

PLATFORM FOR CYBERSECURITY

**CPNI.NL**



The Dutch Public Private Approach

# Connecting initiatives

Greece, June 28 2011



June 28, 2011

Public Private Partnership      ISACs  
Cybercrime      Smart Grids  
Information Sharing      Meridian      TRUST  
European Commission      TLP  
Information Exchanges      SCADA  
pcs      Membership Guidelines  
Cybersecurity      ENISA      MPCSIE  
VALUE      E-SCSIE



# Why is action needed?

**Situation**

- ICT is of fundamental importance for our society
- Society becomes more and more vulnerable for disruption or misuse of ICT-infrastructures
- Recent incidents: Stuxnet, Night Dragon, RSA, DDoS-attacks

**Complications**

- Most critical infrastructures or owned by private sector
- Private sector has its own responsibility, voluntary partnerships
- Not enough information exchange between public and private organisations
- International problem

**Main question** How can we raise the resilience of critical infrastructure against cyber disturbance?

**Answer**

- Build and facilitate a (inter)national Public Private network based on:
  - Trust and Value
- Create the Cybercrime Information Exchange (with sectoral ISACs)
- Use clear membership guidelines (incl TLP)
- Sector is in the lead (chair of the ISAC is from industry)



June 28, 2011

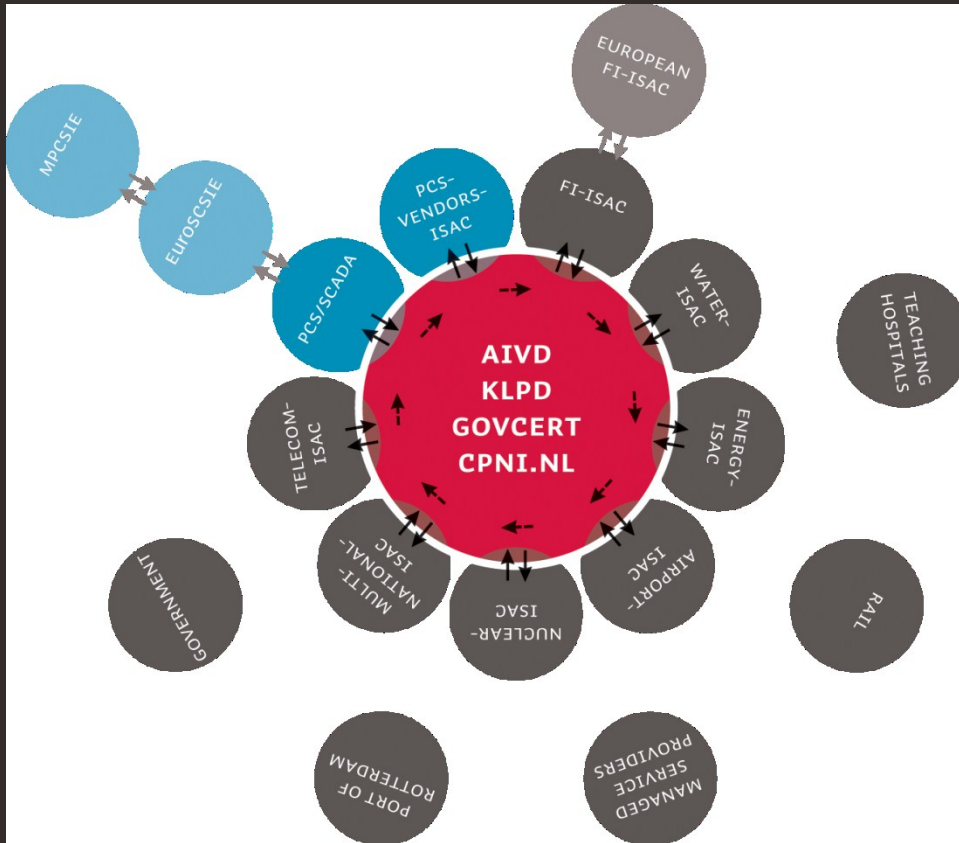
# Cybercrime Information Exchange

Point of departure is that companies themselves will only take effective measures if they have access to the right information and are able to make accurate **risk assessments**.

By **sharing information intensively** about incidents, threats, vulnerabilities and good practices , the participants can prevent incidents themselves. This will safeguard the Dutch economy as a whole and the continuity of the individual organisations at the same time.



