

# Experiences from establishing a national Centre for Information Security in Norway

TERENA Networking Conference 2003

Maria Bartnes Dahl & Lillian Røstad  
Centre for Information Security  
SINTEF Telecom and Informatics



2003-05-19

# Background

- Two major incidents recent years:
  - Telenor: Main and backup cable cut at the same time
    - Large areas without telephone connection, >5 hrs
  - EDB Teamco: One human mistake - all Internet banking services unavailable
    - A whole week until normal operation restored
- Increased focus on information security
  - Have realised how vulnerable the society is
  - Vulnerability Committee and a national strategy

# Establishment of SIS (I)

- Commissioned by the Norwegian Ministry of Trade and Industry
- Preliminary duration: Apr 1<sup>st</sup> 2002 - Dec 31<sup>st</sup> 2004
- Part of the national strategy for reducing society's vulnerability within information and communication (ICT) technology



2003-05-19

# Establishment of SIS (II)

- Hosted by SINTEF Telecom and Informatics in collaboration with UNINETT in Trondheim
- SINTEF:
  - Foundation for Industrial and Technological Research
  - Vision: “Technology for a better society”
  - ~2000 employees
- UNINETT:
  - The Norwegian Network for Research & Education
  - Computer Emergency Response Team (CERT)



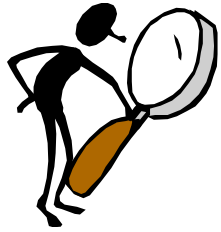
2003-05-19

# Why SINTEF?

- Alternatives:
  - Governmental departments, directorates
  - Norw. Defense - Norwegian National Security Authority
  - Private organisations
- SINTEF:
  - Large, independent research institution
  - Experience within the areas of safety and security
  - Located close to the Norwegian University of Science and Technology (NTNU) and UNINETT



2003-05-19



# Main objectives

- To survey the threats towards ICT systems in Norwegian society
- Spread knowledge and expertise about threats and their countermeasures
- Network with organisations providing similar services in other countries

# Deliverables



- Threat assessment: a dynamic updated overview of threats
- Overview of who delivers security services and products
- Increase awareness about security in both private and public sectors
- Establish a network of relevant contacts

# Long-term objective

To be responsible for the national coordination of tasks within incident response, warning, response of threats and attacks, and exchange of expertise.

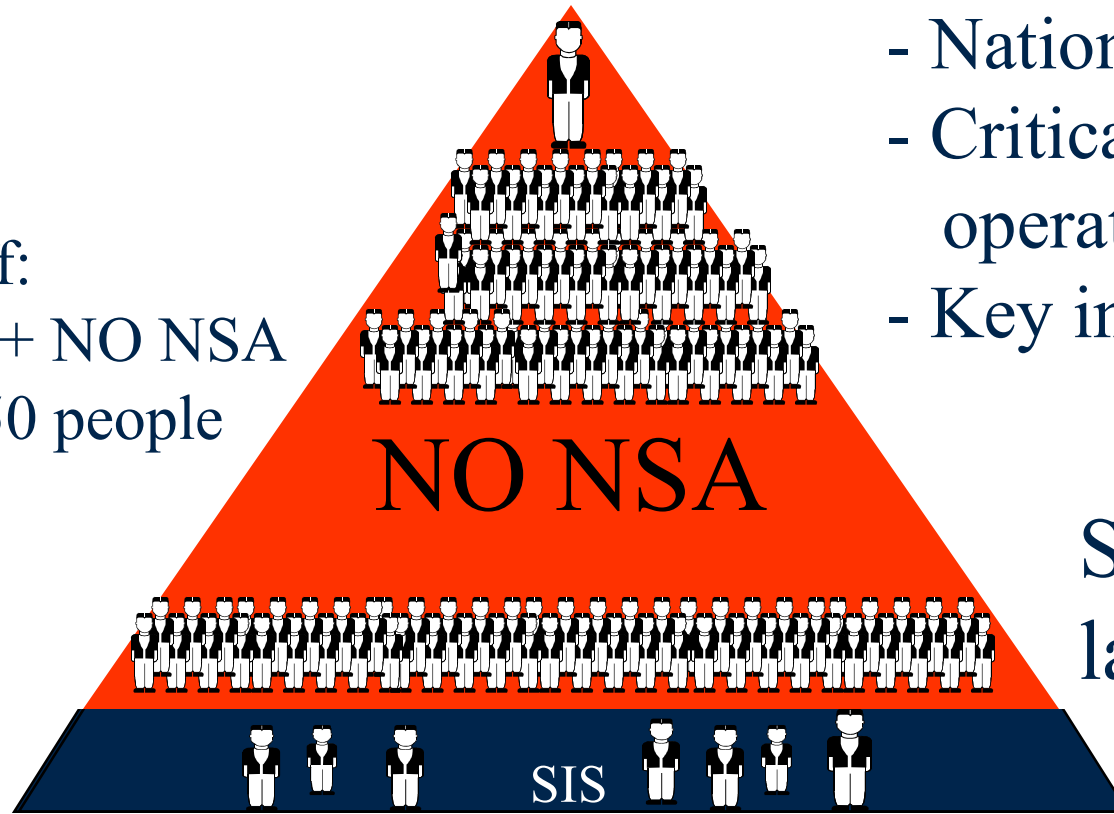
- In trial period not responsible for security and preparedness in emergency situations



# SIS complements existing efforts

*Degree of protection*

Staff:  
SIS + NO NSA  
≈ 150 people



- National security
- Critical societal operations
- Key industry

Society at large

*Extent*



2003-05-19

# Current status

- Premises approved according to the Norwegian Security Act
  - Approved for handling classified information
- Fully staffed as of Jan 1<sup>st</sup> 2003:
  - Seven people
  - Educated and/or work experienced within information security
- Web page: <http://www.norsis.no>

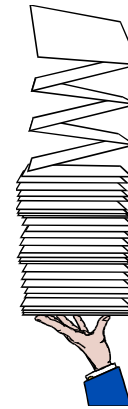


# Status - main objectives (I)

- Threat assessment:
  - formal agreements
  - based on reported incidents

AND

  - other surveys and information sources
  - June 2003 - first publication
- Challenge:
  - Evaluate tools and methods for handling and analyzing incident reports
  - Produce useful reports - determine what constitutes a useful report based on user demands



# Status - main objectives (II)

- Spread knowledge:
  - Participation in national and international conferences
  - Student tutoring
  - [www.norsis.no](http://www.norsis.no)
    - Advisories and articles
    - Best practice
    - Checklists
- Challenge:
  - Collect, sort out and communicate publicly available information
  - Supplement where necessary



# Status - main objectives (III)

- Networking:
  - Established trust relationships - contact networks in Norway
  - Nordic meeting fall 2003
  - UK - NISCC/UNIRAS
- Challenge:
  - Identify and establish relationships with key people within important organisations



# Main challenge

- Determine possible functions, goals and working methods of the centre
  - Identify main users, and
  - Figure out what is really needed by the users



# Results so far

- June 2003:
  - Publication of the first threat assessment
- Formal agreements - information exchange
- Map of the security industry in Norway
- Identified key players - both governmental and commercial

# Contact SIS:

<http://www.norsis.no>  
[post@norsis.no](mailto:post@norsis.no)

Maria Bartnes Dahl



2003-05-19