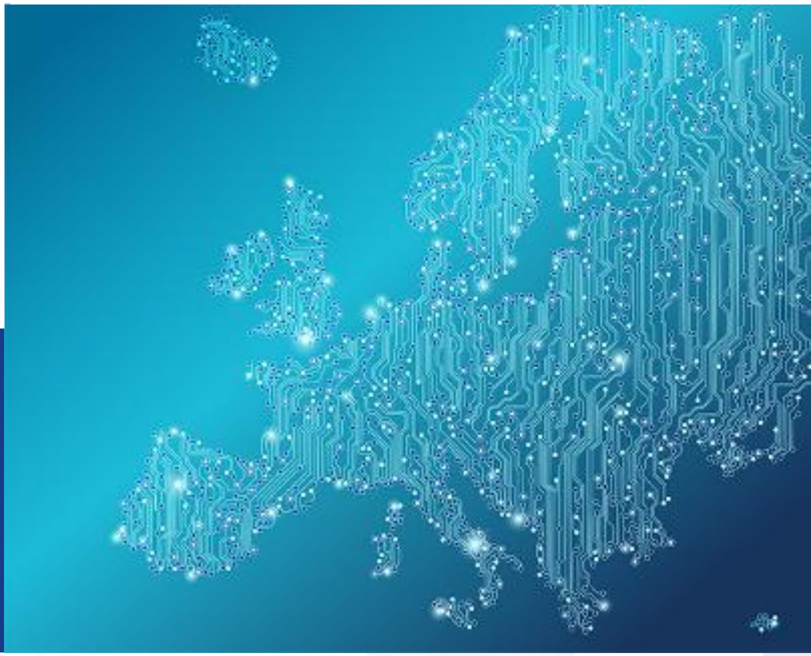


# EU NIS Directive & OES - ENISA's contribution

Paraskevi Kasse

Network and Information Security Officers, 22nd March 2018

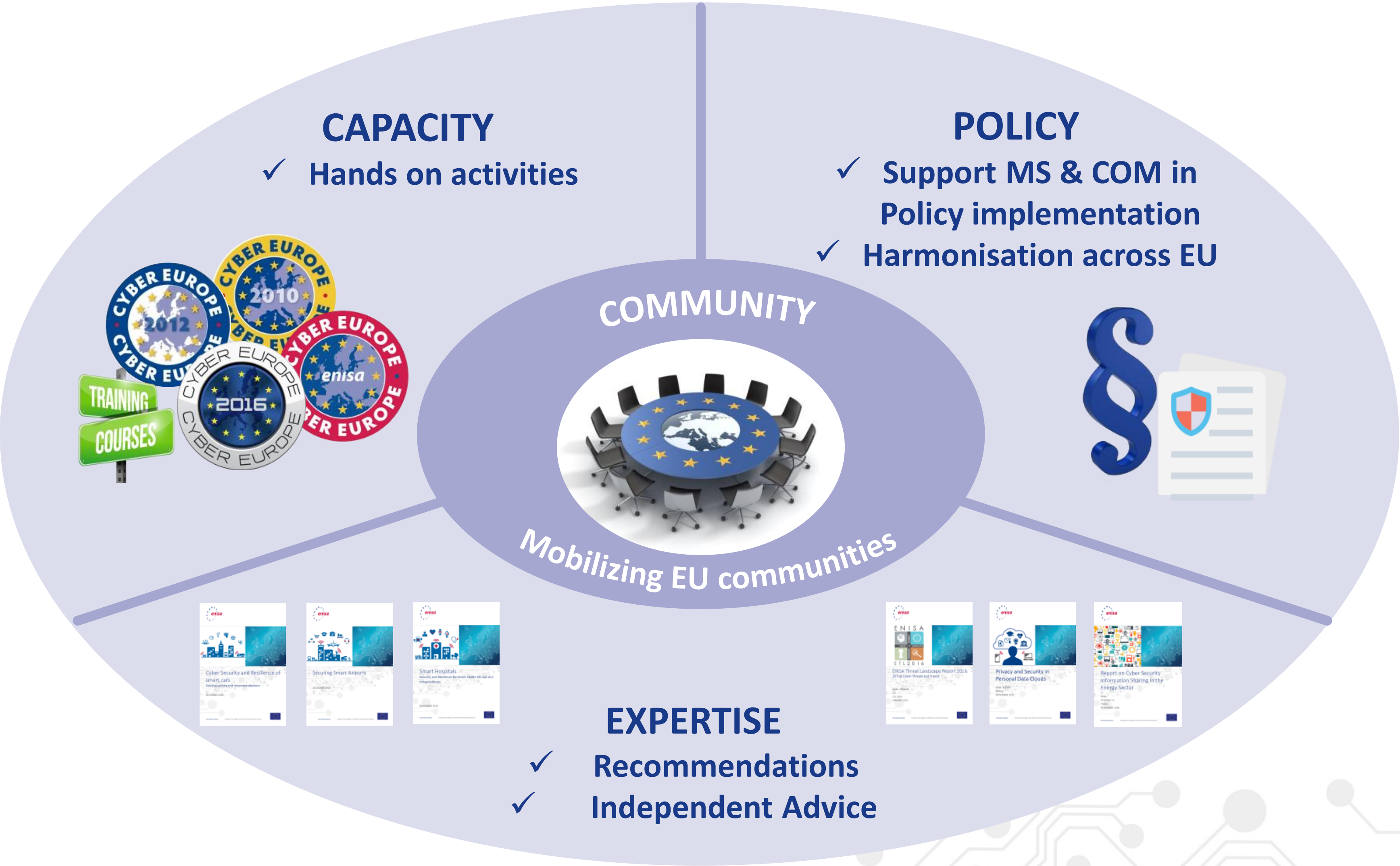
European Union Agency for Network and Information Security

