

Actions to Promote Resilience and Confidence in e-Communication Infrastructures

Briefing for NIS '09



Swedish Post and Telecom Agency

- Ministry of Enterprise & Communications
- Agency in charge of security in electronic communications
- Network Security Department ~ 30 staff
- 20 million EUR/year
- Financed by fees from 50 operators
- 2/3 of the budget are spent on private-public partnerships and procurement

The Government's Measures

- Laws and regulations
- Lead-customer
- Procurement
- Coordination and facilitation

Four Criteria for Measures to Improve Redundancy and Flexibility

- Places that are highly likely to be affected by disruptions
- Vulnerable functions
- Needs for functions vital to society
- Number of subscribers affected

Some Examples of Measures

- Prioritisation
- Adding extra nodes
- Creating redundant connections
- Co-use of networks in extraordinary situations
- Enhanced technical perimeter protection

National Telecommunications Coordination Group (NTCG)

- NTCG supports the restoration of national infrastructures of electronic communications during critical disturbances
- NTCG consists of the eight largest Telcos and ISP:s, the leading distributor of radio & television, the national powergrid (backbone), the national railroad authority, the armed forces, and is chaired by PTS
- NTCG compiles situational reports, act as advisor and can, when needed, co-ordinate operations in the field during crisis
- NTCG conducts one exercise per year (TELÖ-series)

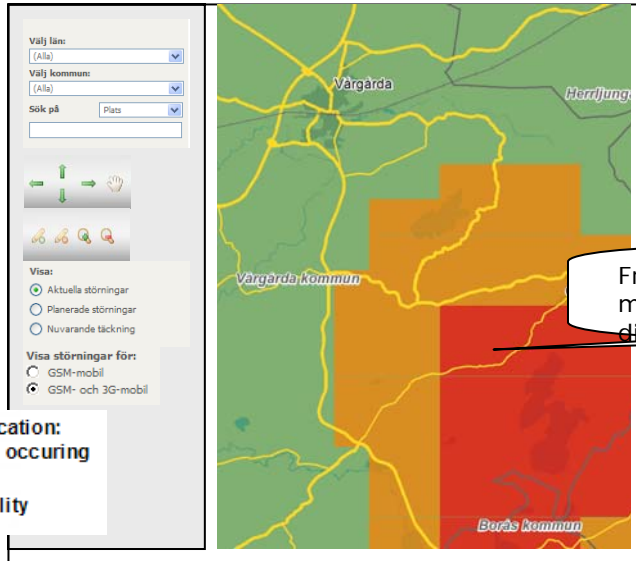
MIMER

- Multipurpose Information Management and Exchange for Robustness
- A tool for crisis management and situational assessment for the electronic communications sector.
- Technical platform for secure information exchange
- Emergency Services interface
- Public information dissemination component
- EU-sponsored (EPCIP)

MIMER II, Common Situation Awareness

GUI example 1: 3 000 000

(Presentation of Map / GIS)



Disturbance classification:
■ Disturbances are occurring
■ No accessibility
■ Normal accessibility

(Presentation of descriptive text)

General information:

Currently there are severe disturbances in broadband in X-county due to... ..

Free text: Descriptive text;
Optional information
Descriptive text does not need to have interactive link to list or map

From zoom situation 1:50000 will each disturbance in the map be identifiable with marking in the map (where disturbance ID is shown).

List automatically generated on the basis of what is shown in the map. The list is populated at scale 1:3 000000 (corresponding to Norrbottens County), i.e. from this scale may the list "be activated" by the member. The list contains all disturbances present in current map

Clickable link, when clicking zoom is activated (and centers) map to disturbance. Map shows the hold disturbance.

Cause is described with standard texts such as "cable malfunction", "equipment malfunction", "maintenance work", "or "weather"

Numbers of affected customers are stated only re fixed networks

(Presentation of List)

Dist. ID	Location	Descr. and Cause	Occurred	Estimated end	Affected service	Customers affe.
Id 1	Municipality in x-county	Limited or no connectivity in X due to...	20070831;08.15	2007-08-31; 10.00	GSM, 3G, GPRS...	
Id 2						
Etc.						

Option to show 10 at one time and/o, if more disturbances, to start paging function

