Digital Ship's Maritime Cyber Resilience Forum Athens

Rossella Mattioli

Secure Infrastructures and Services

European Union Agency for Network and Information Security

Securing Europe's Information society

Positioning ENISA activities

CAPACITY

- ✓ Hands on activities

POLICY

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

COMMUNITY

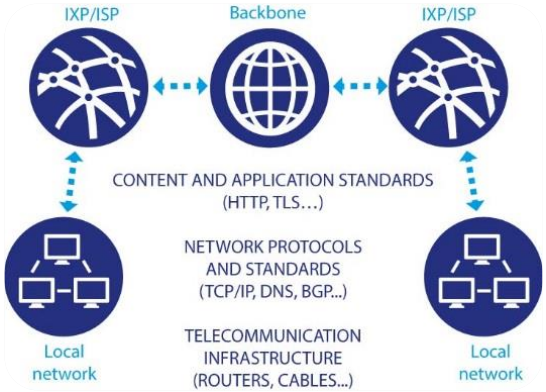
Mobilizing EU communities

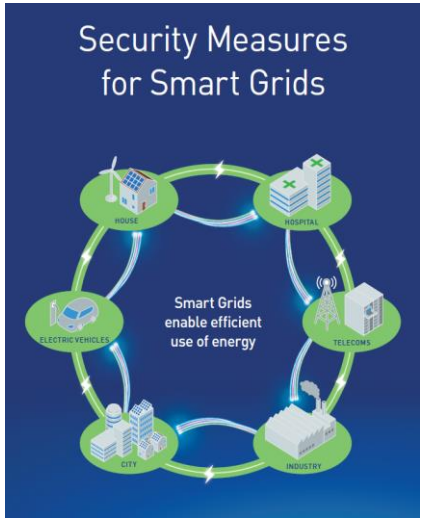
EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

Secure Infrastructure and Services

Communication networks: Critical Information Infrastructure and Internet Infrastructure





