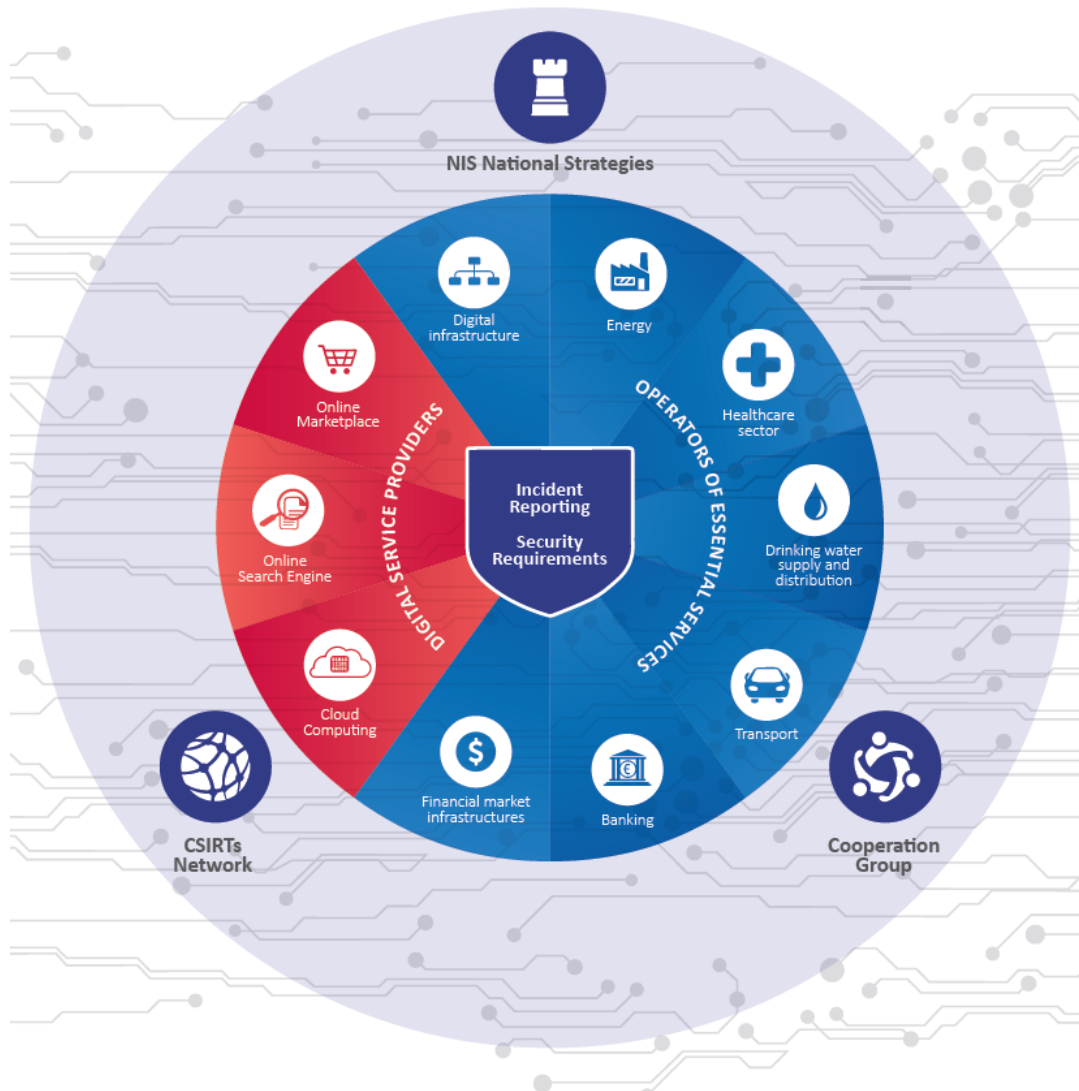


Konstantinos Moulinos | Information Security Expert | 3rd IMPROVER-ERNICIP Operators Workshop | Lisbon | 23.05.2018



NIS Directive



ENISA's role in the NISD



- 01** Assist MS and the EU Commission

- 02** Participate in the EU NIS Cooperation Group

- 03** Secretariat for CSIRTs Network

- 04** Elaborate advices and guidelines regarding standardization in NIS security

- 05** Organize exercises

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

National Cyber Security Strategies



- All 28 MS have a NCSS
- Challenges:
 - Effective cooperation between public stakeholders
 - Establish trust between public and private stakeholders
 - Lack of resources
 - Lack of common approach and awareness for privacy
 - The implementation of vulnerability and risk analysis
- MS are considering reviewing their NCSS in the light of the NISD