# Show time …

# Securing Europe’s Information society

enisa
enisa

# Positioning ENISA activities



## CAPACITY

- ✓ Hands on activities

## POLICY

- ✓ Support MS & COM in Policy implementation
- ✓ Harmonisation across EU

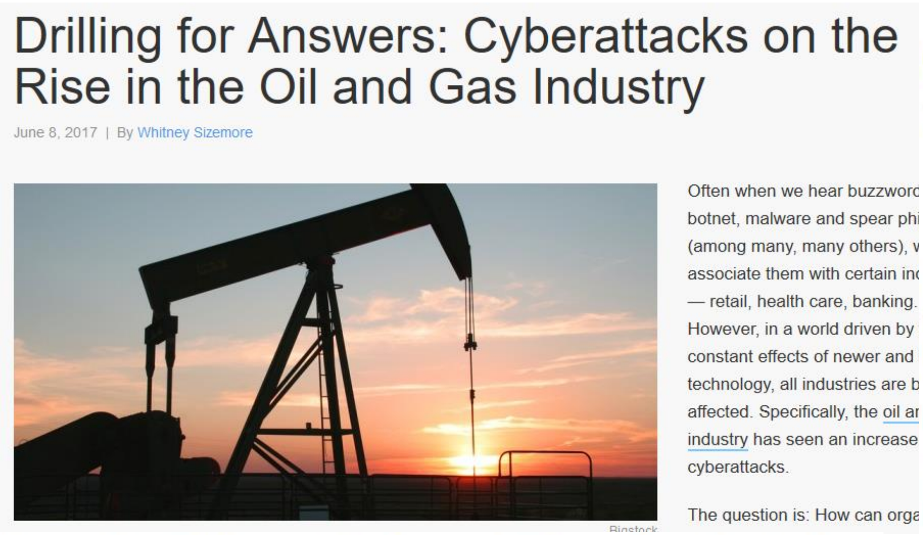
## COMMUNITY

Mobilizing EU communities

## EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

# Browsing the net …



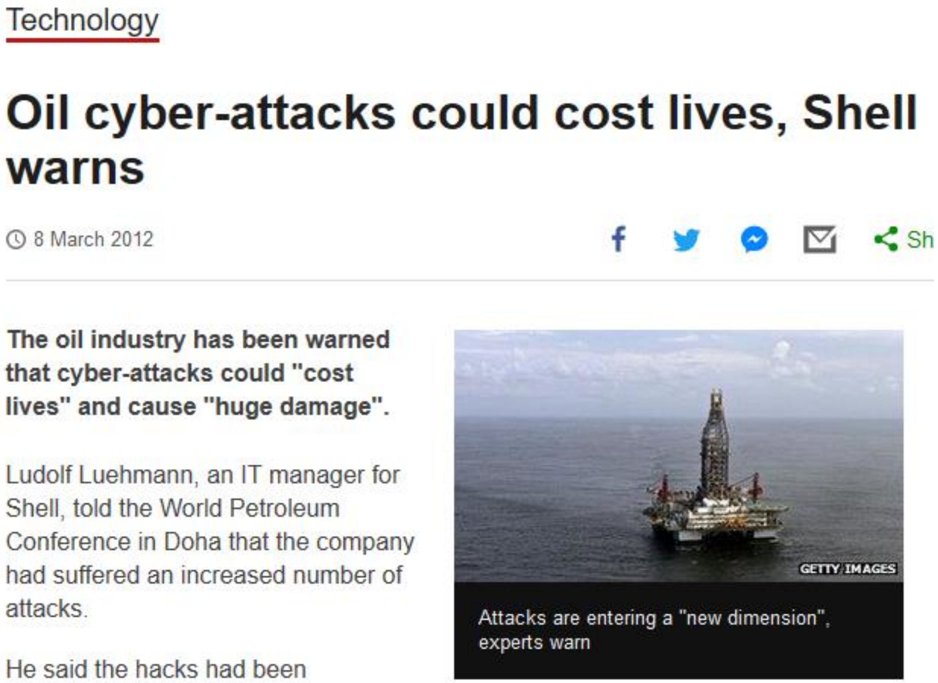
Drilling for Answers: Cyberattacks on the Rise in the Oil and Gas Industry

June 8, 2017 | By Whitney Sizemore

Often when we hear buzzworc botnet, malware and spear phi (among many, many others), v associate them with certain inc — retail, health care, banking. However, in a world driven by constant effects of newer and technology, all industries are b affected. Specifically, the oil ar industry has seen an increase cyberattacks.

