



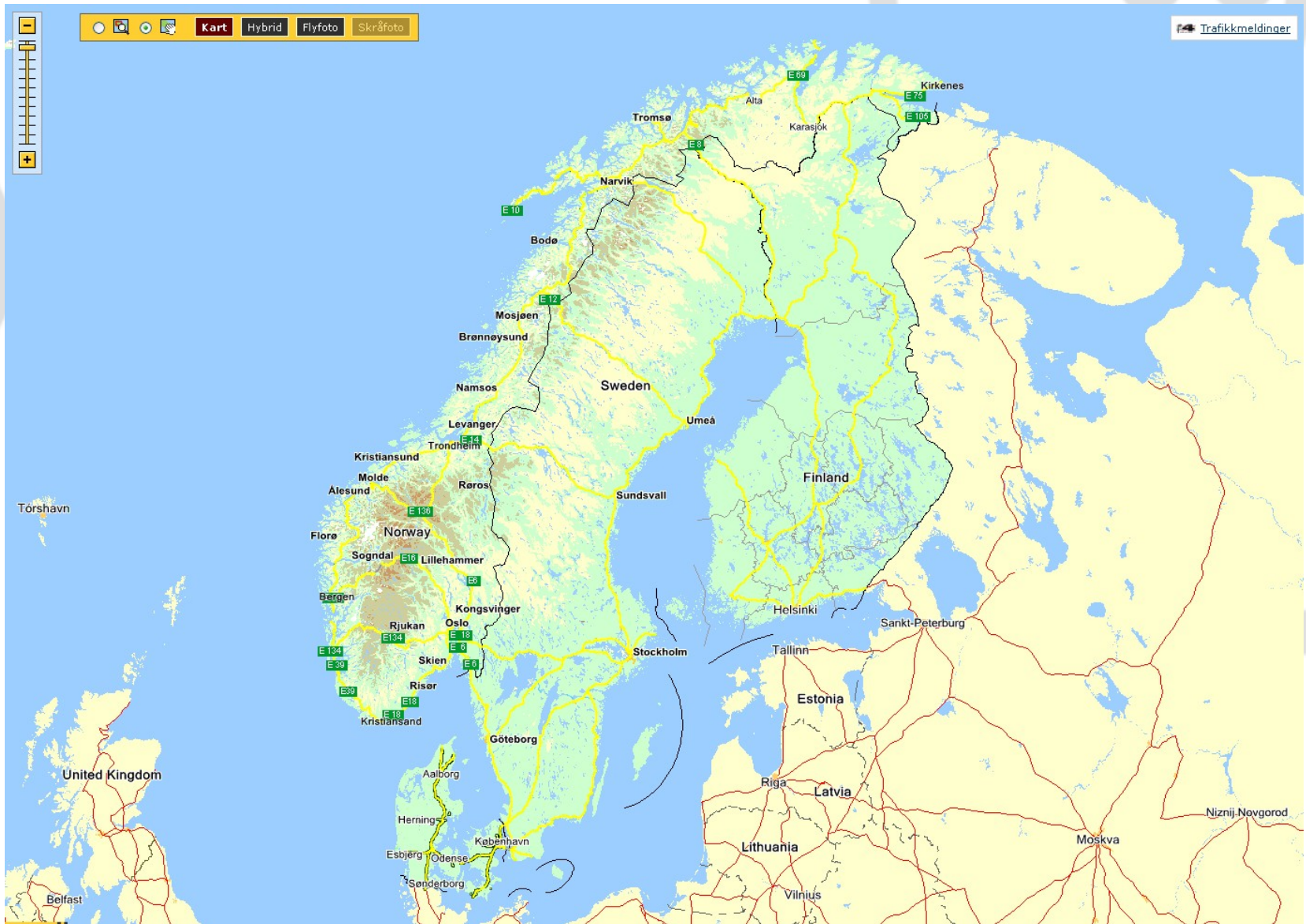
24.Th TF-CSIRT
Team presentation:

UNINETT CERT

May 14th 2008
Per Arne Enstad

UNINETT? What? where?