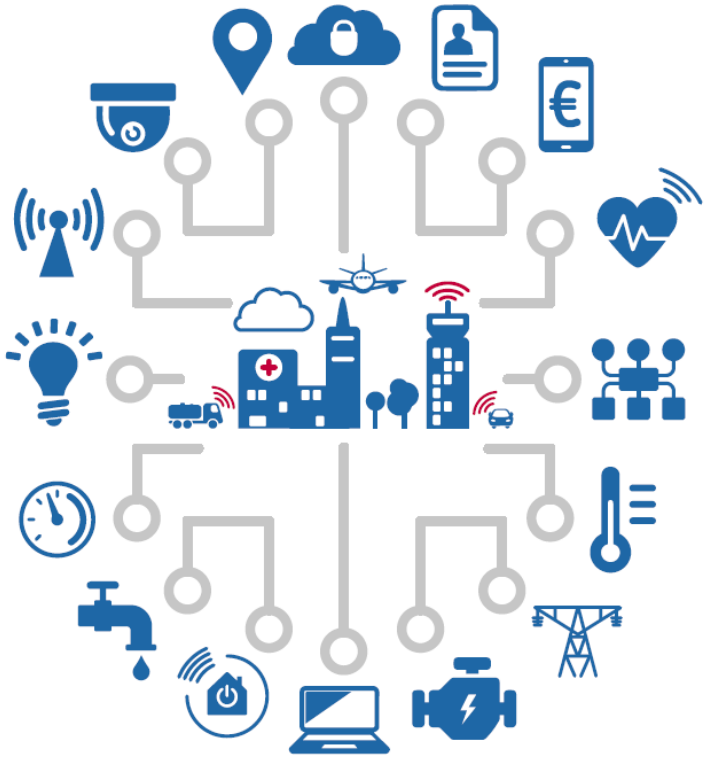
Transport

eHealth and Smart Hospitals

Finance

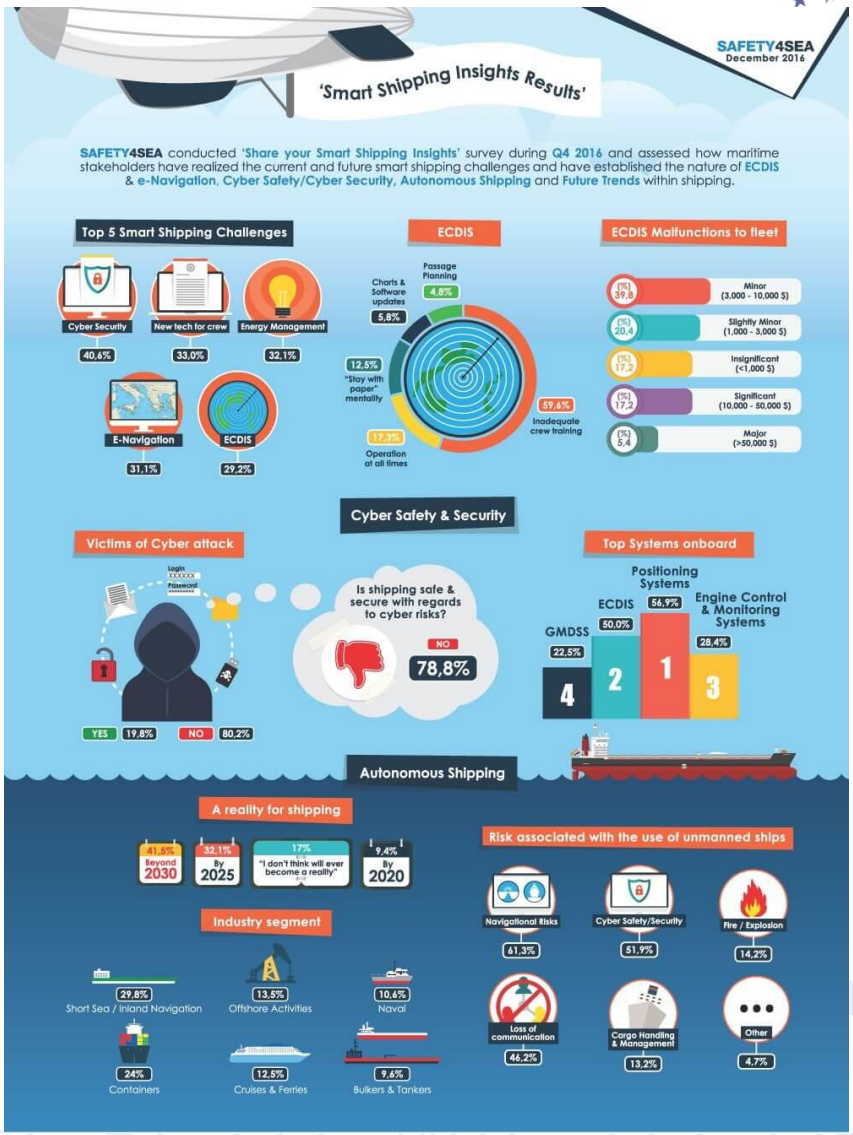
https://www.enisa.europa.eu/topics

Securing Europe's transport infrastructure



Everything becomes connected

- Fundamental component of European and national Critical Infrastructures
- Passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies
- Advanced data collection and processing
- Statistics and remote control
- Convergence and interconnection with devices and services
- More functionalities



http://www.safety4sea.com/smart-shipping-survey-findings/

What could possibly go wrong?

Shipping industry vulnerable to cyber attacks and GPS jamming

Luke Graham | @LukeWGraham
Wednesday, 1 Feb 2017 | 8:32 AM ET

CNBC

The shipping industry is increasingly at risk from cybersecurity attacks and a gap in insurance policies is leaving them vulnerable, industry experts have told CNBC.

Cybersecurity has come into focus
become more capable. Meanwhile,
electronic devices to operate.

"This includes software to run the e
systems, automatic identification sy
systems (GPS) and electronic chart
(ECDIS)," explained Matthew Montg
international law firm Holman Fenw

"The added incentive for a hacker is
high value assets and the movemer

Homeland Security

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Critical Infrastructure Security and Resilience Note

