Swedish Civil Contingencies Agency

National Cyber Security Exercise (NISÖ 2012)

- Conducting the exercise and main lessons learned

Roger Holfeldt, MSB

Deputy Project Manager and Head of Ex Con

Swedish Civil Contingencies Agency

- Why, what and who?

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

Purpose

The purpose of NISÖ 2012 is to strengthen society's ability to ***manage national IT-related crises***, primarily by developing the ability to cooperate and coordinate between public and private actors.

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

Objectives

Participating organisations are to:

1. work together to create and uphold a common situational awareness.
2. work together to create consequence and operation assessment.
3. cooperate to create coordinated information to the public and media.
4. cooperate within their individual networks to facilitate coordinated decision-making for efficient use of society's collective resources (technical operative collaboration).
5. apply policies, process and routines for management of serious IT incidents.

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

Participating organisations

- Participants in NISÖ 2012 were private organisations from the energy, telecommunication and transport sectors together with responsible agencies.

- In total 17 organisations took part in the exercise

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

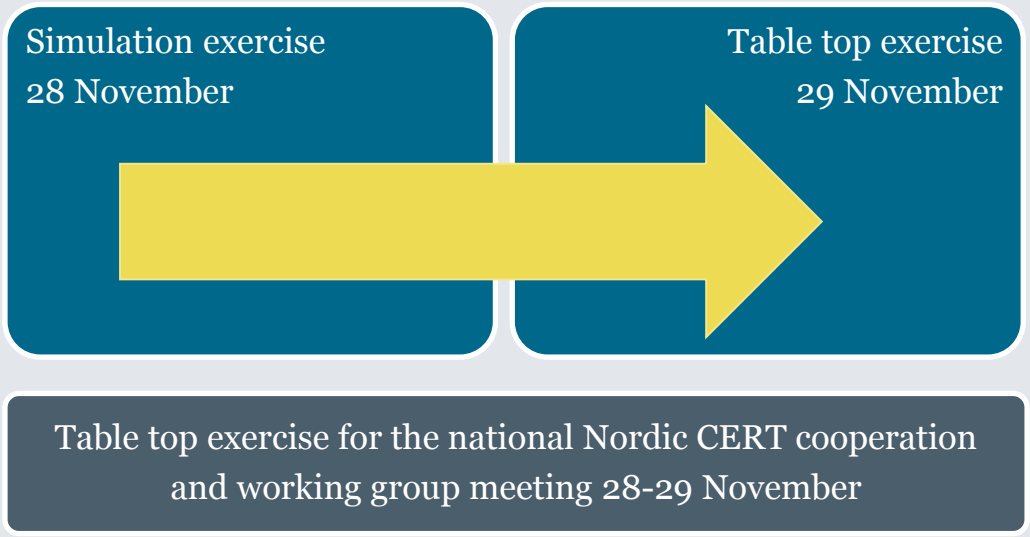
- How?

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

Exercise methods

- Real-time simulation, day 1
- Table-top, day 2
- Parallel table top exercise running two days



NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

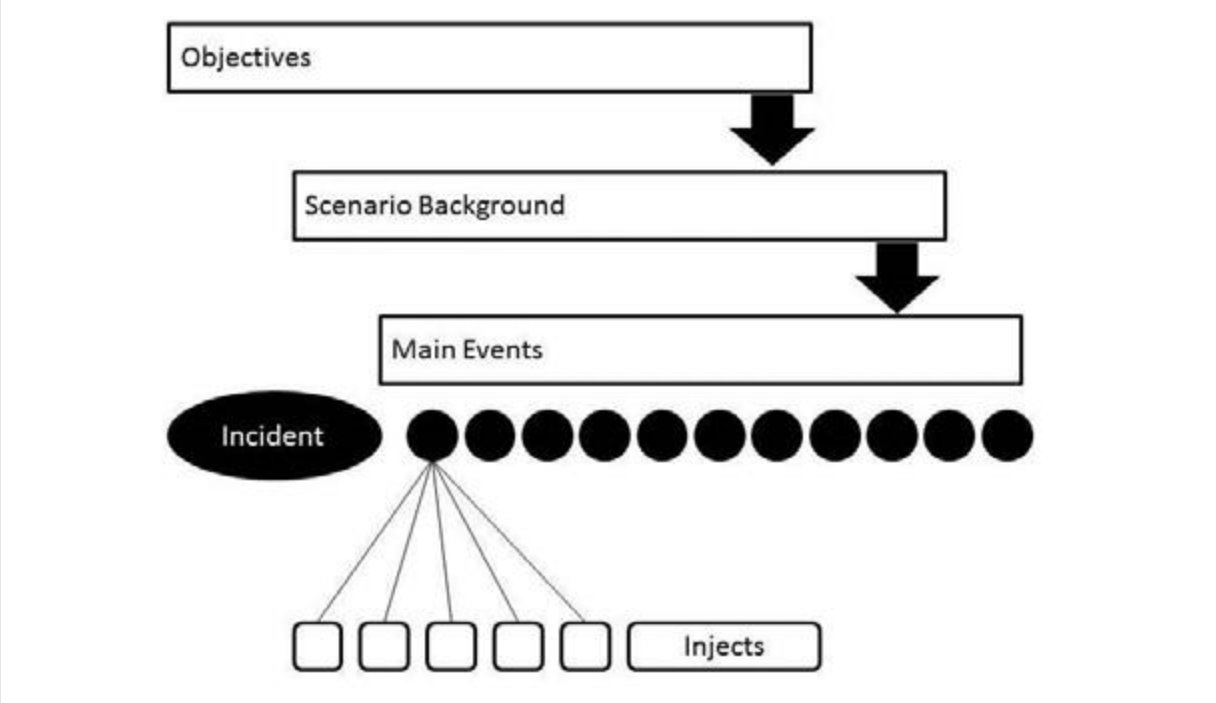
Swedish Civil Contingencies Agency

- The scenario

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

From objectives to injects



NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

- Real-time simulation

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

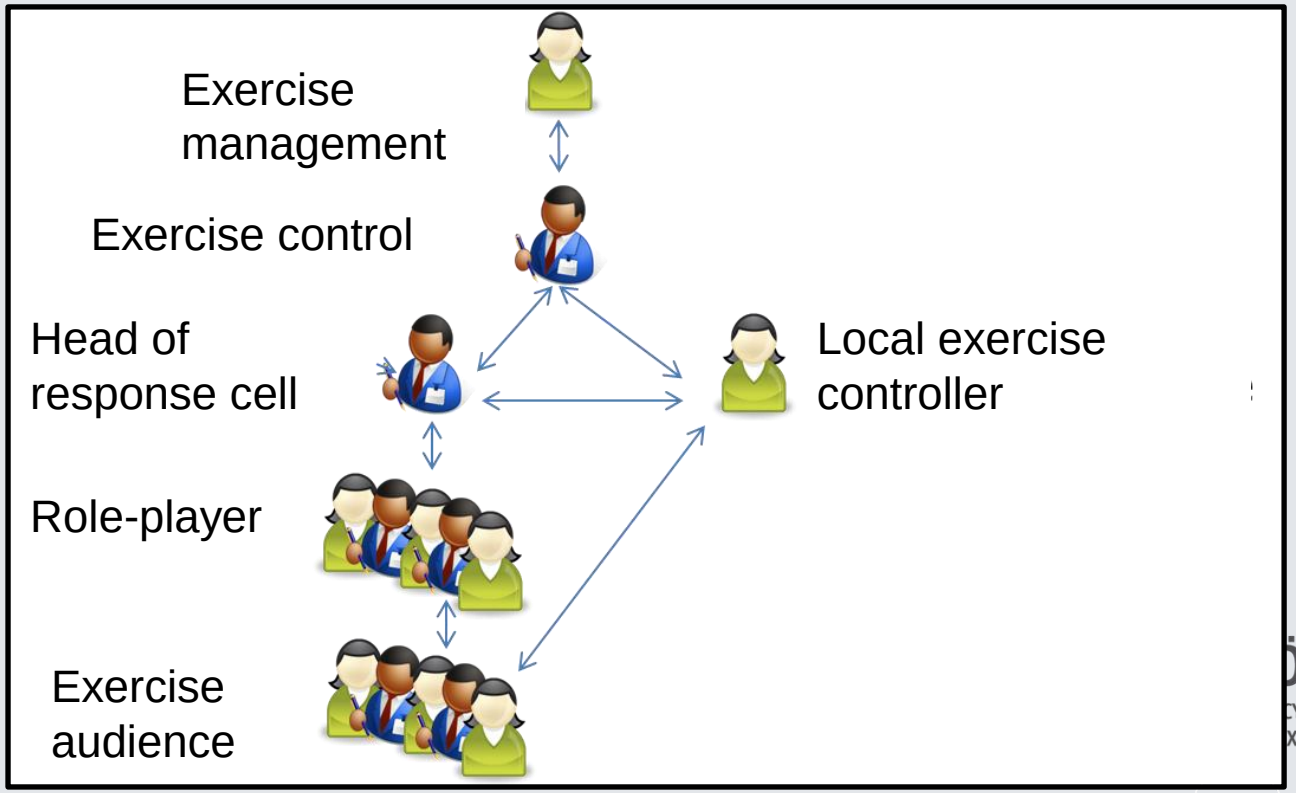
Swedish Civil Contingencies Agency

Simulation exercise

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

