted header information.
- Only header information is counted, which is **not considered as data privacy relevant**.
- The system gathers information over a **great period of time**!
- A centrally managed **Evaluation System** is used to analyze the raw data and to display the detailed results in an intuitive manner.



Internet Analysis System (2/3)
→ Targets



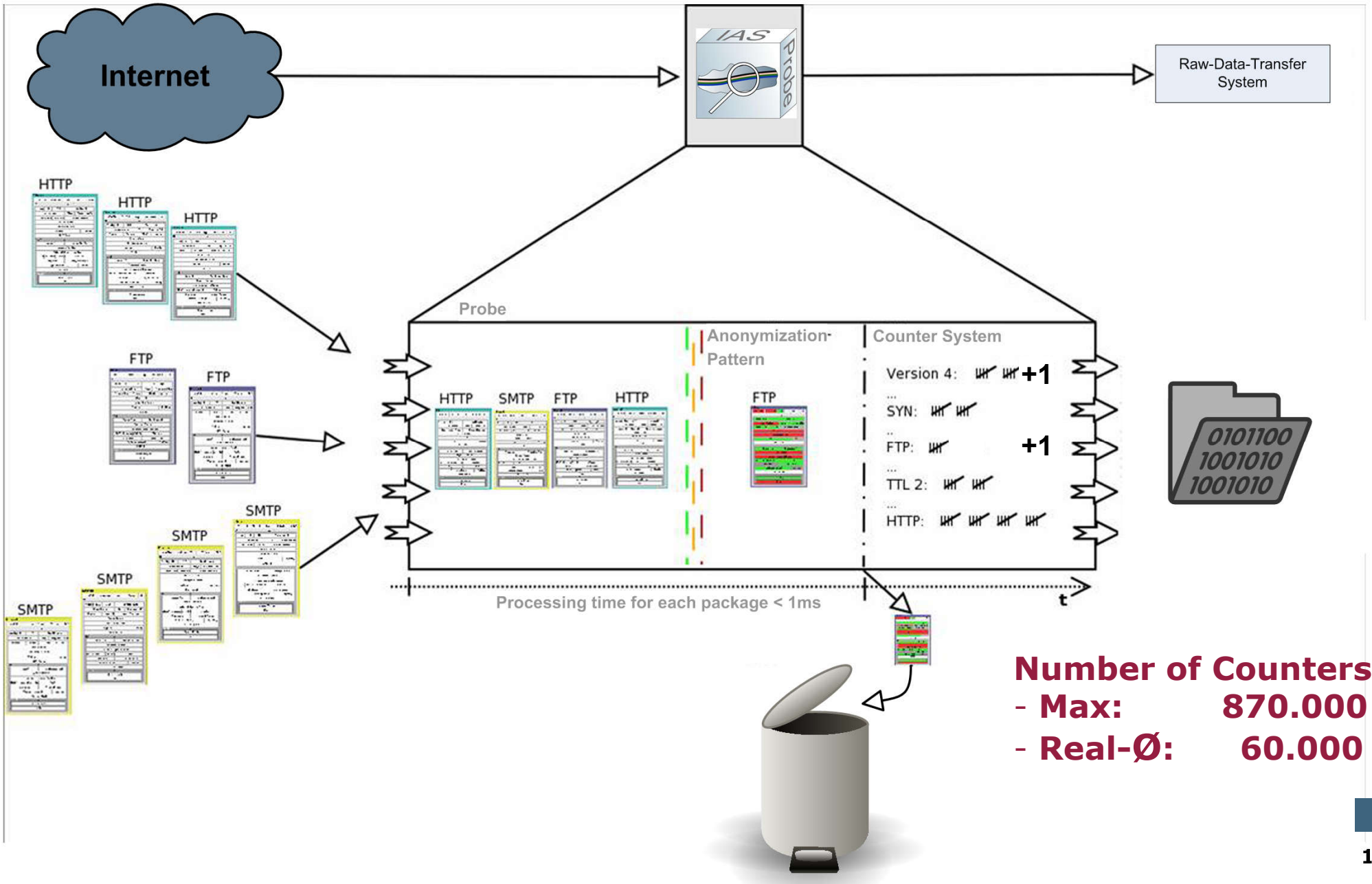
Description of profiles, patterns and coherences, creation of a knowledge base.

Outline of the current state of the internet.

Detection of attacks and of deflections.

Forecast of patterns and attacks.