The question is: How can orga

Bigstock



Technology

Oil cyber-attacks could cost lives, Shell warns

8 March 2012

**The oil industry has been warned that cyber-attacks could "cost lives" and cause "huge damage".**

Ludolf Luehmann, an IT manager for Shell, told the World Petroleum Conference in Doha that the company had suffered an increased number of attacks.

He said the hacks had been

GETTY IMAGES

Attacks are entering a "new dimension", experts warn

Combatting Cyber-Attacks In The Oil And Gas Industry

By Tsvetana Paraskova - Dec 15, 2016, 3:00 PM CST

Stuxnet: the father of cyber-kinetic weapons

While Stuxnet is gone, the world now knows what can be accomplished through cyber-kinetic attacks.

Industroyer: Biggest threat to industrial control systems since Stuxnet

BY ANTON CHEREPANOV AND ROBERT LIPOVSKY POSTED 12 JUN 2017 - 02:00PM

MALWARE

# Why cyber security in the Energy sector?

## Increased resilience against cyber and privacy attacks

- Real time requirements
- Ensure **SAFETY** & continuity of critical business energy operations
- Cascading effects
- Cost

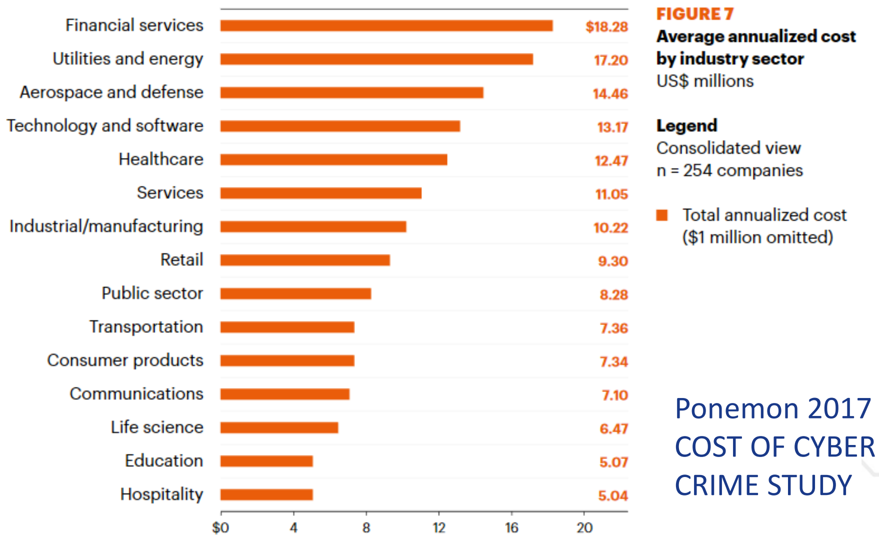


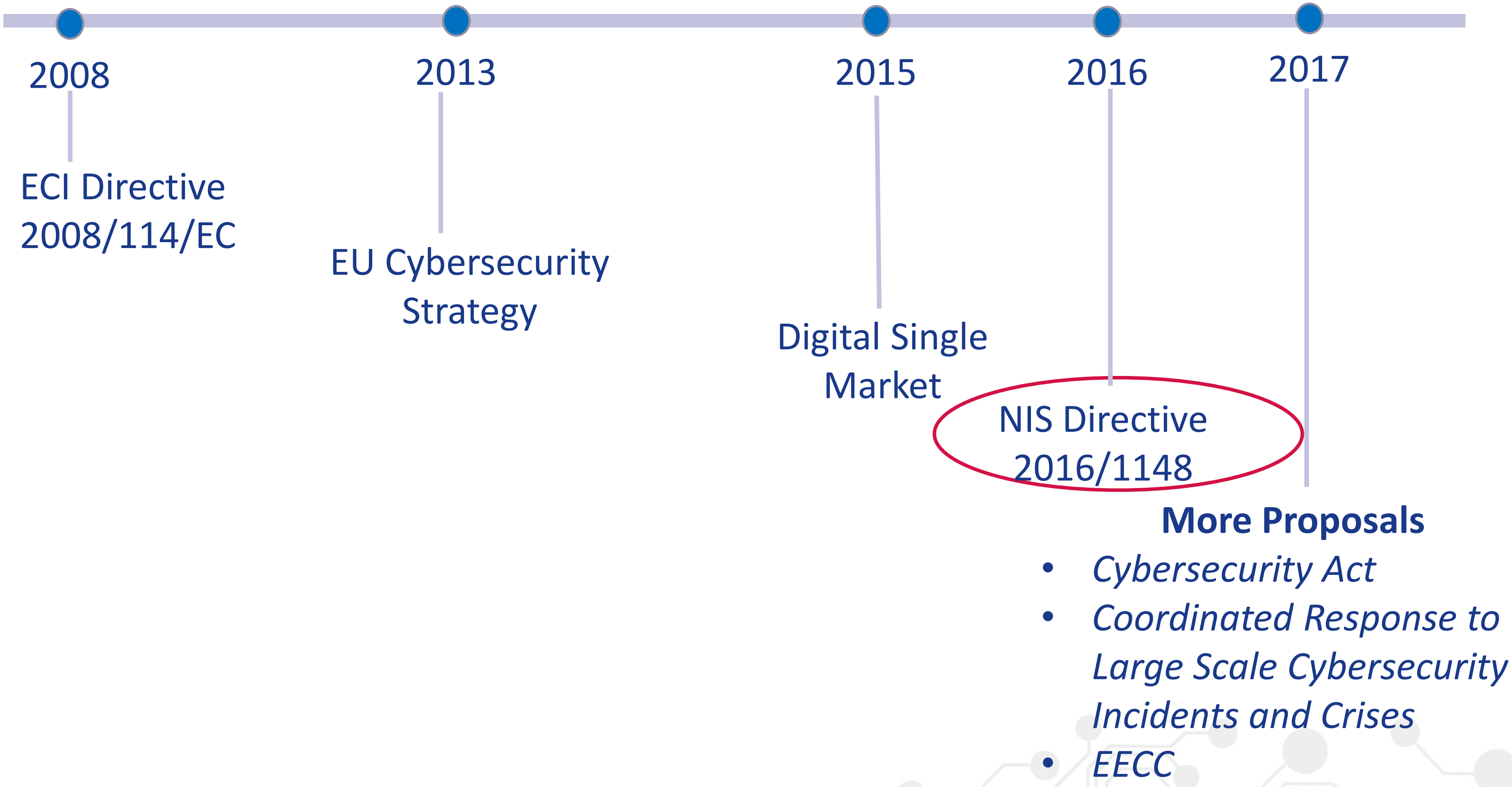
**FIGURE 7**
**Average annualized cost by industry sector**
US$ millions

Ponemon 2017
COST OF CYBER CRIME STUDY

# Emerging Threat Environment

- Complex networks and services
- Legacy and digital technologies
- Low quality of software and hardware
- Asymmetric threats allowing remote attacks to CII
- Significant physical disasters affecting CIIs
- Increase in organised cybercrime and industrial espionage
- Lack of international agreements & well functioning of an international operational mechanism

