



Agentschap Telecom  
Ministerie van Economische Zaken  
en Klimaat

# CEER: 21th June 2019 workshop Security Radiocommunications Agency Netherlands

Security: in control  
Restricted sharing, attendees  
only.

Ron Spuijbroek



Agentschap Telecom  
Ministerie van Economische Zaken  
en Klimaat



Secure Infrastructures

5G

4G

3G



Public Trust



MinEZK: Ministry of Economic Affairs and  
Climate Policy → Competent Authority

Agentschap Telecom:  
Radiocommunications Agency →  
Supervisory body

“Energy”: Oil, Gas,  
Electricity,..

“Internet” : DSP’s, Cloud,  
Marketplaces, Searchengines ,  
InternetExchanges ,....



Agentschap Telecom  
Ministerie van Economische Zaken  
en Klimaat

# Supervisory Bodies

Keystone of European Security  
between law and companies

Closing te Gap in Security: together



# Supervising the Energysector

Current focus:

- Oil;
- Gas;
- Electricity;

Expected energytransition:

- Heat networks;
- Cooling networks;
- Hydrogen;
- LPG, CNG, LNG;
- Biogas;
- CCS;
- (coal, biomass, wood,..)

Per sector: chain-approach(source, network, users, Suppliers, admin systems, marketsystems)

i.e. electricity:

- DSO, TSO;
- Energyproducers: conventional
- New energy: Wind, Solar, incl distributed (inverters);
- Large (incl distributed) consumers; E-charge, etc;
- Essential assetSuppliers OT/IT;
- Energymarket/traders;
- Branche organisations;
- Associated supervisors, regulators (NL-ACM),
- chair NL-supervisory bodies on NIS-directive;

International collaboration ENISA, WS8, etc.



## How do we do that:

Just culture; (No automatic fine on a reported incident)  
Used for learning not for fines;

1. General inspections;
2. Thematic inspections;
3. Incident based inspections;

Close contact with companies & stakeholders



# What do we do in supervising the Energysector

- Company-Boardmeetings, board primarily responsible;
  - Open guidelines: use what's already in place, the 'security-languages' of the sector'
  - Self-assessments; ENISA, CAF (UK), Branche Standards;
  - Increasing levels: basics first, increased attention, up to APT-ready;
  - Cyber Maturity Model, KPI's;
  - In parallel: Reality Checks: websites, mailservers, FTP services; Customer log-in sites,
  - IP-adressspace scanning on agenda;
  - InternetChallenges: 'Internet-sickness', ancient insecure protocols, DDoS, DNS, certificates, and IPv6, Stop IP-Spoofing, BGP; (from controled/improved by universities to non-controled commercial)
  - All interfaces are in scope: wireless, phone, Sat, etc
  - Focus on ISMS, Riskassessment.
- 
- Objective: Europe more resilient by: creating dashboards, KPI's , close communication:
  - Continous improvement



# Take away

*"Will we be asimilated, or do we work together fast: CCMM, dashboards, Reality Checks, anti-DDoS,..*

*Joint-Supervising, joint responsibility*

Will we be in time?

# No Time to Waste!





work together

Keep up the good work!