Internet Analysis System (3/3)
→ Counting of header information

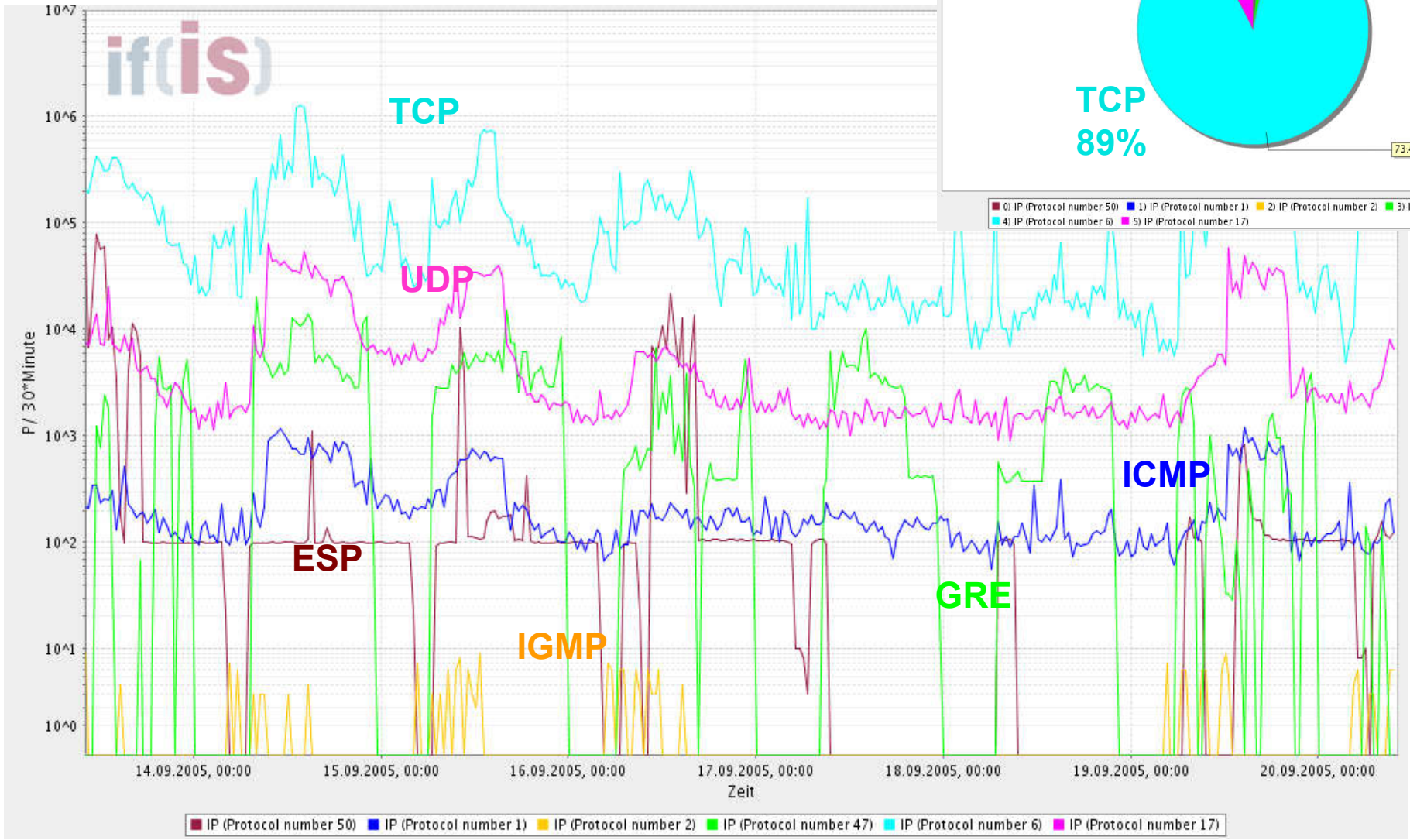


Number of Counters:
- **Max: 870.000**
- **Real-Ø: 60.000**

IAS: Current State of Development
→ Result: Knowledge base

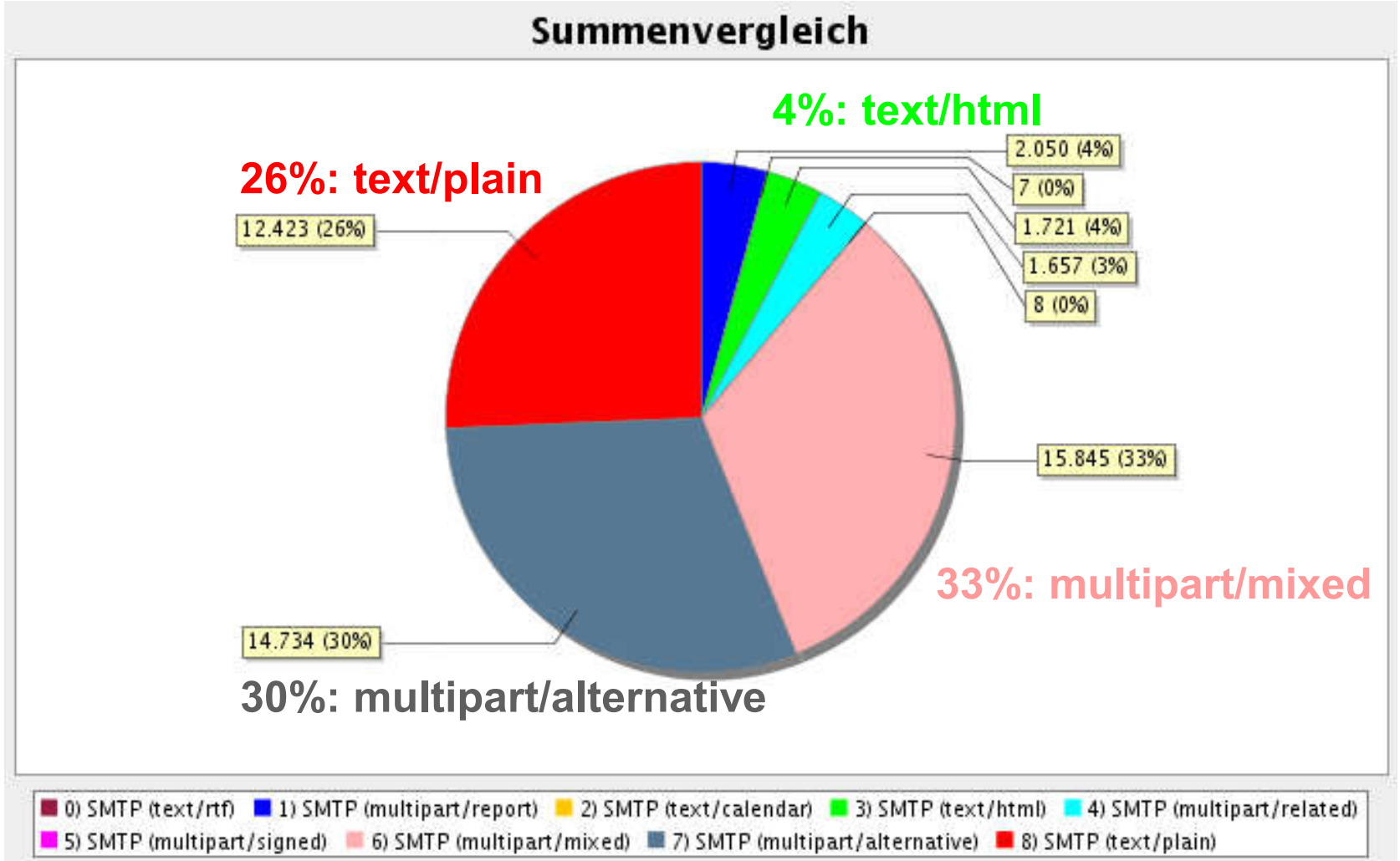
- **Distribution of Transport Protocols**

  Profile shaping und trend development



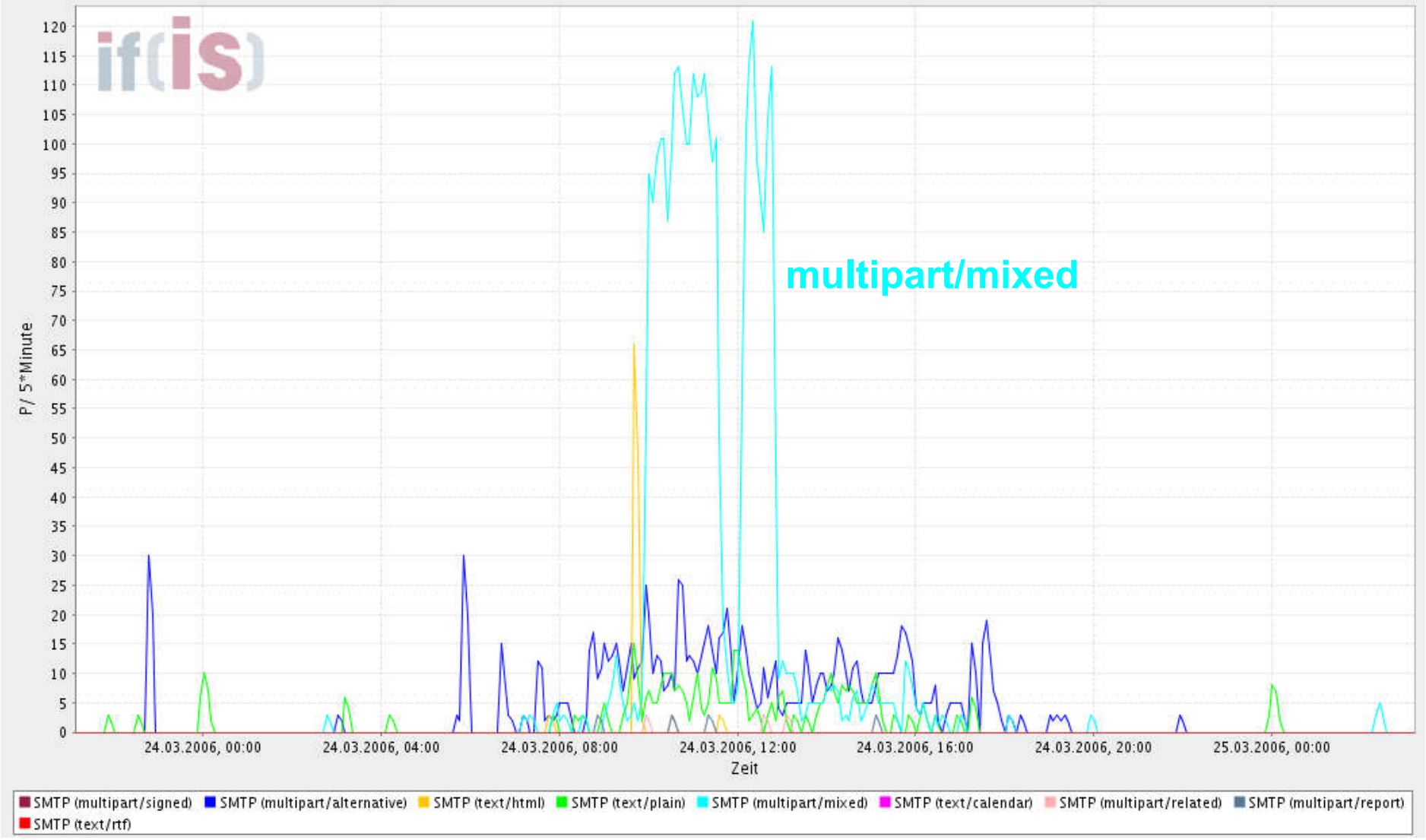
IAS: Current State of Development
→ Result: Knowledge base

- **SMTP Content Type**
  - 60% “text” Mails
  - 33 % “attachments”



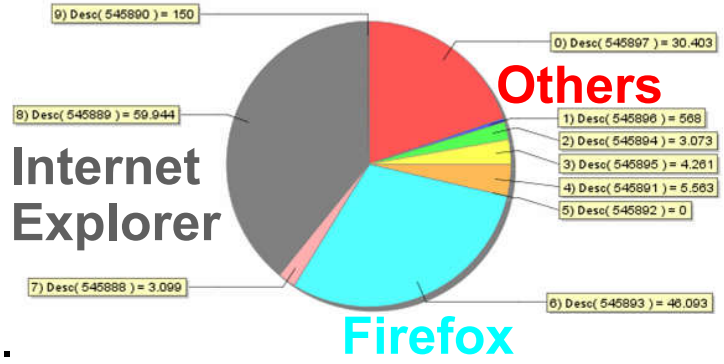
IAS: Current State of Development
→ Result: Detection of attacks