# EU Policy



2008

ECI Directive
2008/114/EC

2013

EU Cybersecurity
Strategy

2015

Digital Single
Market

2016

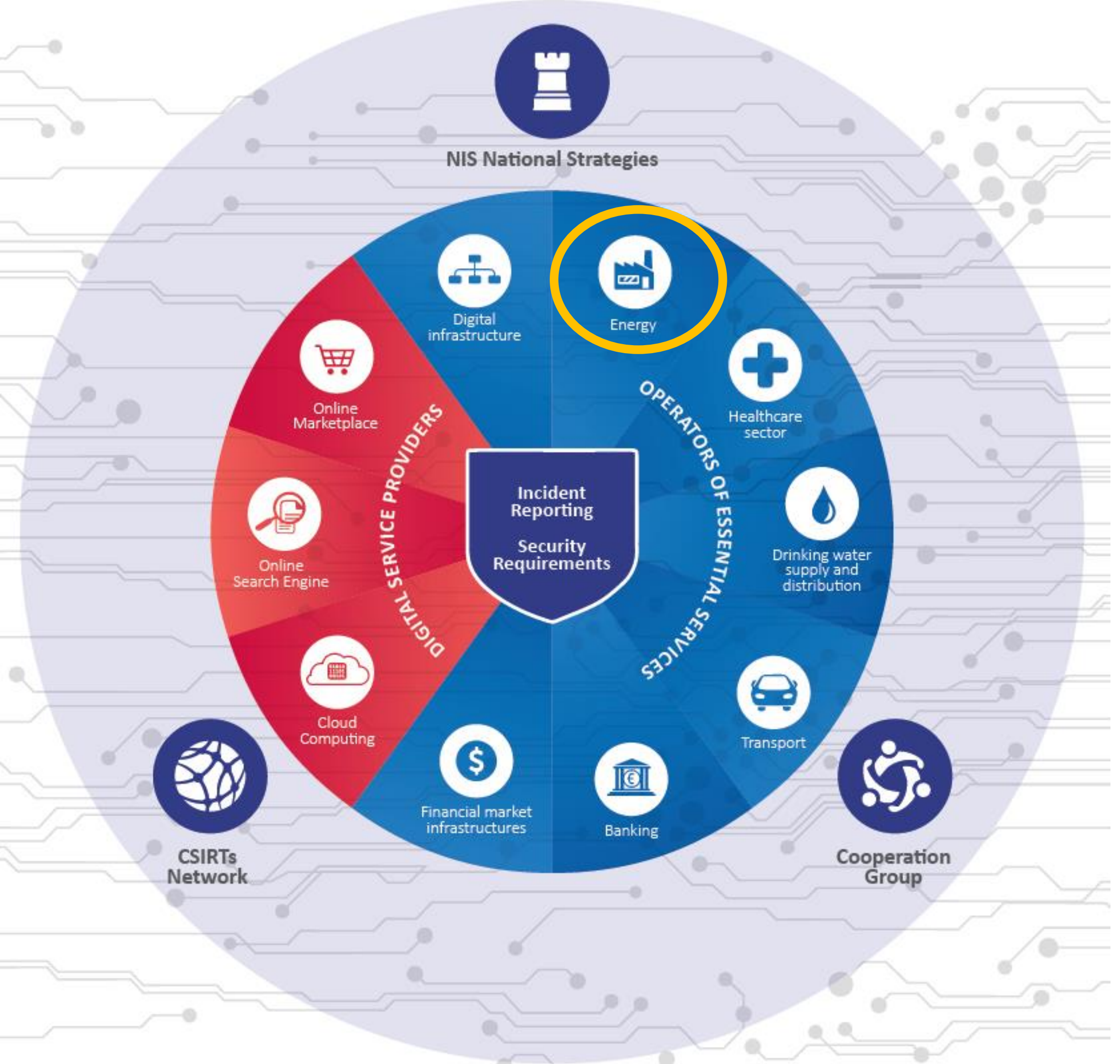
NIS Directive
2016/1148

2017

**More Proposals**

- *Cybersecurity Act*
- *Coordinated Response to Large Scale Cybersecurity Incidents and Crises*
- *EECC*

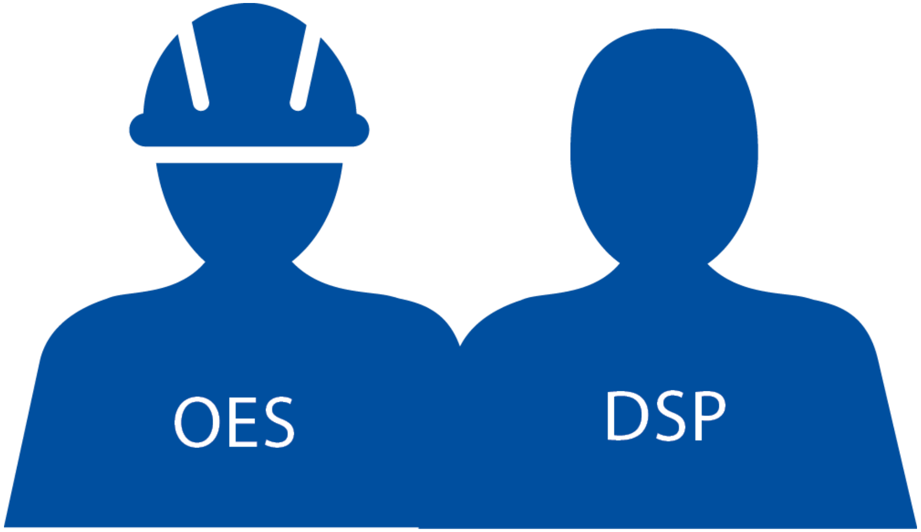
# NIS Directive



## Oil

- Operators of oil transmission pipelines
- Operators of oil production, refining and treatment facilities, storage and transmission