Telö-series

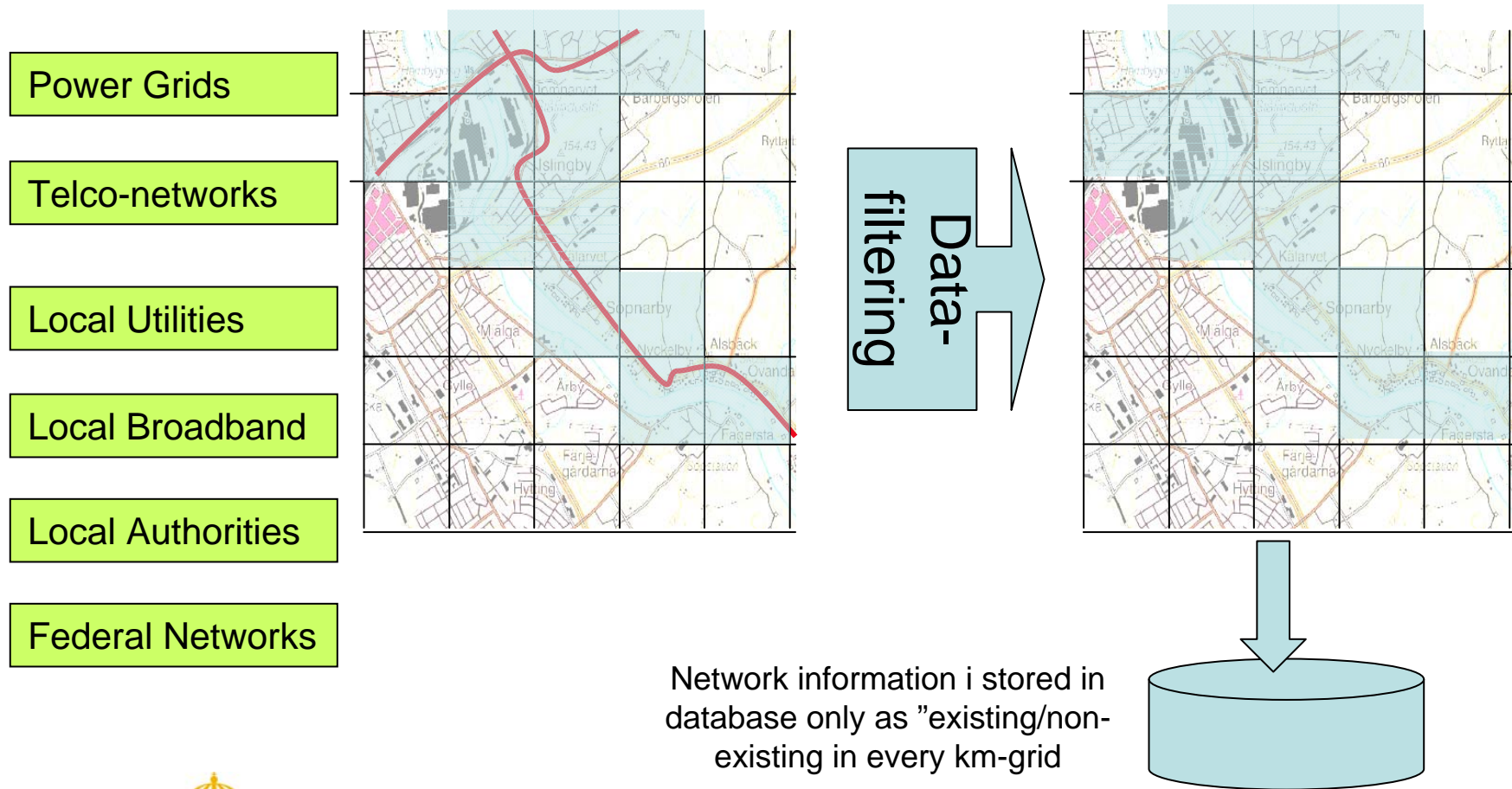
- Bi-annual national electronic communications exercises
- TELÖ-09 was the largest exercise in the electronic communications sector to this date
- Aim: strengthen crisis management capabilities within the sector, test NTCG and its capability to operate virtually, test the MIMER concept
- Terrorism-scenario

National Portal for Cable and Pipe Identification



2009-10-12

Network-owners registers information about his network in a database – existing/non-existing in a km-grid throughout the nation



Query

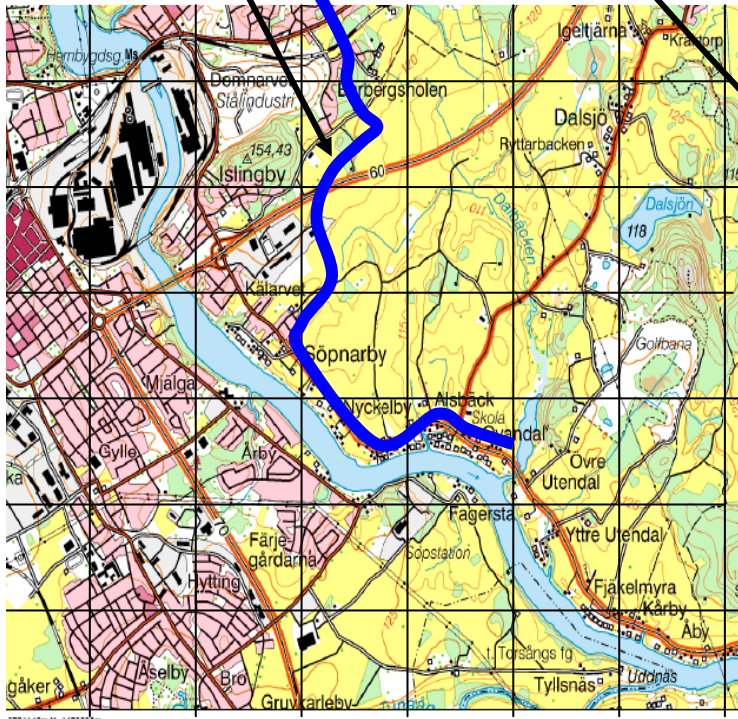


2

Query is sent to database

In the portal, planned digging is outlined by contractor

1



Databas
Call center

4

Information is relayed to network-owners who have networks in relevant km-grid

3

Database confirms immediately that there are four network-owners in the area and that the contractor will receive information from relevant network-owners