DSPs & OESs Obligations



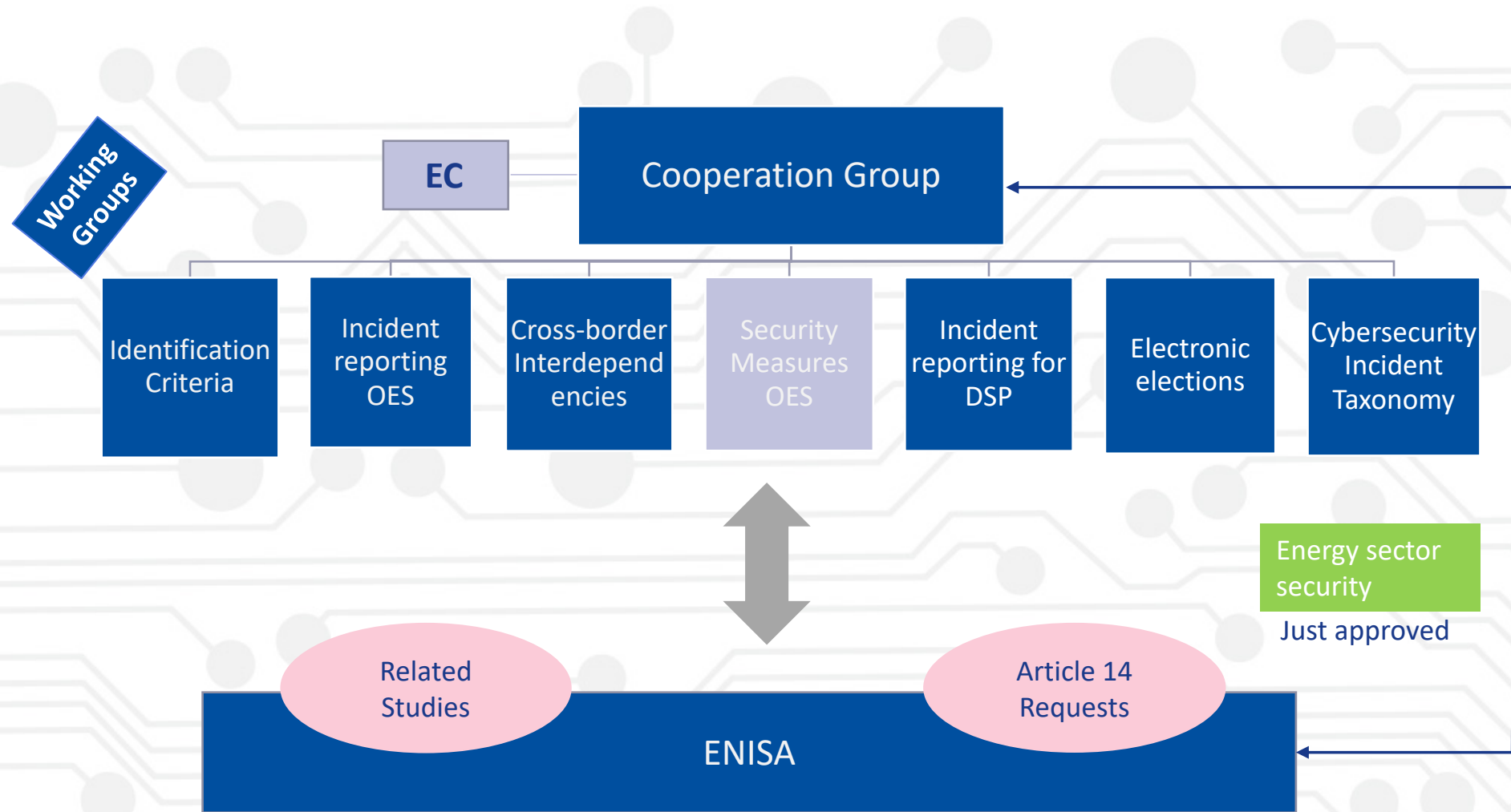
Commonalities

- Security measures
- Incident notification

Differences

- Identification criteria
- Audit
- Implementing Acts
- Light touch approach
- Medium & Large enterprises

OES obligations



Identification criteria for OES



Main steps for MS to create and list OES:

- **Identify the essential services** that are critical for societal and economic activities.
- **Identify operators of essential services:** define specific criteria and thresholds.
- **Identify critical business processes and assets that support the provision of essential services.**
- **Create a list of OES.**
- **Review and update the list of OES every two years.**