# DSPs & OESs Obligations



**Commonalities**

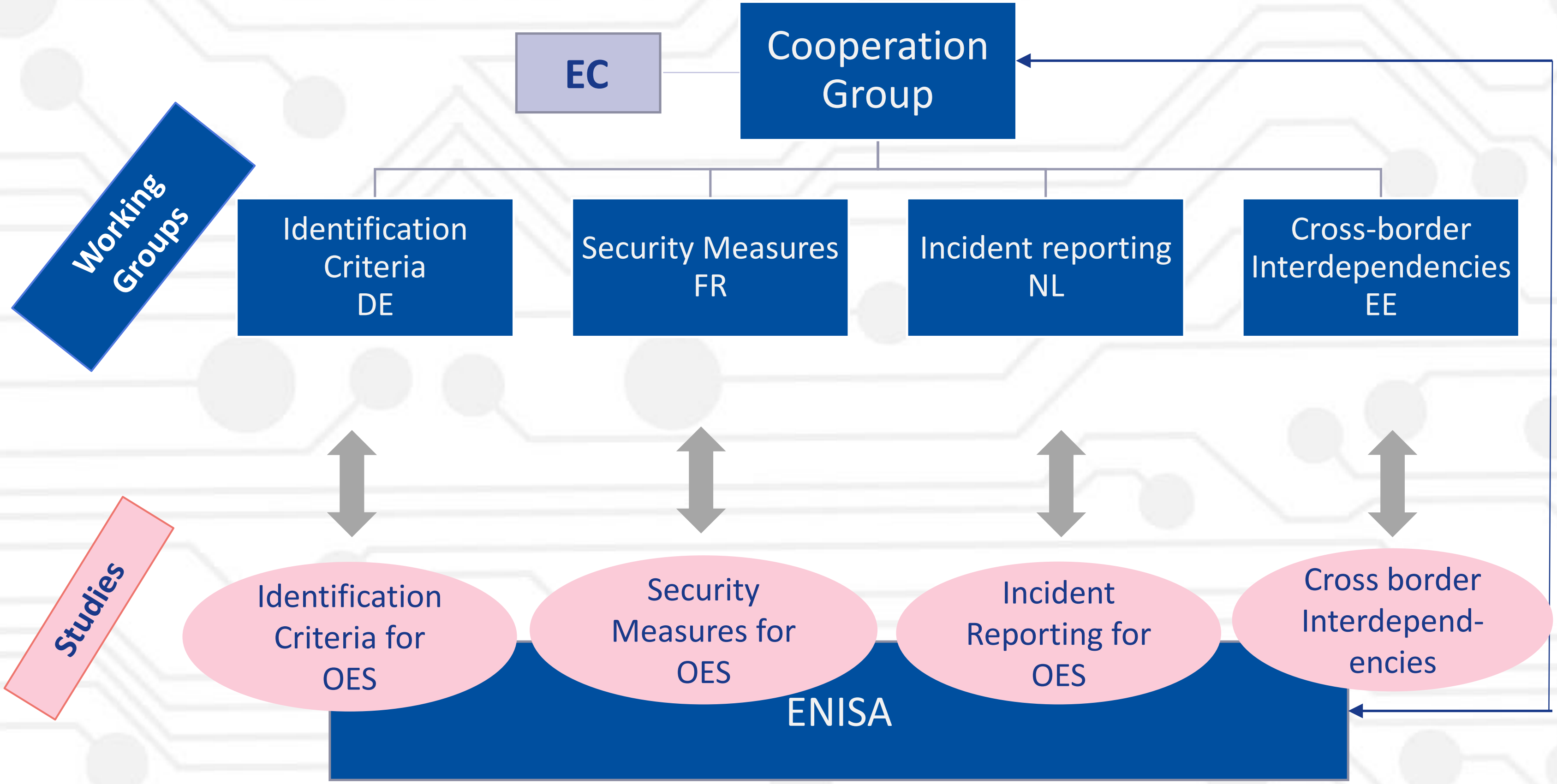
- Security measures
- Incident notification

**Differences**

- Identification criteria
- Audit

- Implementing Acts
- Light touch approach
- Medium & Large enterprises

# OES obligations


EC
Cooperation Group
Working Groups
Identification Criteria DE
Security Measures FR
Incident reporting NL
Cross-border Interdependencies EE
Studies
Identification Criteria for OES
Security Measures for OES
Incident Reporting for OES
Cross border Interdepend-encies
ENISA