CONSEQUENCES TO SEAPORT OPERATIONS FROM MALICIOUS CYBER ACTIVITY

March 3, 2016; 1300 EST

PREPARED BY: OPERATIONAL ANALYSIS DIVISION

SECURITY

Home News Columns Management Physical Cyber

Home » Maritime Companies Warned of Cyber Attacks

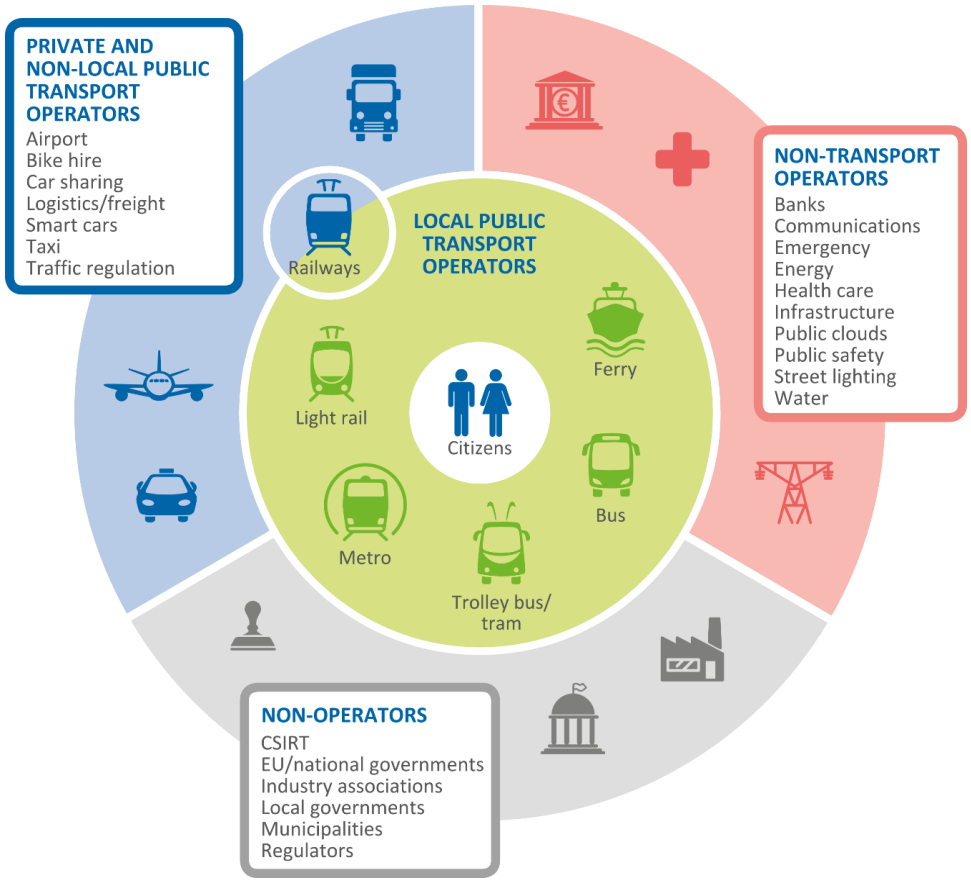
Cyber Security News | Security Newswire | Ports: Sea, Land, & Air

Maritime Companies Warned of Cyber Attacks

Ships are already under cyber attack

Tue 18 Apr 2017 by Martyn Wingrove

Securing transport in Europe



ENISA efforts:

- Understand threats and assets
- Highlight security good practices in specific sectors
- Provide recommendations to enhance cyber security
- Engage with communities

https://www.enisa.europa.eu/smartinfra

Cyber security aspects in the maritime sector

- Low awareness and focus on maritime cyber security
- Complexity of the maritime ICT environment including SCADA and emerging IoT usage
- Fragmented maritime governance context
- No holistic approach to maritime cyber risks
- Overall lack of direct economic incentives to implement good cyber security in maritime sector