- UNINETT develops and operates the Norwegian national research network, which links together domestic educational and research institutions and connects them into international networks
- Short form: The norwegian NREN



**So, you think *this* was far
north..?**

So, you think *this* was far north..?



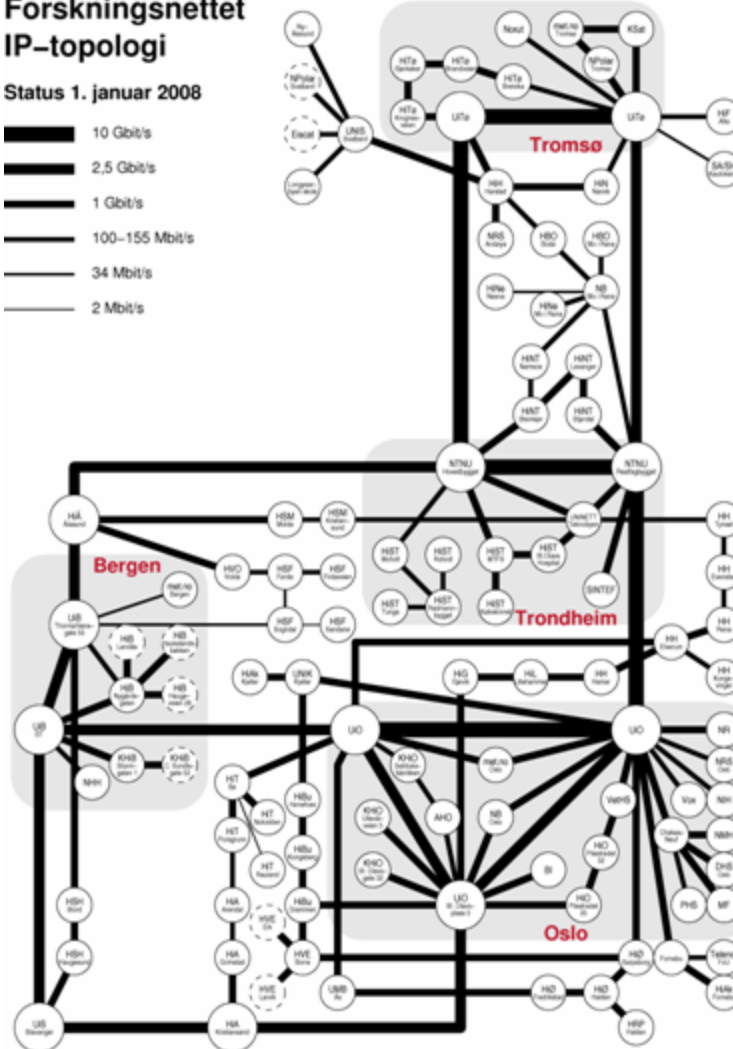
UNINETT

- Key figures:
 - ◆ Serving 75+ customers
 - ◆ Approx. 300 POPs
 - ◆ Approx. 400K end users
 - ◆ Approx. 100 employees
 - ★ ...and counting

Our main product:

Forskningsnettet IP-topologi

Status 1. januar 2008



UNINETT CERT

- Established 1995
- Constituency:
 - ◆ All customers within our address space
- Virtual team organized within the NOC
 - ◆ Core team: 4 persons working part time
- Member of FIRST since 2000
- TI Accredited Team since 2001

UNINETT CERT

- Work profile:
 - ◆ Incident prevention
 - ★ Security policy deployment
 - ★ Security audits
 - ★ IRT-courses
 - ★ Best practices
 - ◆ Incident handling
 - ★ Mostly coordination, but still a few "hands on" cases
 - ★ Workload: approx 5000 incidents/year

Current development efforts

- Further RTIR-work
 - ◆ Extensions and integration
- Passive DNS monitoring
- Flow visualisation
 - ◆ Ongoing masters thesis
- Anomaly detection
 - ◆ Testing techniques of varying complexity
- Child Sexual Abuse Anti-Distribution Filter

Current development efforts (contd)

- Scripting and extending nfdump/nfsen
 - ◆ e.g. internal per-organization aggregation
- IPv6 flow collection

Contact info:

- Report an incident:
cert@uninett.no
- Any other business:
cert-info@uninett.no

Questions?