# Significance of incidents

multiple parameters

↓

multiple thresholds

σημαντικό περιστατικό

incident significatif

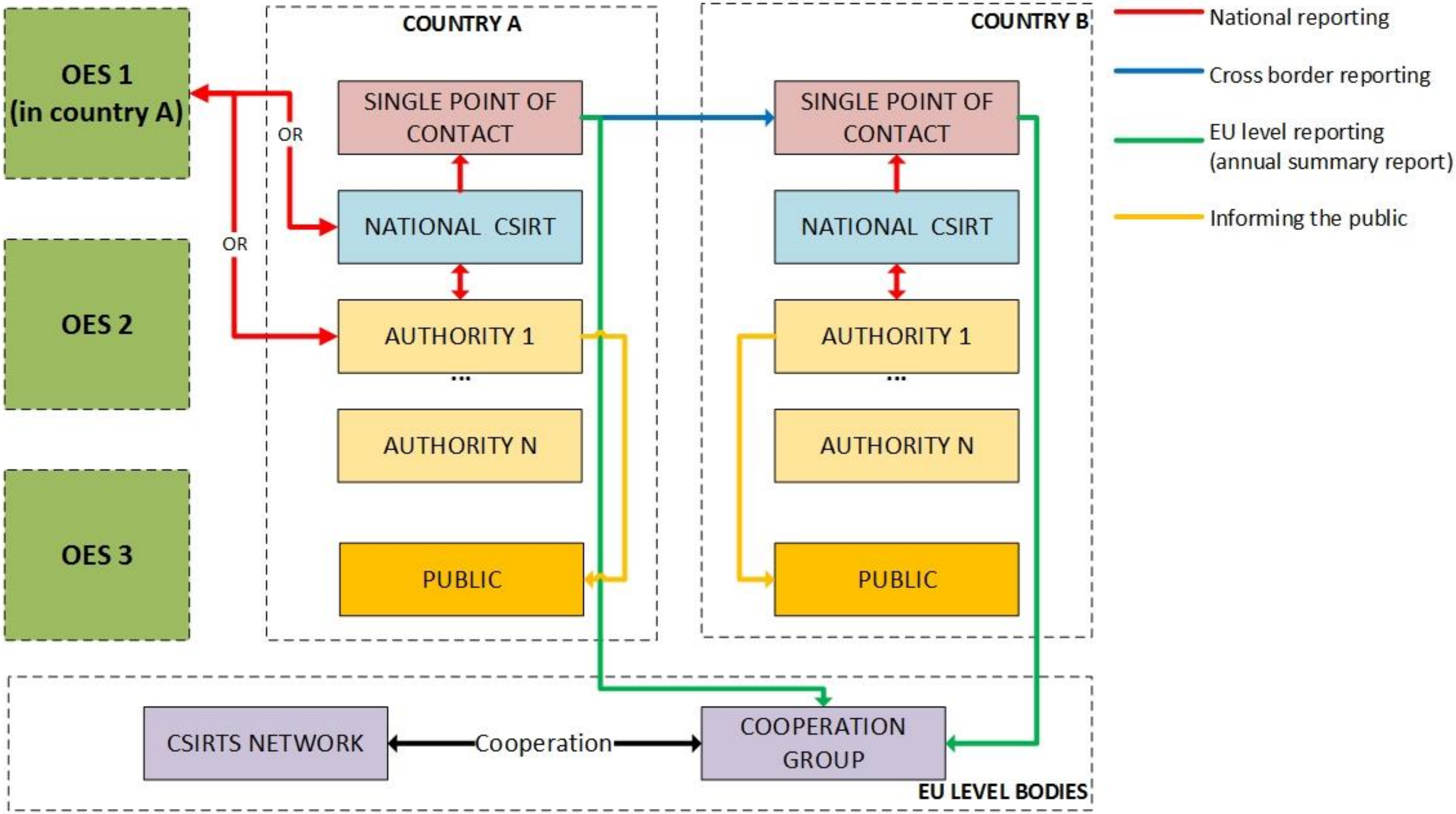
significant incident

märkimisväärne vahejuhtum

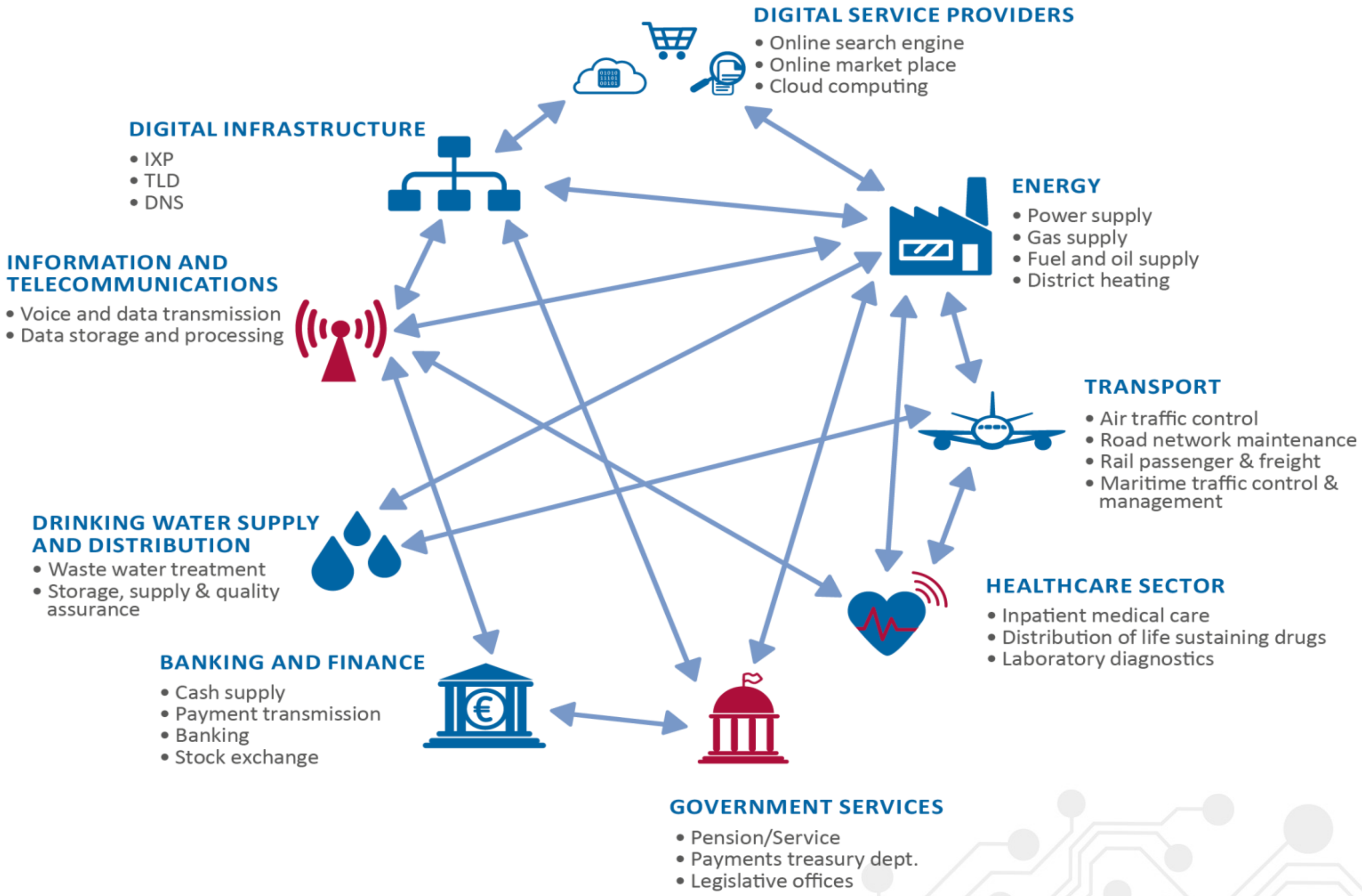
значителен инцидент

incidente significativo

# Incident Reporting for OES: the process



# Cross border interdependencies



**DIGITAL SERVICE PROVIDERS**

- Online search engine
- Online market place
- Cloud computing

**DIGITAL INFRASTRUCTURE**

- IXP
- TLD
- DNS

**ENERGY**

- Power supply
- Gas supply
- Fuel and oil supply
- District heating

**INFORMATION AND TELECOMMUNICATIONS**

- Voice and data transmission
- Data storage and processing

**TRANSPORT**

- Air traffic control
- Road network maintenance
- Rail passenger & freight
- Maritime traffic control & management

**DRINKING WATER SUPPLY AND DISTRIBUTION**

- Waste water treatment
- Storage, supply & quality assurance

**HEALTHCARE SECTOR**

- Inpatient medical care
- Distribution of life sustaining drugs
- Laboratory diagnostics

**BANKING AND FINANCE**

- Cash supply
- Payment transmission
- Banking
- Stock exchange

**GOVERNMENT SERVICES**

- Pension/Service
- Payments treasury dept.
- Legislative offices

# NISD Timeline

| Date | entry into force + … | Milestone |
|---|---|---|
| August 2016 | - | Entry into force |
| February 2017 | 6 months | Cooperation Group begins tasks |
| August 2017 | 12 months | Adoption of implementing on security and notification requirements for DSPs |
| February 2018 | 18 months | Cooperation Group establishes work programme |