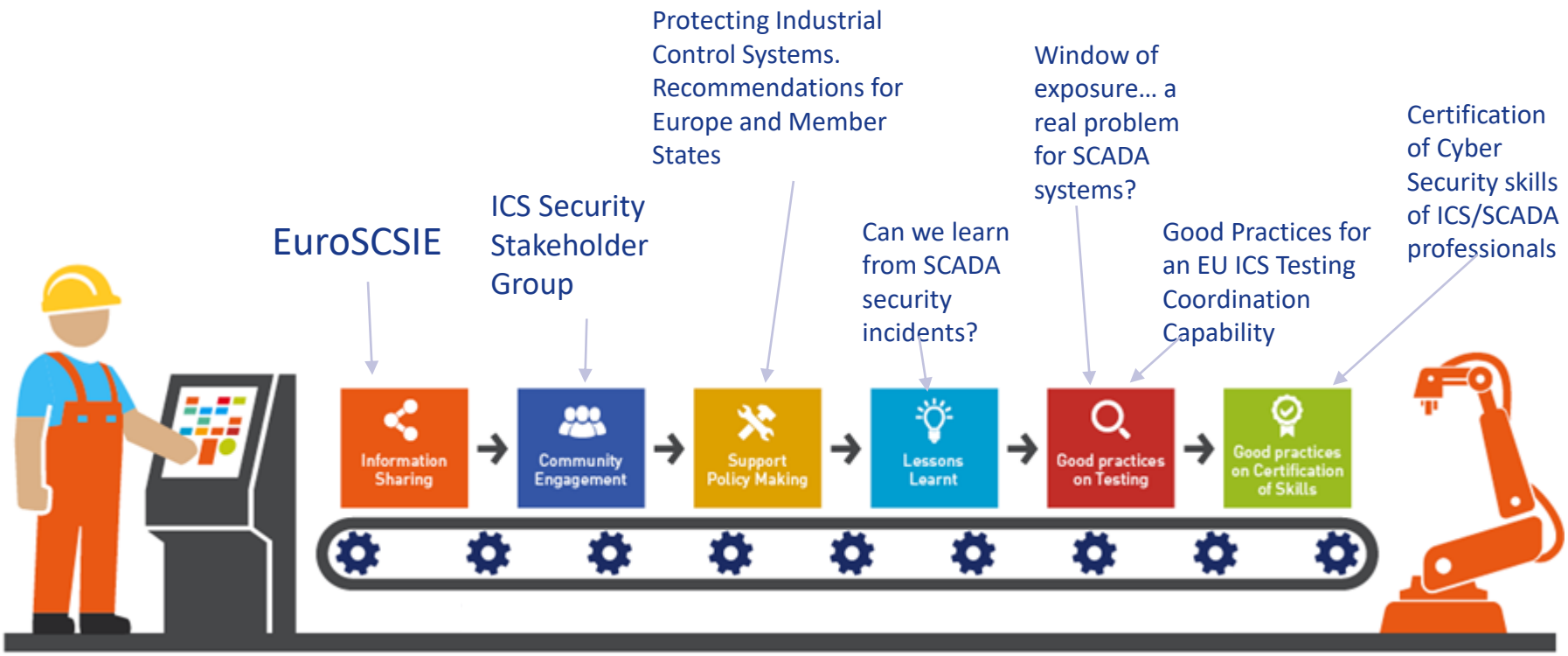
https://www.enisa.europa.eu/water

Increasing attack surface

- Positioning systems
- Electronic Chart Display and Information System (ECDIS)
- Engine Control and monitoring systems
- Global Maritime Distress and Safety System (GMDSS)
- Automatic Identification System (AIS)
- Maritime ICS SCADA
  - Alarms and safety
  - Bridge Systems
  - Passenger Servicing & Mgt.
  - Passenger - facing Networks
  - Cargo Management System
  - Etc…

Securing ICS/SCADA components in maritime

Cybersecurity for ICS SCADA



https://www.enisa.europa.eu/scada

SCADA Threats

Likelihood: Low Medium Very high

Impact: Medium /High High High/Crucial Crucial

Attacks scenarios and PoCs

- Against the administration systems of SCADA
- Against actuators
- Against the network link between sensors/actuators and HMI or controller
- Against sensors
- Against the information transiting the network
- Compromised ICT components as backdoors
- Exploit Protocol vulnerabilities
- Against Control data historian, HMI or controllers

https://www.enisa.europa.eu/scada

SCADA Good Practices

- Security in the SCADA network guidelines
- Security by Design
- Software updates
- Defense-in-depth
- Secure network communications
- Physical Security
- Wireless networking
- Staff and Top management awareness
- Asset Management
- Third-parties
- Governance and Compliance
- Malware protection

