Capturing a Cyber defence exercise

Who is Dennis Andersson?

- Master of Engineering at Linköping University
  - Major in Computer Science
- Employee at FOI since 2004
  - Researching evaluation of distributed tactical operations
- Ph.D. student at Linköping University
  - Automated event classification from heterogeneous datasets
  - Methods and tools for After-Action Review (AAR)
  - Fusion-based anomaly detection

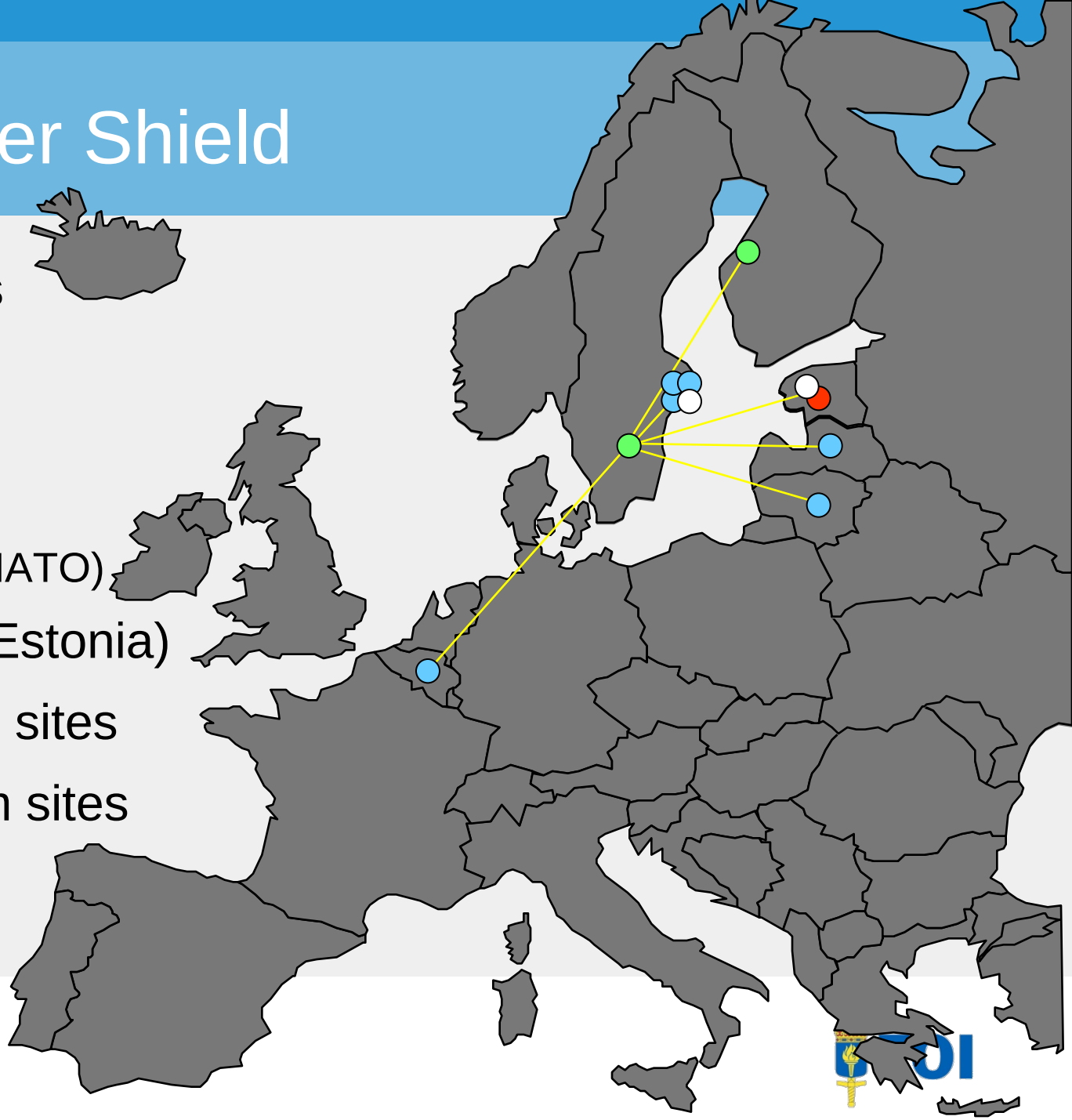
FOI

Baltic Cyber Shield

- Scenario-driven 2-day multinational CDX in 2010
  - Swedish side coordinated by MSB
- Motivated by cyber attacks on Estonia 2007
- Main objectives
  - Improve capability of conducting technical IT security exercises
  - Investigate how to study IT attacks and defence of critical infrastructure

Baltic Cyber Shield

- 6 blue teams
  - 3 Swedish
  - 1 Latvian
  - 1 Lithuanian
  - 1 Belgian (NATO)
- 1 red team (Estonia)
- 2 white team sites
- 2 green team sites

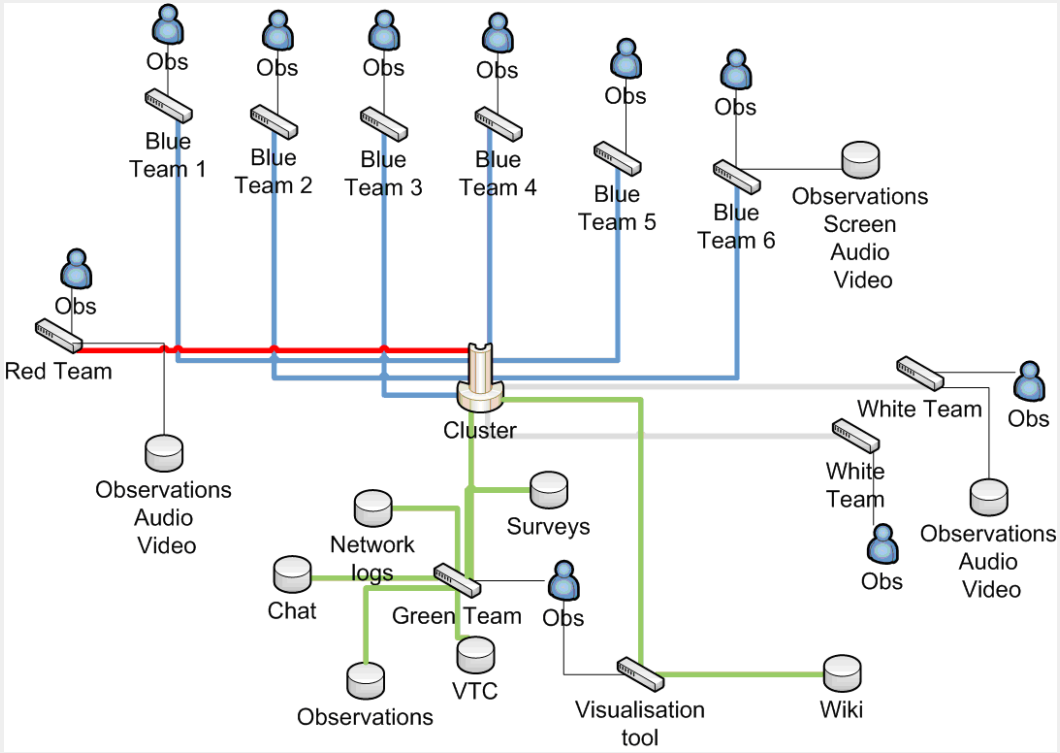


Baltic Cyber Shield

- Mixed-reality
  - Internet simulated at FOI cluster
  - Isolated corporate networks connect to cluster through VPN tunnels
  - Corporate factory replicas accessible through the cluster

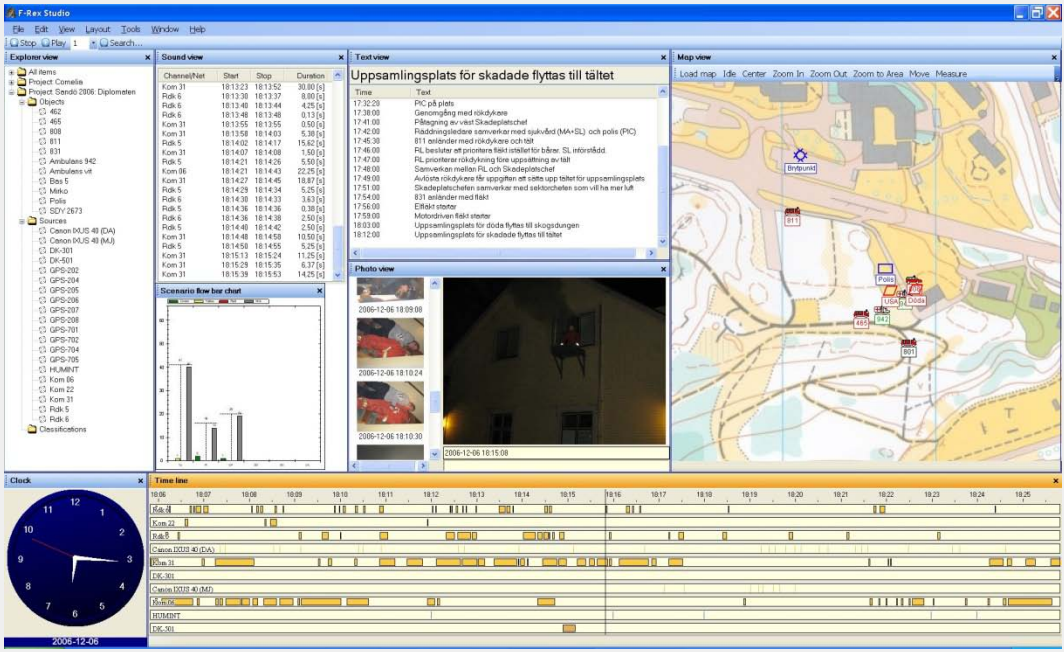
Data collection

- Cover both behavioural and technical aspects
- 3 TB of collected data
  - IP traffic
  - network status data
  - processor utilization
  - observation reports
  - surveys
  - computer screens
  - surveillance video
  - audio (intra-team)
  - e-mail communication
  - chat logs



Motivation for data collection

- Enable after-action reviews
- Enable long-term studies of one exercise, and validation of results
- Ongoing studies
  - Team aspects @ FOI
  - IT security assessment @ KTH and FOI
  - Event detection @ FOI
  - IDS system evaluation @ CERT-FI



Results

- General-purpose data collection in a large scale CDX is a challenging task that needs thorough preparation
- Human observers are essential
- Providing team members with pre-configured workstations simplifies data collection
- Getting the red team to report on failed attacks proved difficult

Results

- The teams' own status reports provide an excellent source of information for situational awareness and in the early stages of reconstruction
- A comprehensive dataset like the collected BCS data is a great resource for many different kind of studies