Security measures for OESs

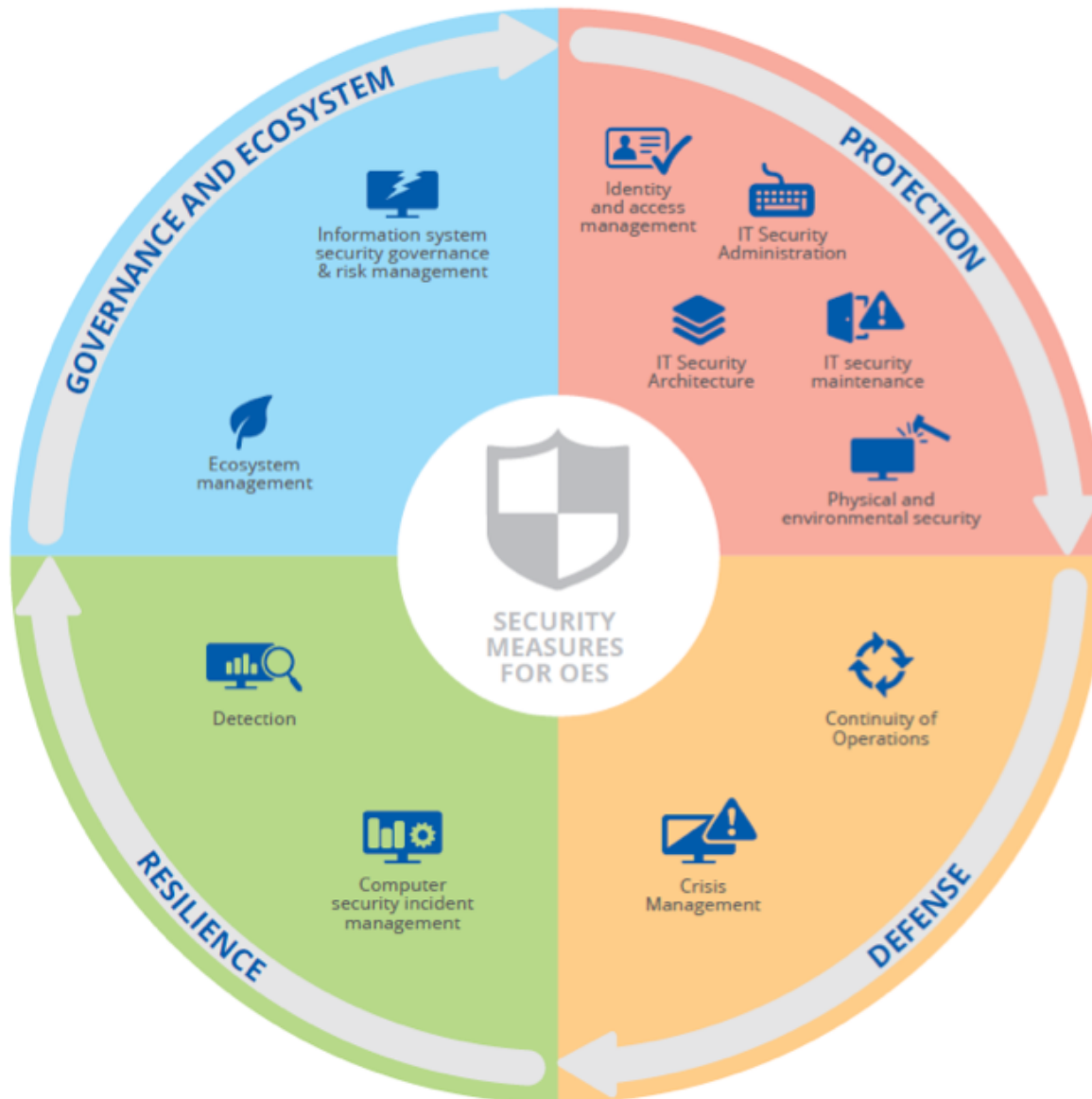


- Security measures reference document
 - List of standards and good practices
 - Cooperation Group survey on the process of identification of security measures at national level

Published

http://ec.europa.eu/information_society/newsroom/image/document/2018-19/reference_document_security_measures_version_to_be_published_44F171BD-9E21-9945-FB43065BDD852E89_52065.pdf