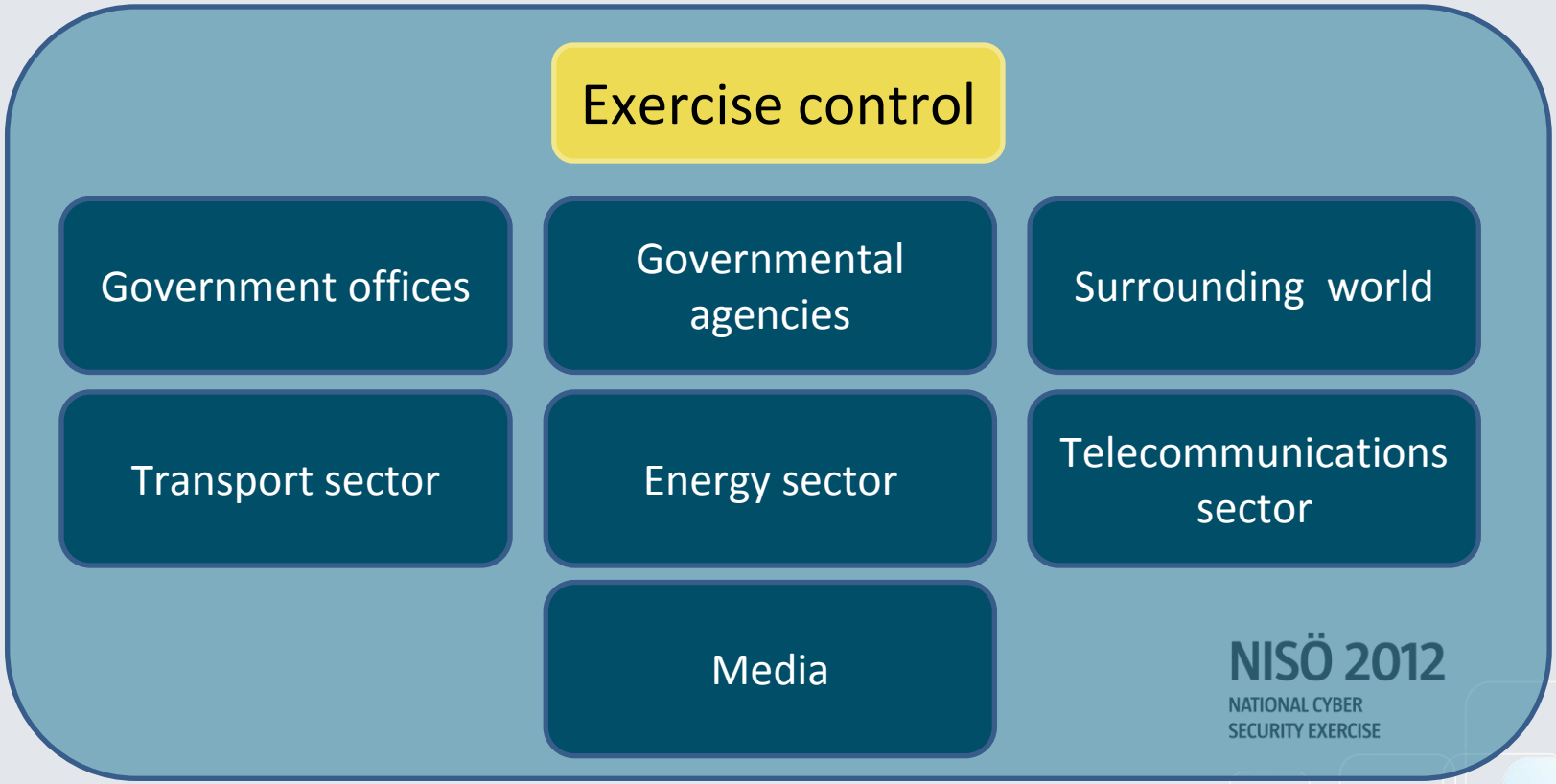
Myndigheten för samhällsskydd och beredskap

Roles in the exercise control



Swedish Civil Contingencies Agency

The exercise control with response cells



Swedish Civil Contingencies Agency

Storyline and events

DDoS-attacks and defacements

Information theft and Internet publication

Insider attack (transport sector)

Hacking attack on the telecommunications sector

Hacking attack on the energy sector

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Myndigheten för samhällsskydd och beredskap

Exercise web

Swedish Civil Contingencies Agency

The dynamic media play

- Tools for the exercise audience to reach the objectives
- Construed from organisations' own injects
- Only written material
- Produces simulated news for the actors' information gathering
- Articles are published on the exercise web portal
- Flashback and Pastebin

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

- Table-top

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

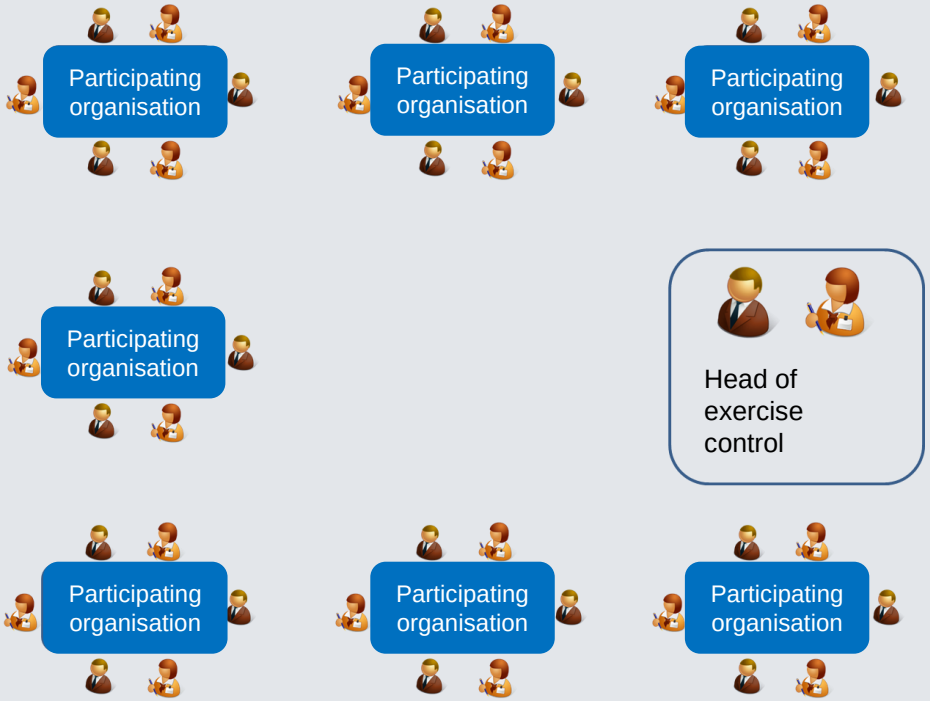
Table-top exercise 1 of 2

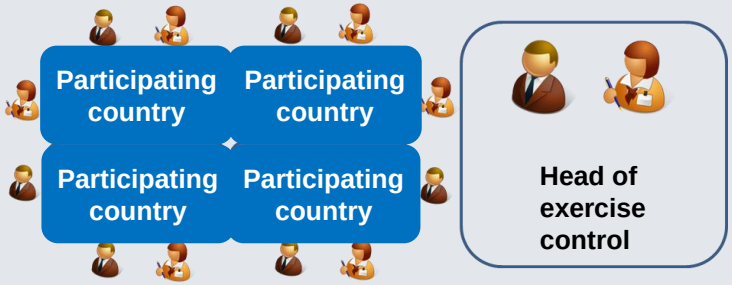
- Discussion-based
- Same scenario as simulation-exercise
- Partially preparded
- Analysis of simulation completes preparation
- Possibility of other discussions than during simulation (long-term etc.)

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Table-top exercise 2 of 2

NISÖ overall table-top exercise





NISÖ national Nordic CERT Cooperation table-top exercise

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

- Evaluation

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

Three evaluation processes for the exercise

- Evaluation focus on objectives
- Evaluation of the planning process
- Evaluation of National Response Plan

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

- AAR & Lessons identified

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

9 focus areas

- Cross-sectoral co-operation
  - Awerness raising activities
  - Strenghten co-operation and information sharing
  - Update policies, plans and processes

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

9 focus areas

- Common operational picture
  - Improve information sharing and collaboratrion
  - Enhanced capability in analyzing consequences and response messures

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

9 focus areas

- Crisis comunication
  - Further develope structures for collaboration
  - Prepare alternative platforms for communcation
  - To be further intergrated in crisis management

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

9 focus areas

- Prioritizing of resources
  - Increase knowledge of ”availible” resourses for cyber crisis management

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE

Swedish Civil Contingencies Agency

Thank you for your attention!

NISÖ 2012
NATIONAL CYBER SECURITY EXERCISE