June 28, 2011



## Information Sharing:

Trust  
Value

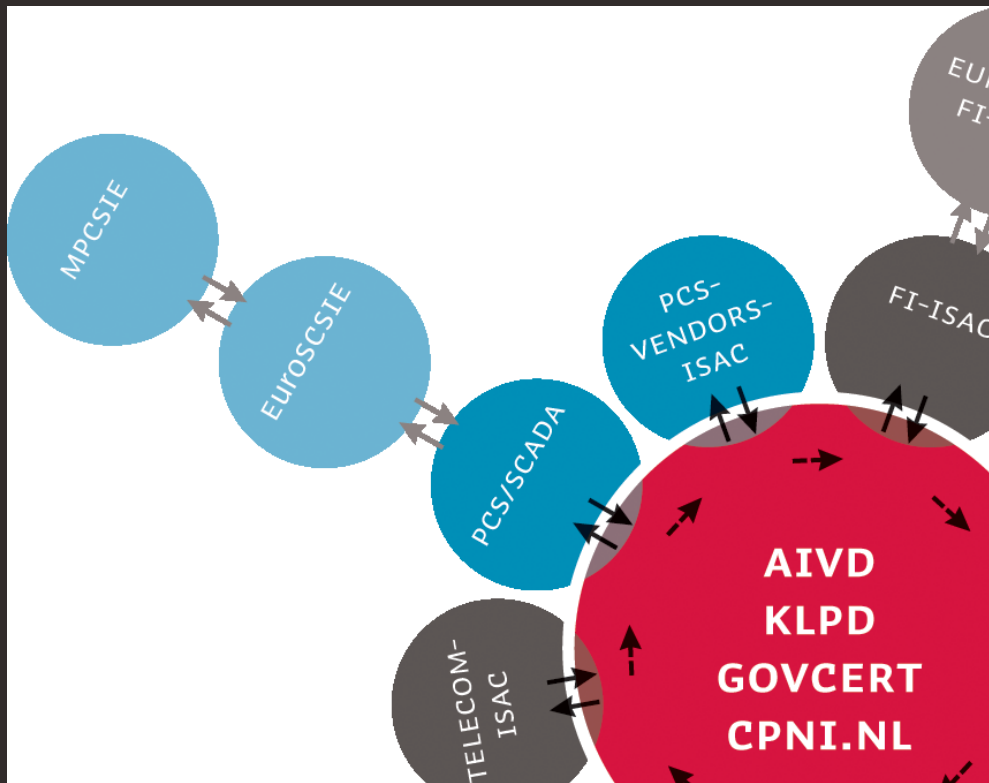
First the social network  
(meeting face-to-face)  
then a technical infra-  
structure to support  
this!



June 28, 2011



- Information Sharing on a European and International level
  - E-SCSIE
  - European FI-ISAC
  - ENISA as a facilitating partner on a European level
- International:
  - Meridian (annual CIIP conference)
  - MPCSIE



# E-SCSIE - members

Users	Government	R&D
<ul style="list-style-type: none"> <li>• EDF (F)</li> <li>• CERN (CH)</li> <li>• Electrabel (B)</li> <li>• Laborolec (B)</li> <li>• Verbund-Austrian Power Grid AG (A)</li> <li>• SwissGrid (CH)</li> <li>• Italian Association of CI Experts (I)</li> <li>• GCSEC (I)</li> <li>• Shell (NL)</li> </ul>	<ul style="list-style-type: none"> <li>• GOVCERT.CH</li> <li>• Melani (CH)</li> <li>• BSI (D)</li> <li>• CERT Hungary</li> <li>• NorCERT (N)</li> <li>• NoNSA (N)</li> <li>• GOVCERT.NL</li> <li>• CPNI.NL</li> <li>• MSB (Se)</li> <li>• CPNI (UK),</li> <li>• ANSSI/COSSI (F)</li> <li>• CERT-FI (Fi)</li> <li>• ENISA (EU)</li> </ul>	<ul style="list-style-type: none"> <li>• JRC (EU)</li> </ul>

# E-SCSIE - Terms of Reference

Started on 20 June 2005

Aim is for European industry, government, and research to benefit from the ability to collaborate on a range of common issues, and to focus effort and share resource where appropriate.

Main focus is Information Sharing

The outcome would be a raised level of protection adopted across Europe's SCADA and Control Systems (SCADA/CS)



June 28, 2011

# E-SCSIE - Information Sharing

The following are examples of what each member should share at E-SCSIE meetings:

- Report events or incidents that have affected SCADA and Control Systems
- Report warnings about vulnerabilities in SCADA and Control System products
- Give advice as to how these vulnerabilities and, or incidents were addressed
- Exchange experience on good practice (amongst which policies) used to mitigate SCADA and Control System security issues



June 28, 2011

# E-SCSIE - Topics

- Sharing of incidents and good practices
- Questionnaire on Control System Cyber-Security (aimed at vendors) 2008/2009
- Standards and requirements (e.g. WIB Process Control Domain Security Requirements for Vendors)
- Self Assessment tools (like the one from CPNI UK)
- Smart Grids (e.g. Smart Grid Conference in Baarn, the Netherlands - 2010)



June 28, 2011

# What do we need?

## Connect initiatives

- Between Dutch, EU and Worldwide institutes in the field of Cyber Security
- Between Private and Public stakeholders
- Between end-users and vendors
- Between critical infrastructure, research institutions and academia
- Between sectors dealing with cyber security

## To provide new input

- By sharing information in a trusted environment
- By setting standards and certification adding to cyber security in the NL, EU and World
- By adding a program to raise cyber security awareness at management level
- By setting up testing and training facilities

Due to the Private Public Partnership we are able to respond quickly to the rapid developments in the field of cyber security and spread this knowledge to other organizations, but also stimulate short- and longtime research.



June 28, 2011

**Annemarie Zielstra**

Director CPNI.NL

Chair EuroSCSIE

**M** +31 6 1299 2883

**E** [annemarie.zielstra@cpni.nl](mailto:annemarie.zielstra@cpni.nl)

**I** [www.cpni.nl](http://www.cpni.nl)