| **May 2018** | **21 months** | **Transposition into national law** |
| **November 2018** | 27 months | **Member States to identify operators of essential services** |
| **May 2019** | 33 months (i.e. 1 year after transposition) | **Commission report assessing the consistency of Member States' identification of operators of essential services** |
| May 2021 | 57 months (i.e. 3 years after transposition) | Commission review of the functioning of the Directive, with a particular focus on strategic and operational cooperation, as well as the scope in relation to operators of essential services and digital service providers |

# Energy sector - ENISA Activities

- DG-ENER
  - European Energy Cybersecurity Strategy – DG ENER
  - SGTF2 -> Cybersecurity Network Code for energy utilities
- Information Sharing / Mobilising community
  - EE-ISAC
  - TNCEIP
  - GIE

# Open issues …

- Appointment of a central authority for Energy sector cyber security
- Harmonization of security requirements across the EU
- Development of security standards for energy systems
- Mandatory reporting of security incidents
- Information sharing - Establishment of a stakeholder network for energy security
- Establishment of a certification board

# ENISA's role

**01** Raise the level of awareness on Infrastructure security in Europe

**02** Support Private and Public Sector with focused studies and tools

**03** Facilitate information exchange and collaboration

**04** Foster the growth of communication networks and industry

**05** Enable higher level of security for Europe's Infrastructures

# Conclusion

# Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu