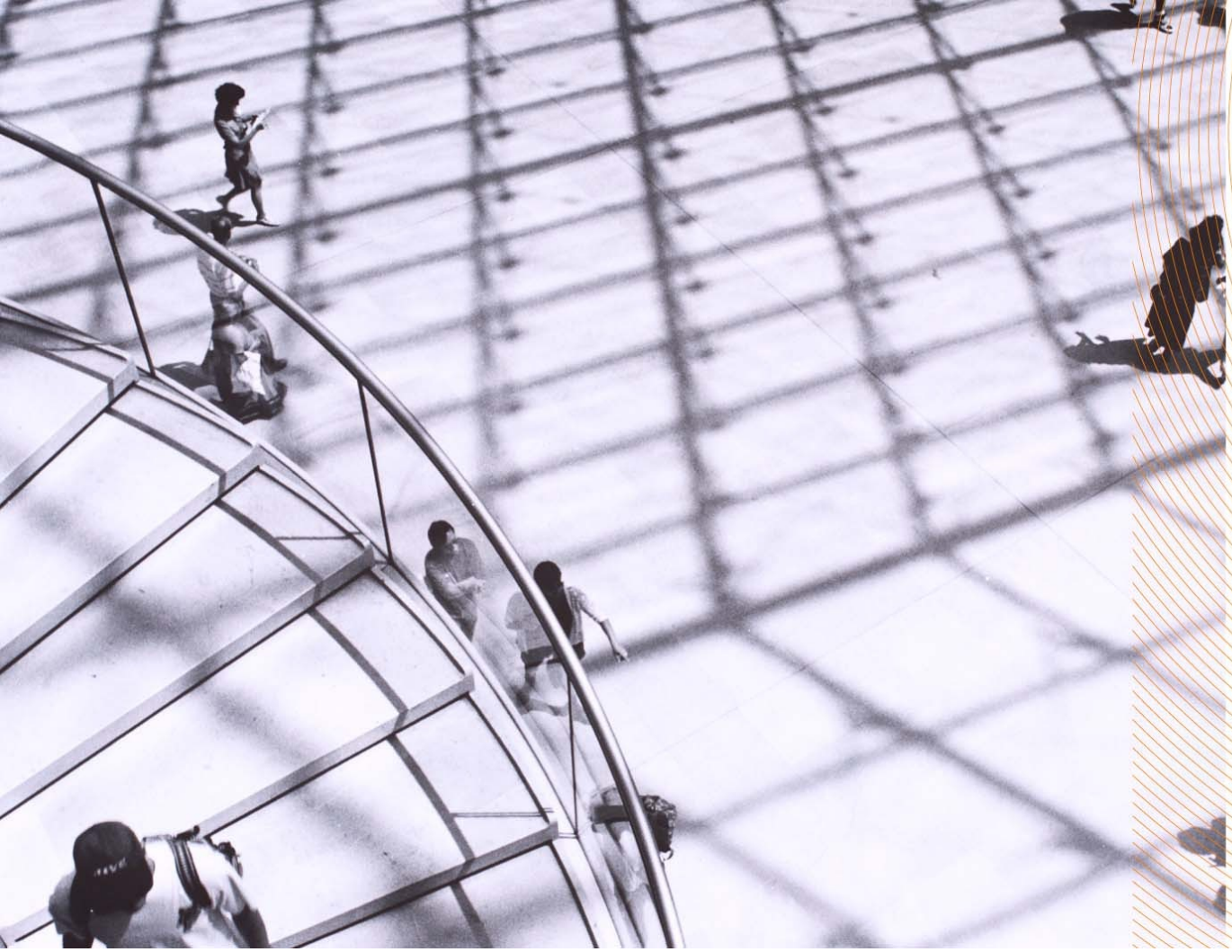


SURFcert Operations

OSCT Face 2 Face Meeting, March 23rd, 2010

Xander Jansen SURFcert

Topics

- SURFnet, the NREN
- SURFcert, the CSIRT
- Incident Handling
- Tools

SURFnet

Dutch National Research & Education Network (NREN)

- Not-for-profit organization, 80 employees
- Owned by the research and education community
- > 1.000.000 end-users from 160 connected institutions

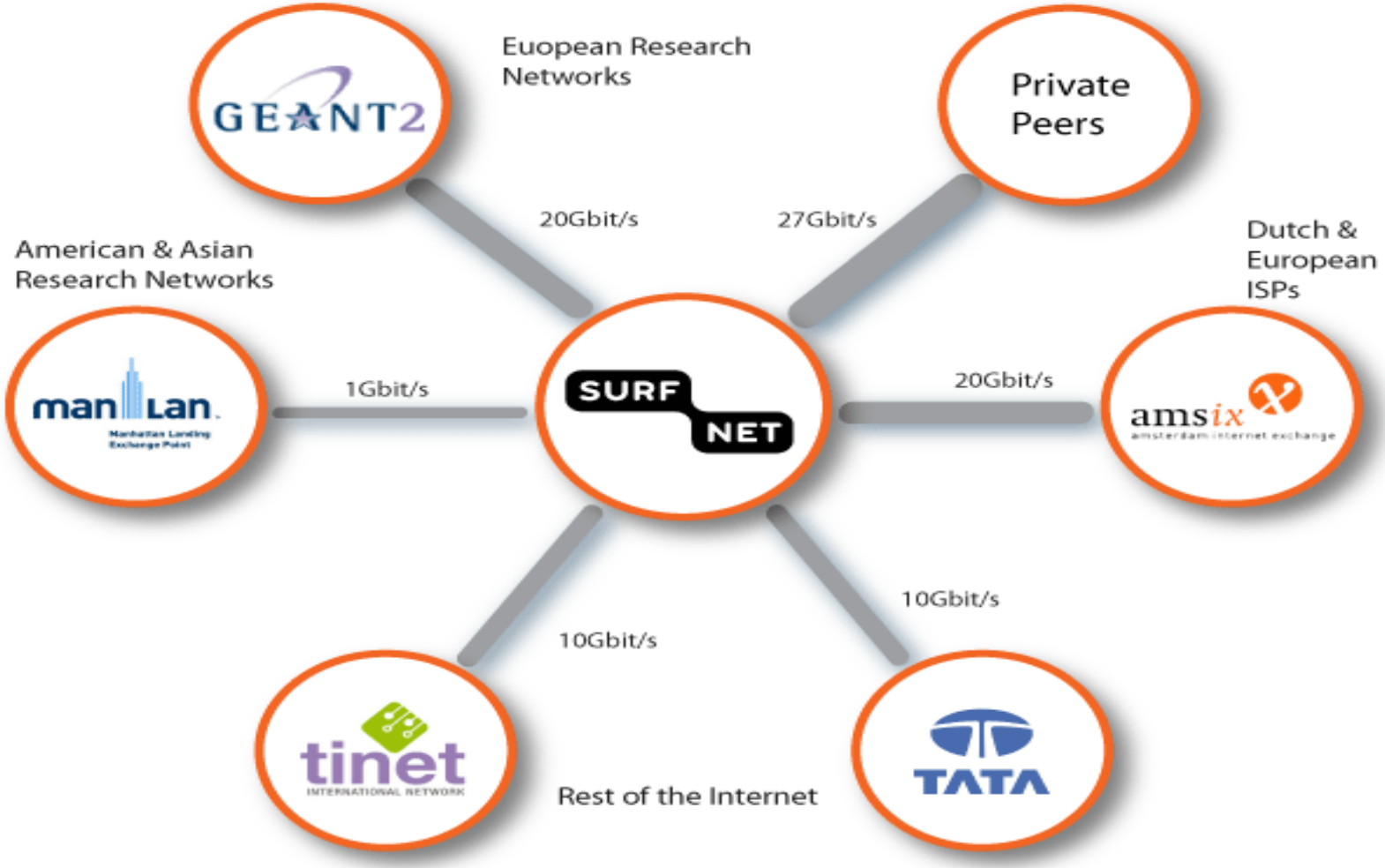
Provides advanced services to research and education

- High performance networking
- Authentication and authorization services
- Advanced online multimedia collaboration
- Innovation projects GigaPort3 and SURFworks

SURFnet6

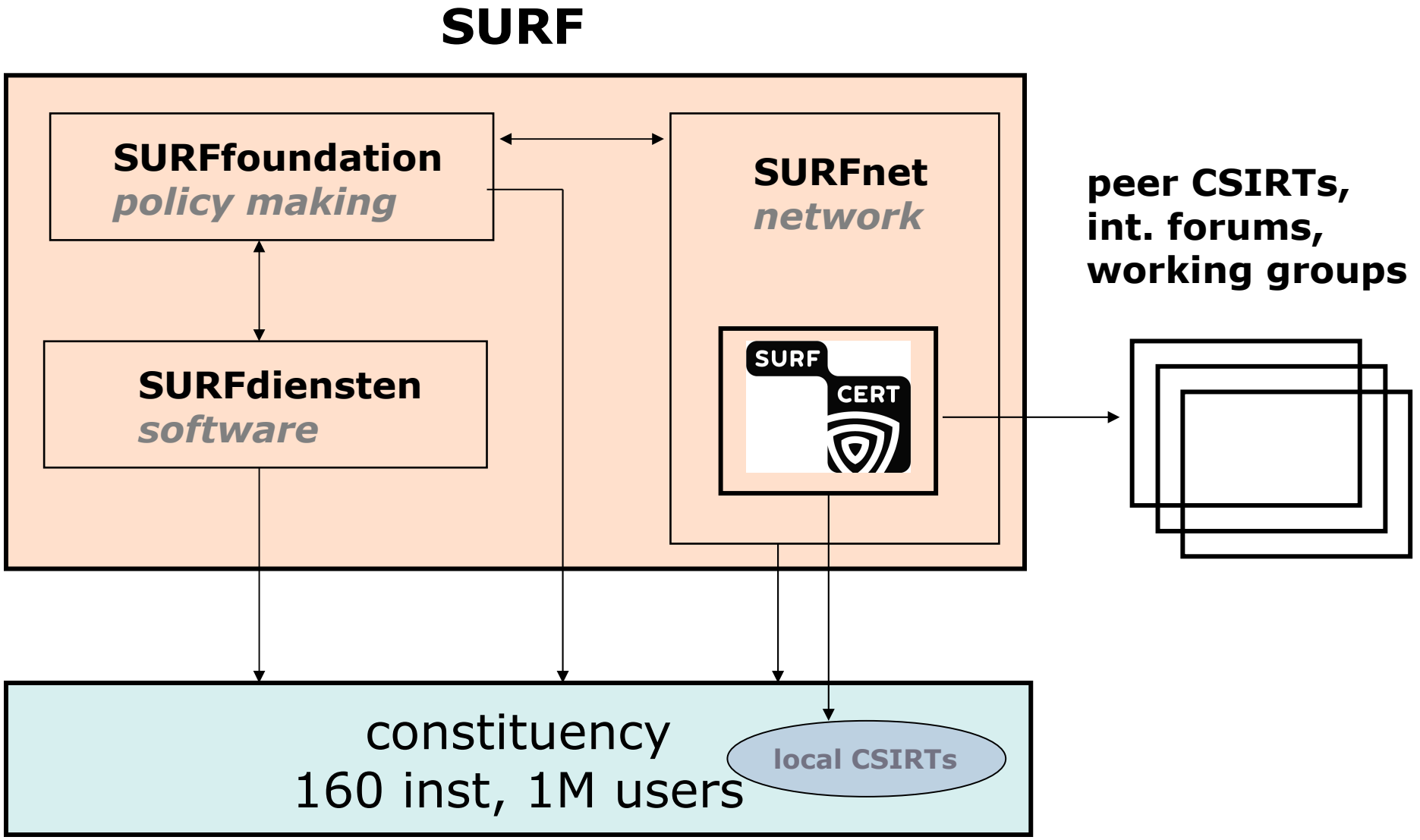
- One of the most advanced networks in the world
- More than 8.000 km dark fiber
- Own photonic network
- Hybryd networkservices
  - IP + lightpaths
  - Dynamic lightpaths

Peers and upstreams



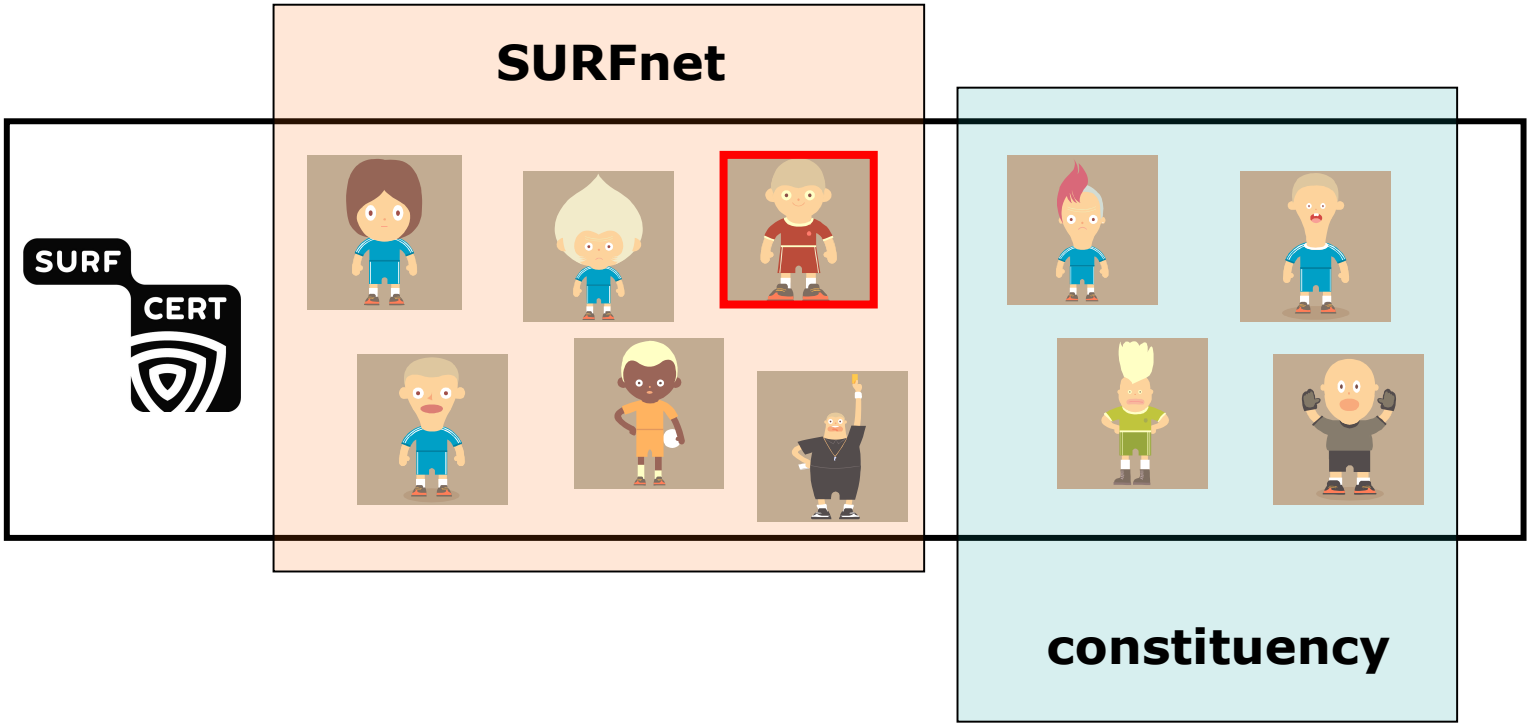
Global IP connectivity - June 2009

Team Context



Face 2 Face

Team Structure



What do we do?

Reactive CSIRT services (SURFcert):

- alerts and warnings
  - advisories (bought-in service from Secunia)
- **incident handling**

Proactive 'CSIRT' services (SURFnet and SURFcert):

- contributing to awareness raising (CSY)
- whitepapers and best current practices
- sharing of knowledge and expertise:
  - light weight seminar sessions (quarterly)
  - annual conference (SURFcert/SURFibo)
  - collaboration on national and international level: o-IRT-o, TF-CSIRT, TI, FIRST,….
- development (Honeyspider, SURFids)

Officer on duty

- 24x7 emergency phone
  - operated by the SURFnet Helpdesk (UCI/RU)
  - only dispatching following strict procedures

- Week shifts for SURFcert team members
  - one shift per 10 weeks
  - 24x7 stand-by
  - regular mailchecks outside office hours
  - handles all incoming incidents

- Back-office, off-loading and specific expertise available from other team members

Sources

Manual:

- 'Free format' mail
- Phone (regular and emergency)
- Fax (mainly law enforcement)

(Semi-)automated:

- netflow alerts
- daily reports from trusted sources
  - bots, infections, spam, malware, defacing…
- feedback loops (mainly spam reports)
- other automatable reports

Destinations

Consituency:

- Connected institutions
  - Site Security Contact (person)
  - Security Entry Point (team)
- Special Interest Groups

'The outside world':

- o-IRT-o teams (dutch)
- Trusted Introducer teams (european)
- FIRST teams (worldwide)
- *OSCT/EGI*
- *abuse@……*

Tools (1/2)

Workflow/Incident tracking

- AIRT Application for Incident Response Teams
  - IP based incident tracking
  - Constituencies
    - networks
    - contacts
  - Import queue for automated import of new incidents from honeypots, IDSes, feedback loops etc…
  - Mail templates (including IODEF)

Tools (2/2)

- Detection
  - netflow
    - nfsen including ‘events’
    - Arbor Peakflow (traffic anomalies)
  - SURFids (honeypot sensor network)

- Analysis
  - nfsen (forensics)

- Mitigation
  - ACL/null route (handled by the SURFnet NOC)
  - (experimental) Arbor TMS

Questions?

Are we prepared for the GRID ?