Security Measures for OES



Significance of incidents



multiple parameters



multiple thresholds



IMPORTANT

σημαντικό περιστατικό

significant incident

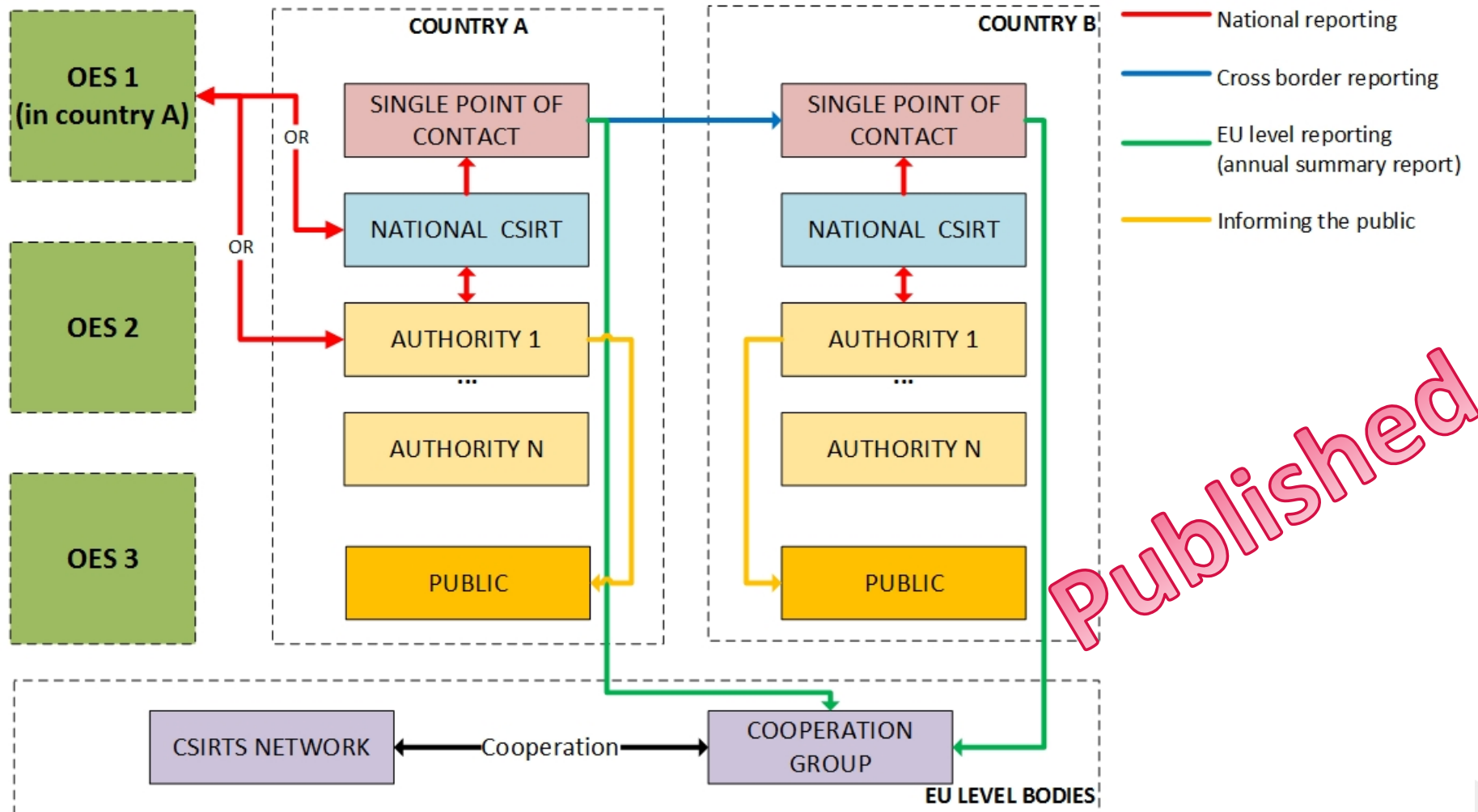
incident significatif

märkimisväärne vahejuhtum

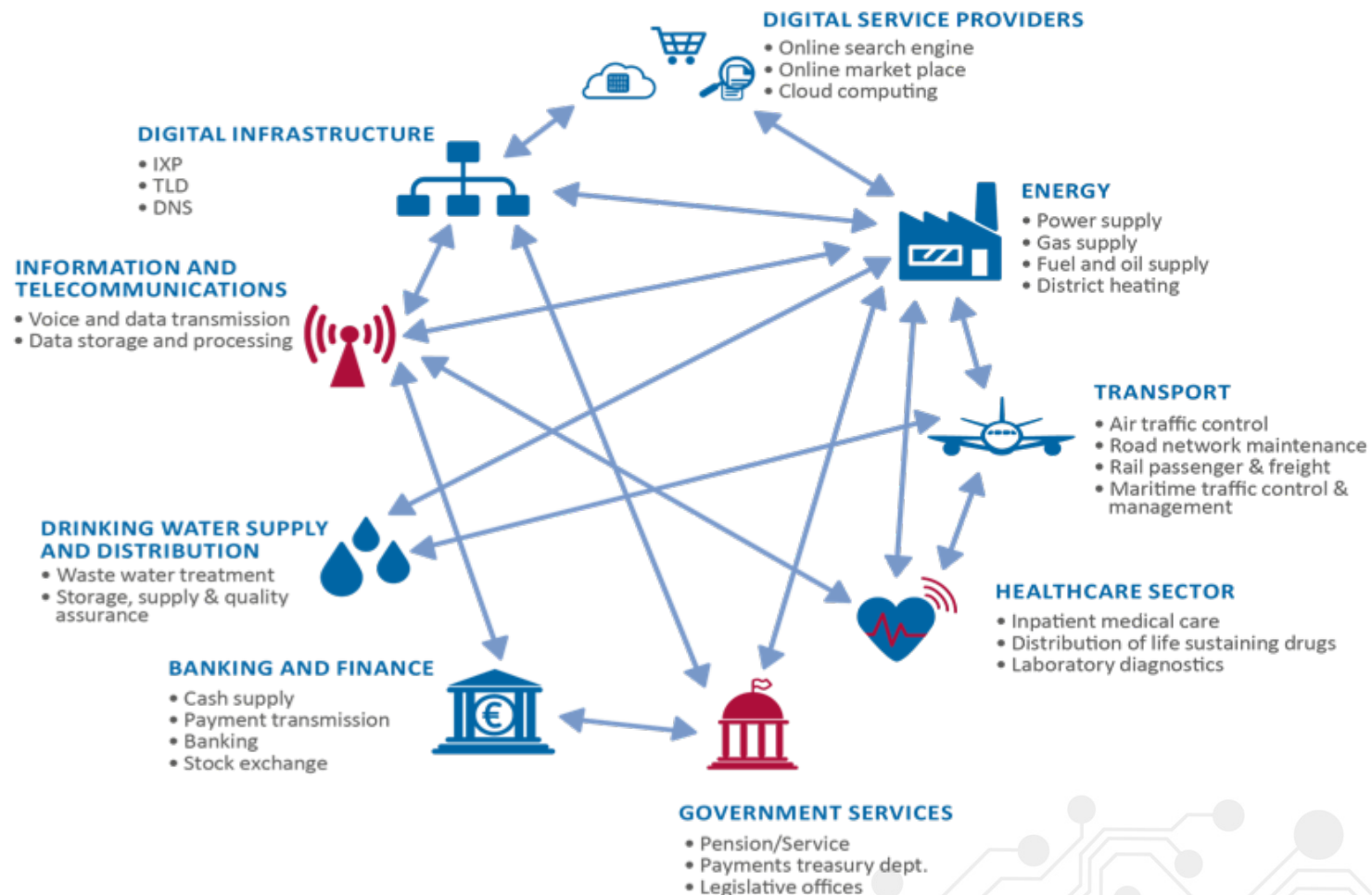
значителен инцидент

incidente significativo

Incident Reporting for OES: the process



Cross border interdependencies



Under development



1. Good practice on consultations for cross border OES (art. 5(4))
2. Data formats and procedures for notification for OES
3. Data formats and procedures for notification for DSP
4. Compendium on Cyber Security of Election Technology
5. Cross border dependencies
6. Cyber security incident taxonomy

Cooperation Group Challenges



- Low engagement of MS
 - Few MSs with experience on the topics
 - Challenges in meeting deadlines by the MSs
- Vague definitions of DSP
- Diverse views regarding the approaches
 - Reluctance to adopt elements which lead to convergence
 - Some MS follow vertical while others cross cutting approach
- Delays in transposition

Different security requirements stemming from other regulations e.g GDPR

Conclusions



1

Cyber attacks on CIs is now the norm than a future trend.

2

Enable higher level of security for Europe's Infrastructures.

NISD first piece of work at EU level
Updated Cyber security strategy

3

MS and private sector, with the assistance of ENISA, should co-operate to protect CIs

- sharing experiences and information
- developing and deploying good practices
- co-operate with NRAs to achieve EU wide harmonization of EU regulations

4

"Collaboration is Everything".





Thank you



PO Box 1309, 710 01 Heraklion, Greece



Tel: +30 28 14 40 9710



info@enisa.europa.eu



www.enisa.europa.eu