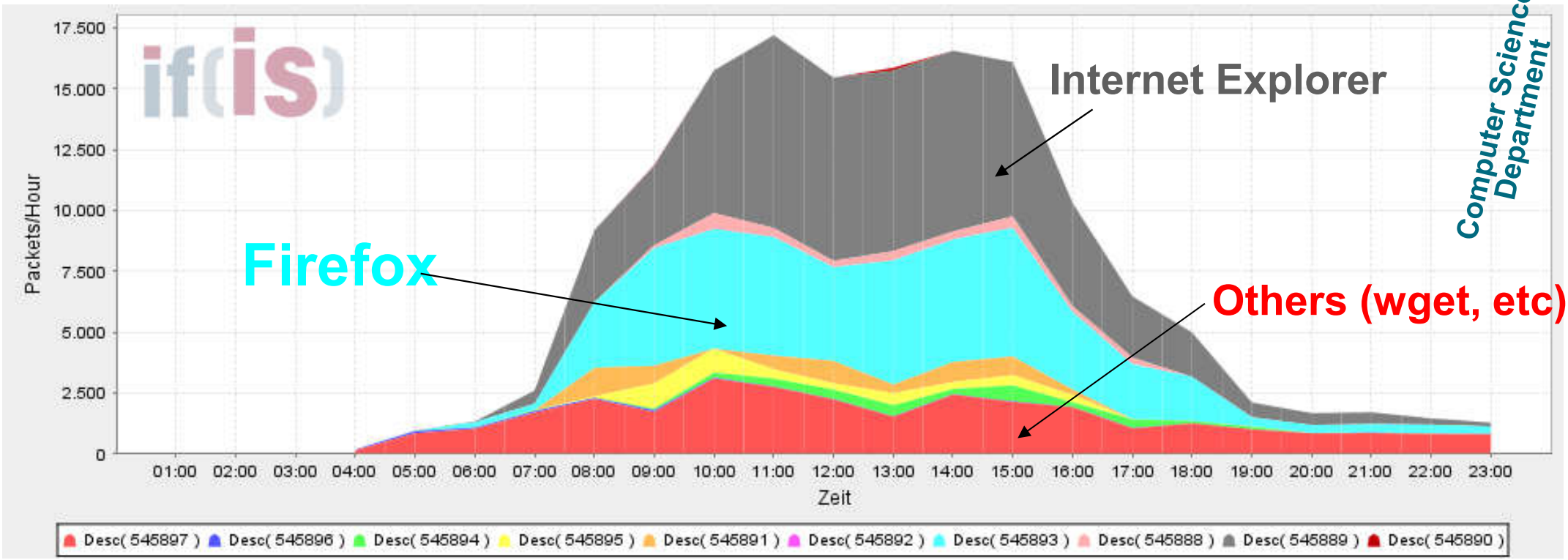
- **SMTP Content Type**
  - Temporarily more e-mails witch attachments -> Mail-Virus!



IAS: Current State of Development
→ Result: Technology trend

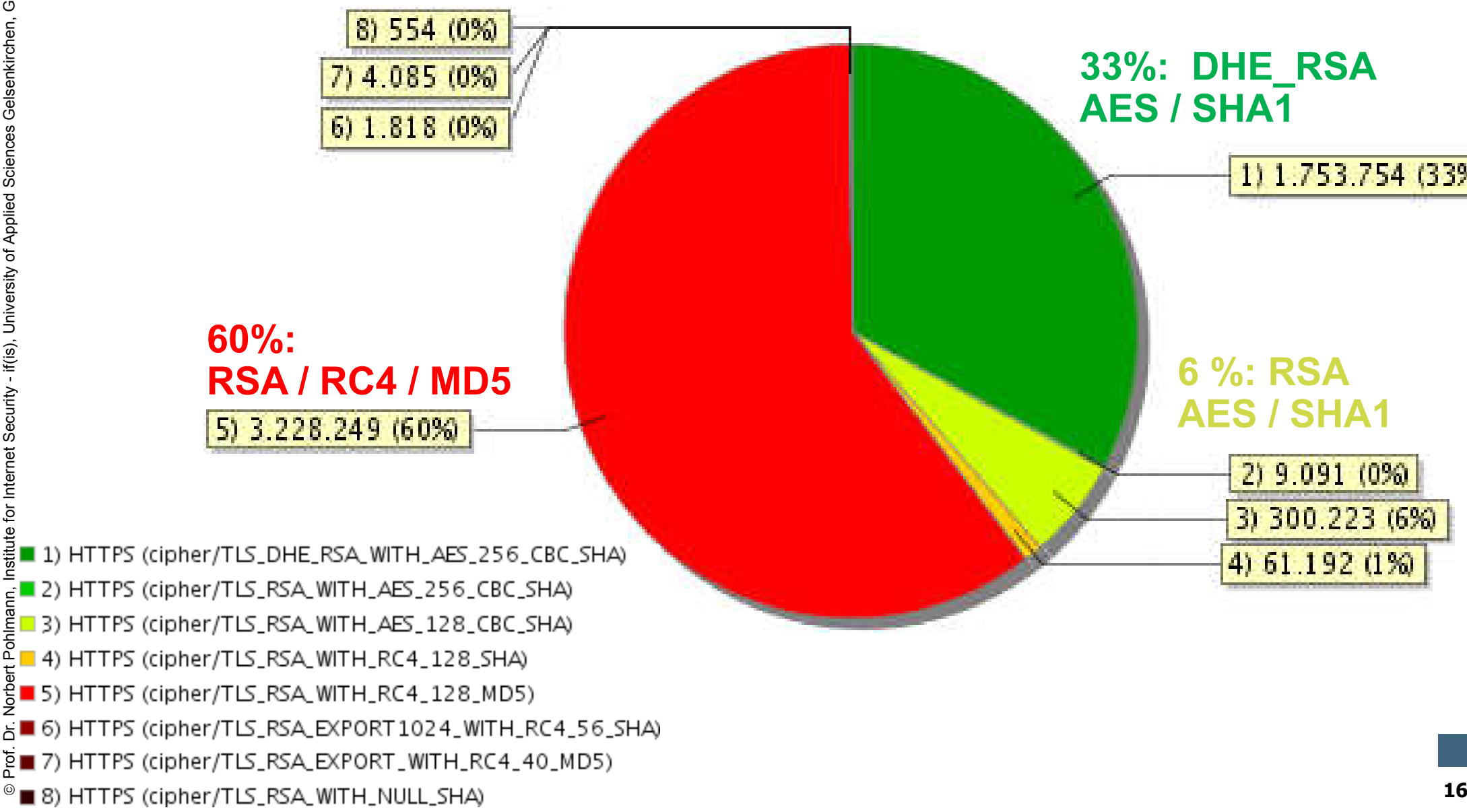
- **Distribution of browsers (Technology Trend)**
  - Diurnal profile
  - Differences between manual use (e.g. Internet Explorer und Firefox) and automated use (z.B. wget) are detectable.



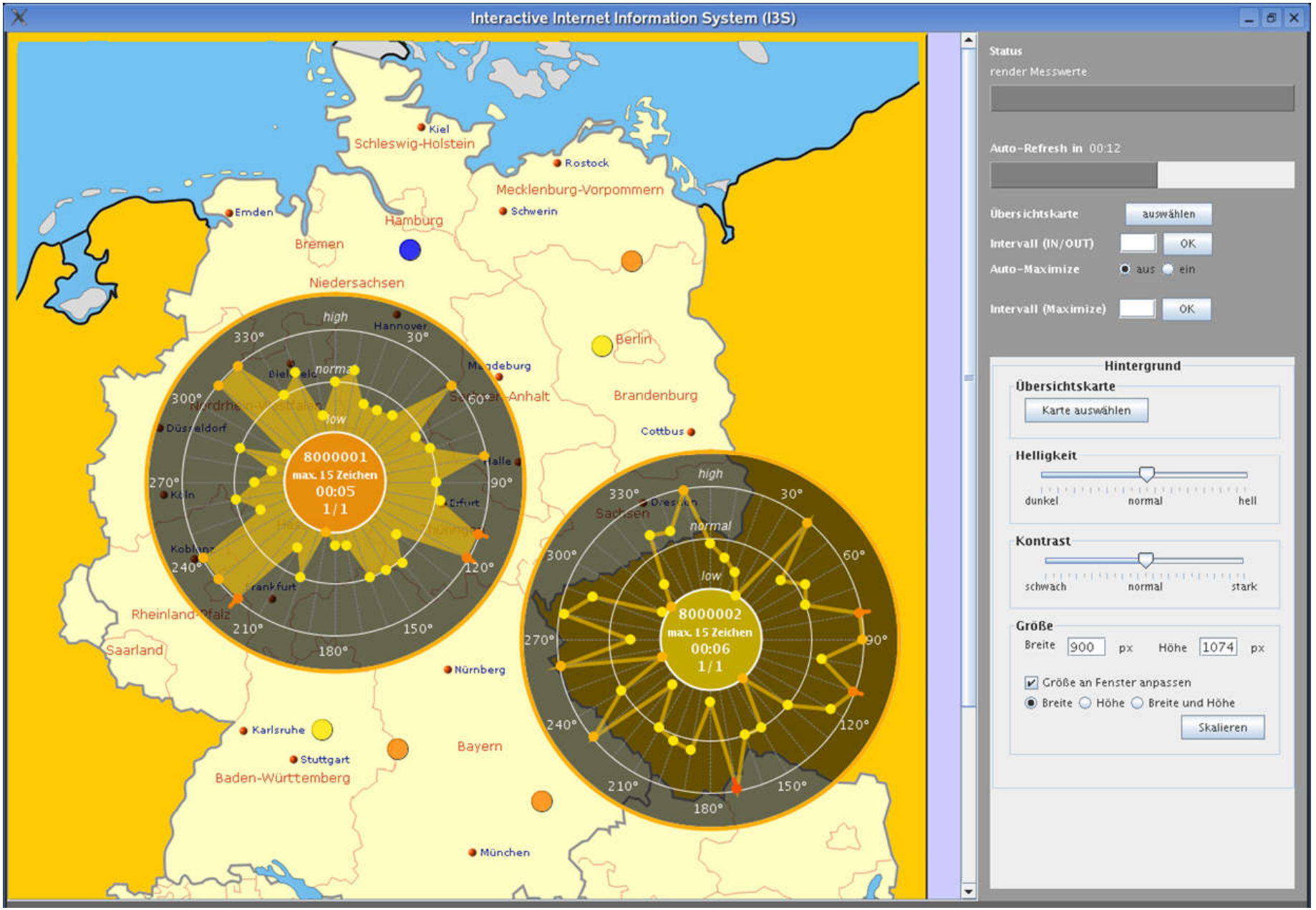


IAS: Current State of Development
→ Result: Awareness (Crypto used TLS)

!! 0.1 %: RSA / Export (40) / SHA1 and 0.01 %: RSA / NULL / SHA1 !!



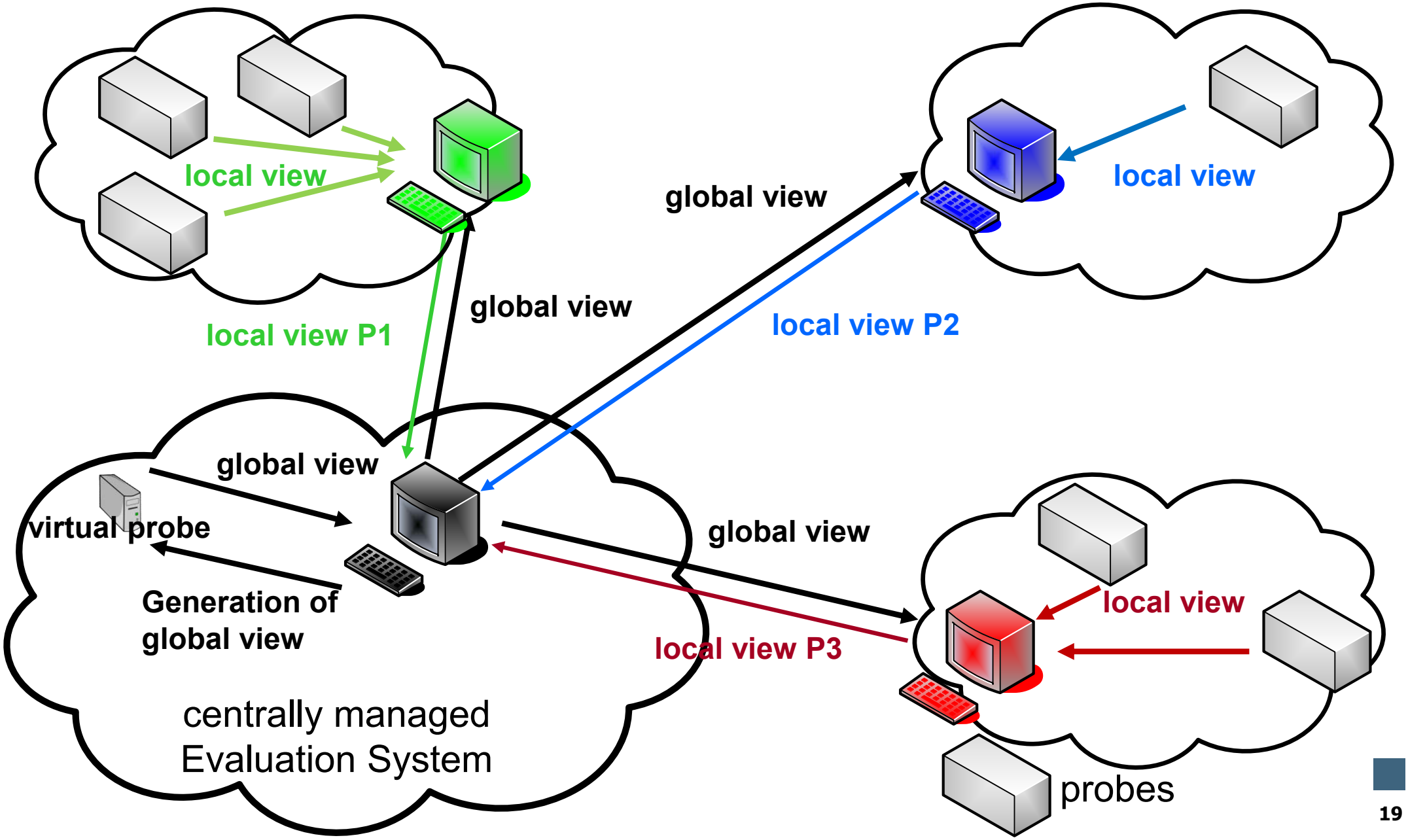
IAS: Current State of Development
→ Continuous situation awareness



Content

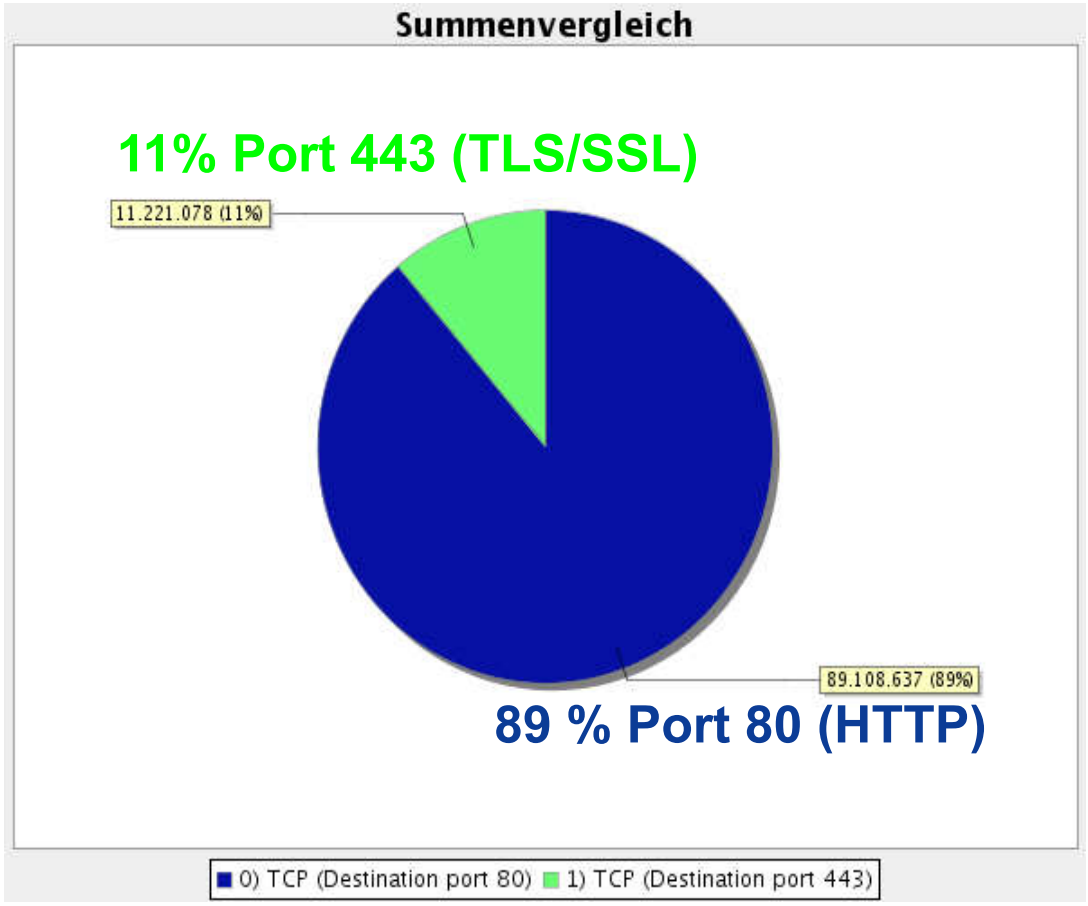
- Structure of the Internet
- Internet Analysis System (IAS)
  (Idea, Targets, Approach, Results)
- **Global view**
- Summary

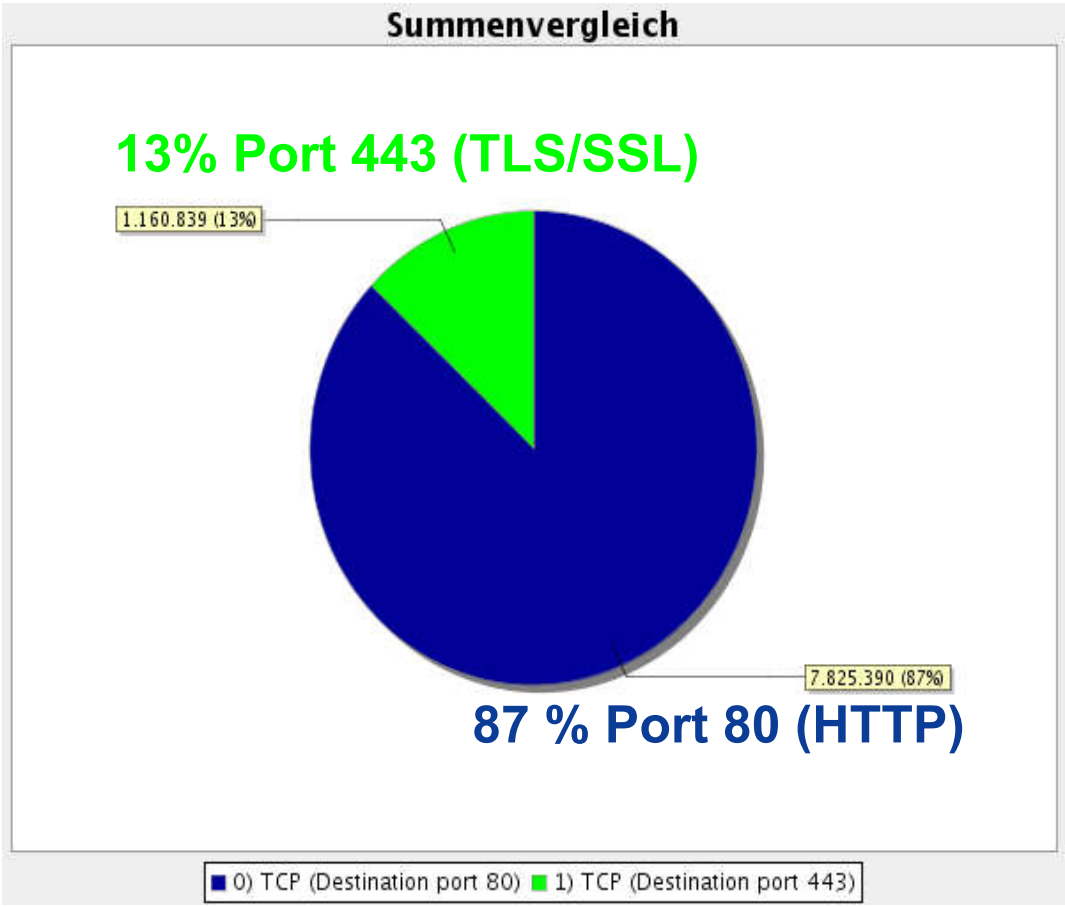
Idea of the global view →Overview



Idea of the global view
→ Relation of used protocols

- Global representation of the relation of different protocols



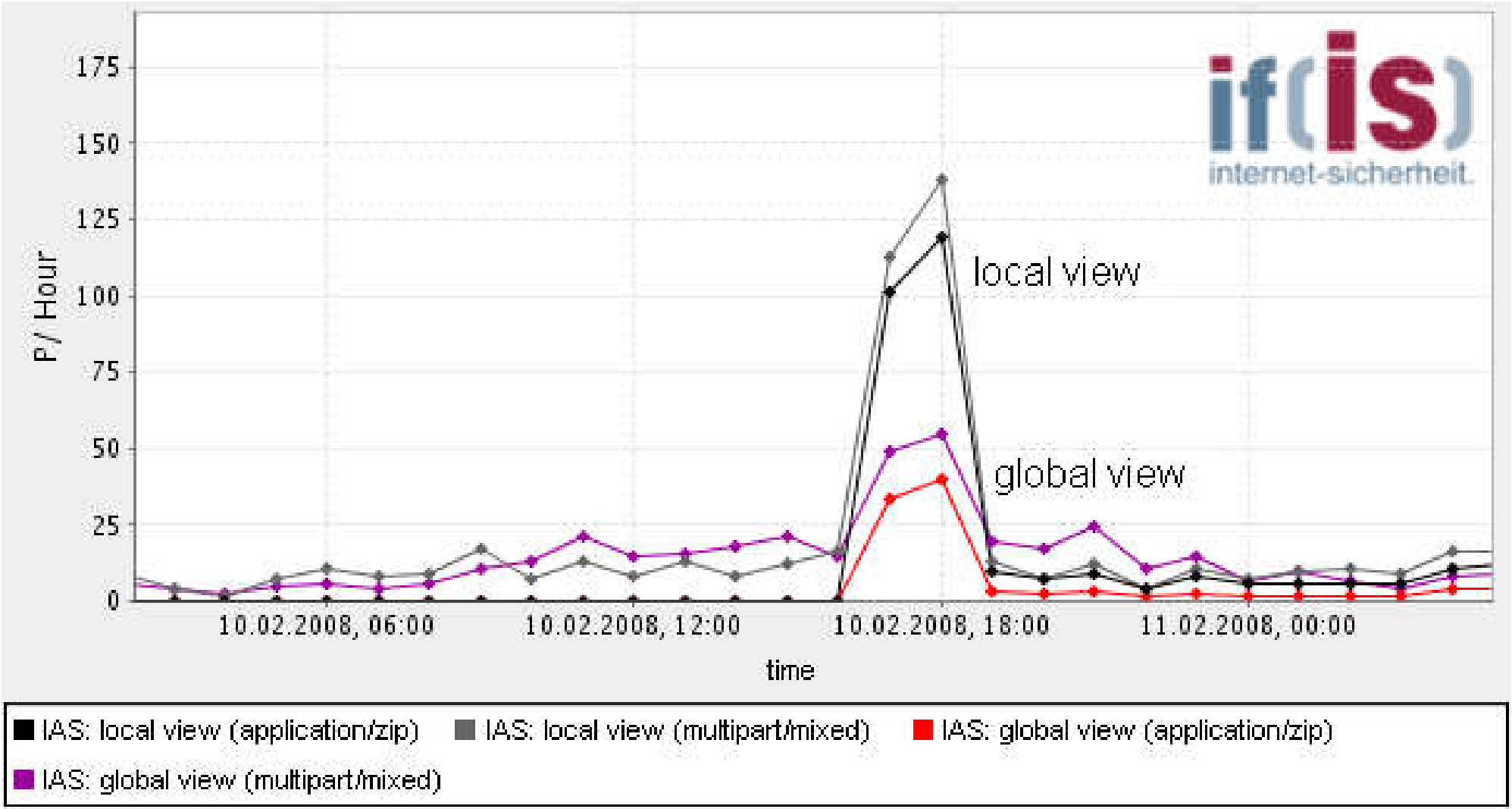


local view

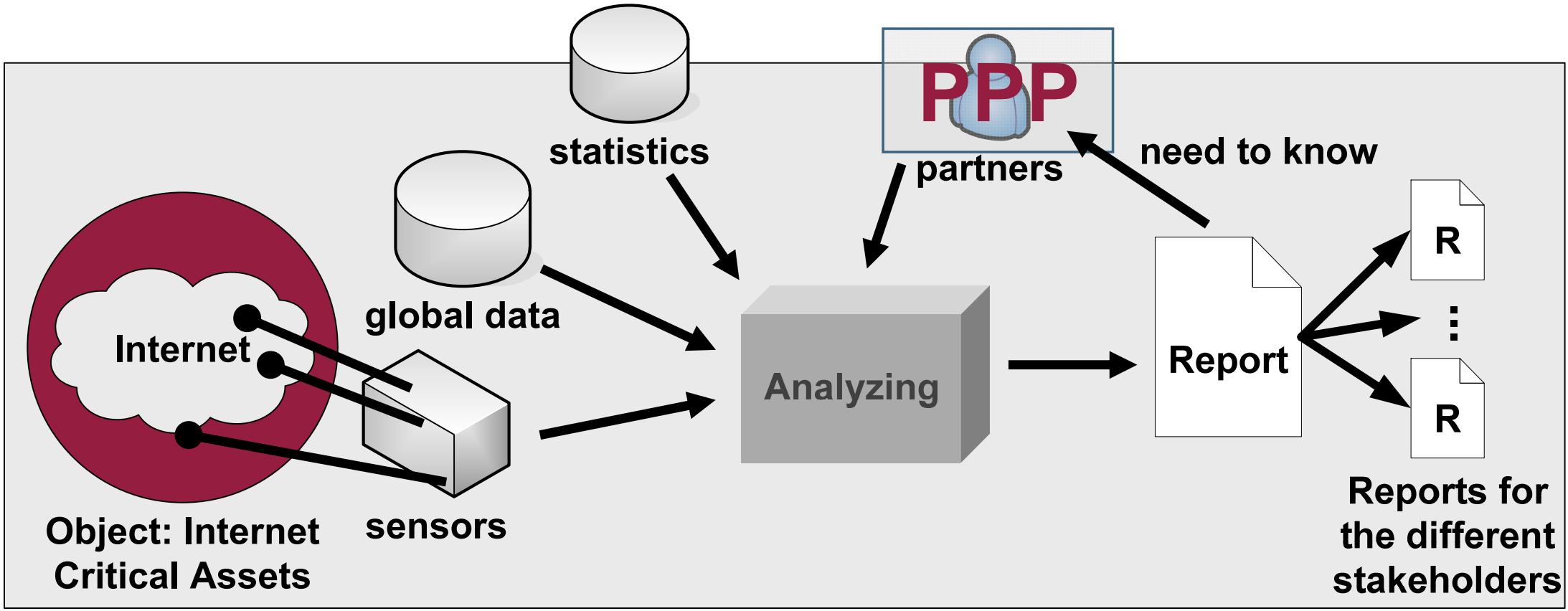
global view

Anomaly detection
→ Malware

- Dangers on the internet (e.g.: attachment ZIP)



European Internet Situation Awareness →Project idea (together with JRC)



- **This will help to:**
  - improve the stability and trustworthiness of the European Internet,
  - raise awareness for critical processes or components, and
  - find out more about the European Internet and its users in order to better support to their needs and service demands

Content

- Main Research Focus of the Institute for Internet Security - if(is)
- Structure of the Internet
- Internet Analysis System (IAS) (Idea, Targets, Approach, Results)
- Global view
- **Summary**

European Internet Security Status
→ Summary

- **Internet**
  - The internet is a critical infrastructure for our society
  - We need a trusted infrastructure to protect our future
  - Organisations running the infrastructure need to cooperate

- **We need the global view of the Internet**
  - To identify the current status
  - To see the new trends
  - To get ´early warnings´ to reduce damage
  - To make forecasts which help us to avoid damage

- Analogical to natural disaster warning systems, like the Tsunami warning system, we need a warning system for the internet to be able to issue countermeasures before the actual threat strikes at us.

- **If you can‘t measure it, you can‘t manage it!**

- **Let us start together now!**

Fachhochschule Gelsenkirchen

European Internet Situation Awareness → The Global View

Thank you for your attention!
Questions?

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.