Power Grids

Telco-networks

Local Utilities

Local Broadband

Local Authorities

Federal Networks

Answers from network-owners



Power Grids

Telco-networks

Local Utilities

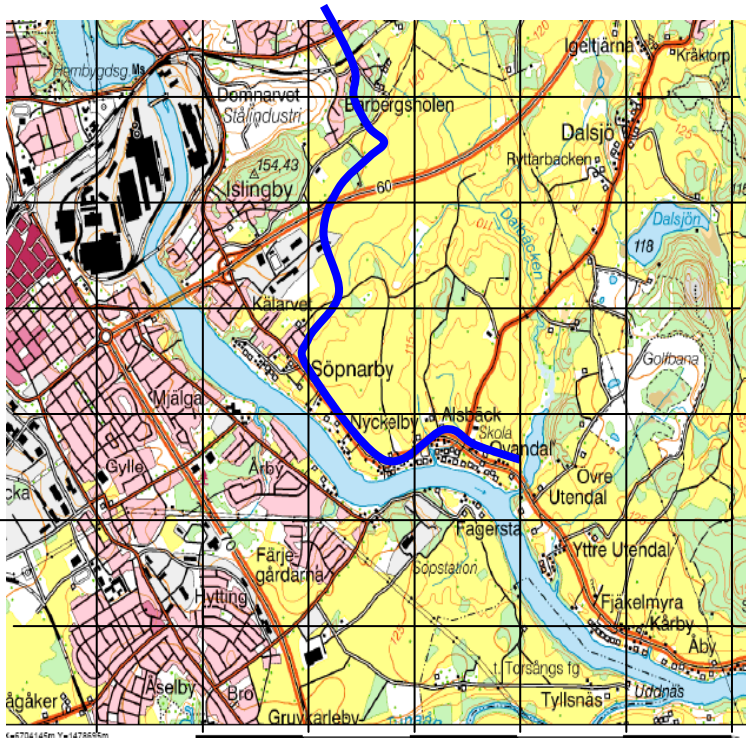
Local Broadband

Local Authorities

Federal Networks

Database
Call centre

Each network-owner will answer the contractor relevant to the respective networks topology



Strategy to Improve Internet Security

- The aim of the strategy is to facilitate and clarify future work to secure the infrastructure of the Internet in Sweden
 - PTS proposed a strategy, an action plan, an allocation of responsibility, and a management plan for the strategy
 - 8 strategic positions were adopted in the strategy
 - 23 actions/measures were proposed in the action plan
- ✓ The proposal is confirmed by the Government as a National Strategy

Examples of Measures in the Action Plan

- Promote the use of DNSSEC in name servers
- Produce recommendations for more secure traffic exchange between Internet operators (BGP)
- Provide the Internet operators with a legal possibility of impeding the dissemination of harmful traffic
- Further develop operative international networks for incident management
- Produce a co-ordinated continuity plan for the Internet infrastructure in Sweden

Swedish IT Incident Centre - SITIC

- A national function, CERT, charged with supporting society in the areas of incident response and proactive measures.
- SITIC rapidly responds to incidents by advising and participating in the coordination of actions needed to remedy and mitigate incidents.
- SITIC advises and supports government agencies, regions, municipalities and the private sector, on proactive measures in the area of network security
- SITIC is the national point of contact for international incident response cooperation.

Cooperation with other CERT's

- TeliaSoneraCERT, SunetCERT
- Nordic CERT-forum (NCF)
- European Government CERT (EGC) Group
 - CERT-FI (FI)
 - CERTA (F)
 - CERT-BUND (D)
 - CERT-Hungary
 - GOVCERT.NL (NL)
 - NorCERT (NO)
 - CCN-CERT (ES)
 - GovCertUK (UK)
 - CSIRTUK (UK)
- FIRST, TF-CSIRT
- International Watch & Warning Network (IWWN)

International Conference on Resilience

- *Resilience in Electronic Communications – A Multistakeholder Challenge*
- In association with the Swedish Presidency of the European Union
- Stockholm 4-5 November
- Eu2009.pts.se

Conference at a Glance

Opening Session		
Regulatory Policy	Public-Private Partnerships	Government CERT Policy
Supervising Resilience	Crisis Management	GovCERT Policy
Status of EU Regulatory Framework Review	Exercises	Ministerial Affiliation
Status of EU NIS Policy	Information Systems	Cooperation
Closing Session		

- Contact me at: peter.wallstrom@pts.se



2009-10-12