GOOD PRACTICES DESCRIPTION	RELATED ATTACK	COMPLEXITY	
1. External connections: Strict limitations and authority control are needed for it.	Unauthorized physical access, deliberate damage	MEDIUM	**Technical**: implement and use only the external network connections needed.
2. Reinforced security system: hardening of the hosts, networks and DMZ interconnections.	Unauthorized access, malicious code, network outage cascade effect	MEDIUM	**Technical**: Reinforce the security for the internal network by using DMZs (network separation).
3. Use of Virtual Private Networks: Enhancing security of remote communications by using VPNs to establish communications.	Eavesdropping, information theft.	MEDIUM	**Technical**: design and implement security measures in the VPN.
4. Simplify the internal network: Minimisation of access path to the internal network and improve the monitoring.	Unauthorized access, information theft, malicious code.	MEDIUM	**Technical**: simplify and monitoring the network.
5. Situational awareness: Regular vulnerability and pentesting inspections allow the detection of issues and allow an evaluation of the current security level of the system and network.	Attack in Control Centre System, Data Theft, Authentication exploiting.	HIGH	**Economical**: cost of implementing periodical inspections of the SCADA systems and the related infrastructure.
6. Implement Security Control: Developing control and monitoring methods to cope with any contingencies in the SCADA equipment such as intrusion detection software, antivirus software and file integrity checking software.	Unauthorized access, information theft, malicious code.	HIGH	**Technical**: develop and implement control and monitoring methods to cope with any contingencies in the SCADA equipment.
7. Network Segmentation: Using segmentation of security zone within the SCADA network and using distributed firewall within the SCADA environment to protect the end devices.	Unauthorized access, malicious code, cascade effect.	MEDIUM	**Technical**: design and implement network segregation. Carry out tests in order to verify connections.

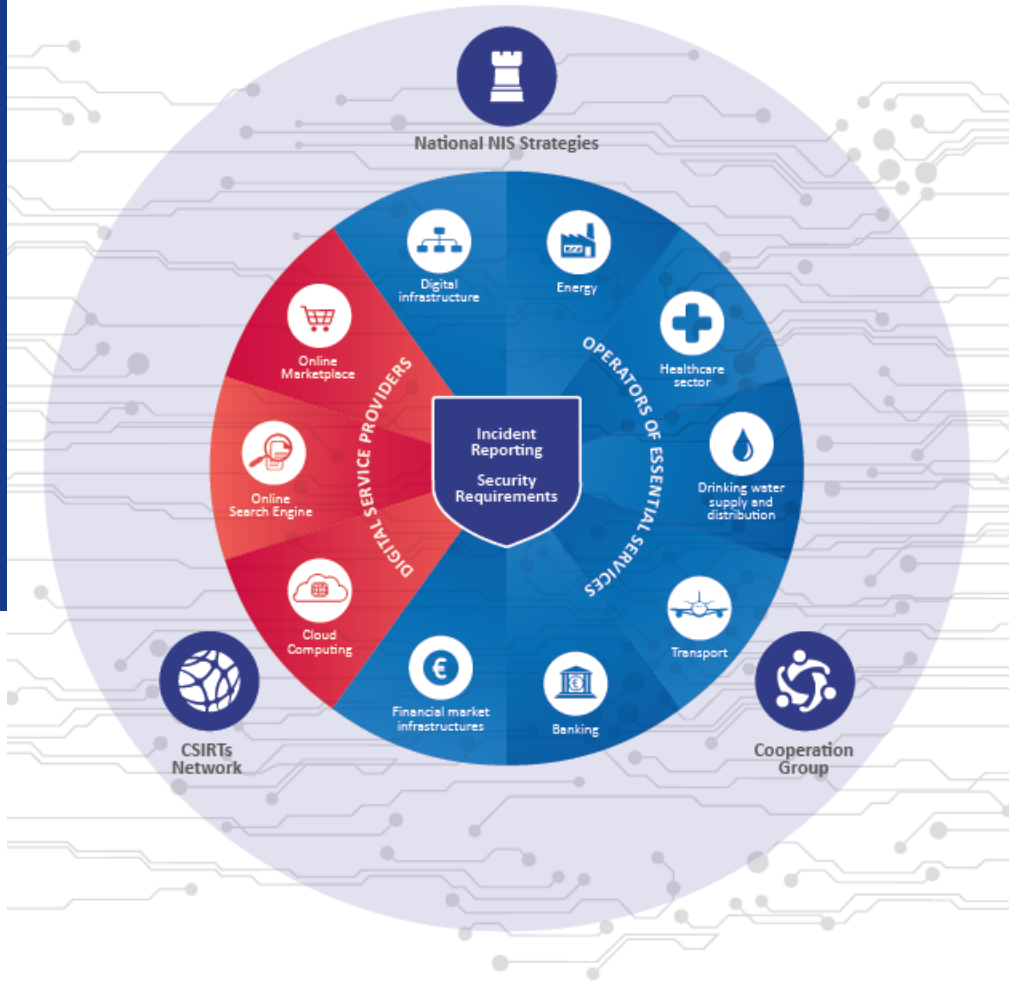
https://www.enisa.europa.eu/scada

What you can do from today:

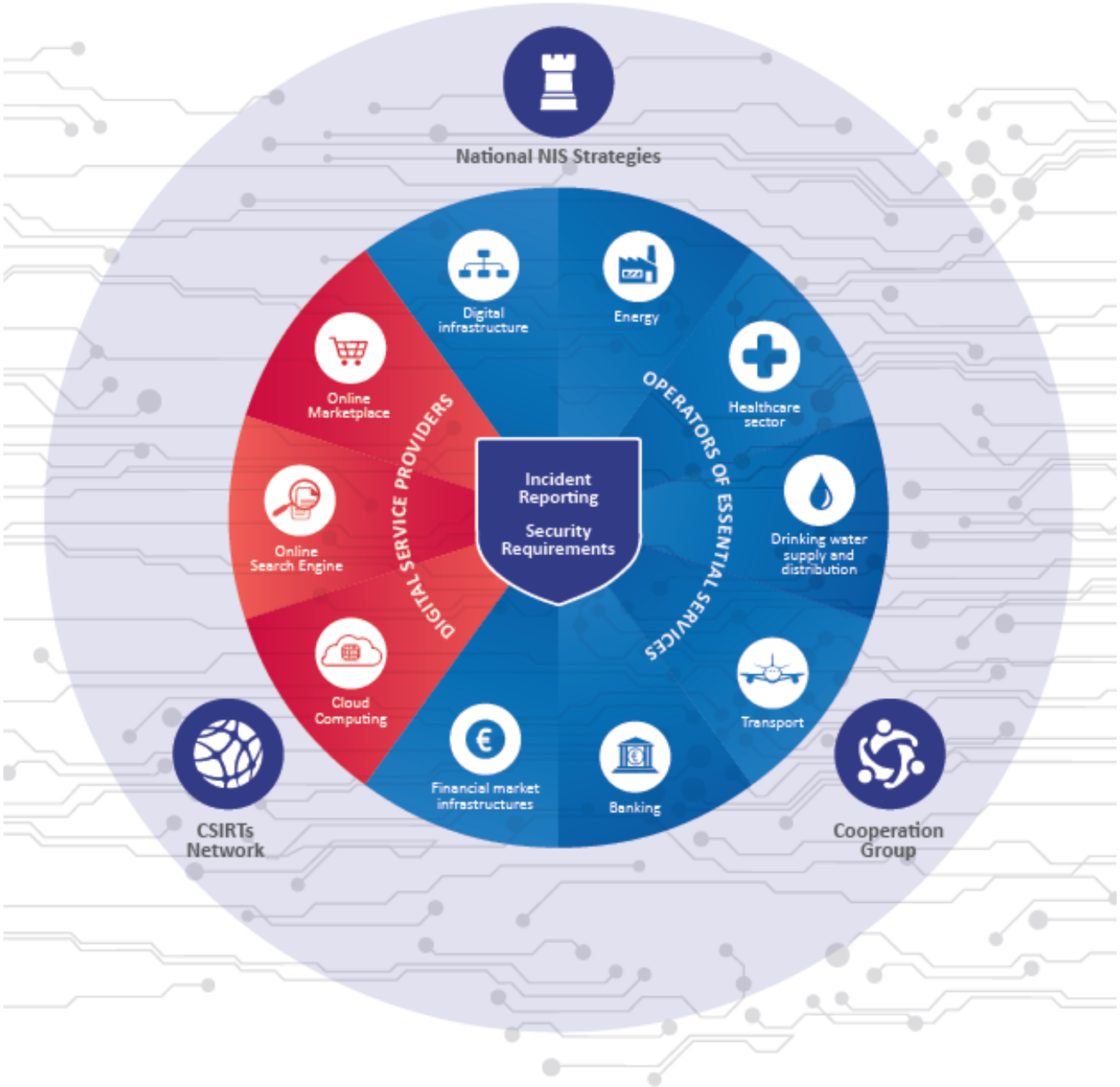
- Consider the cybersecurity impact on safety
- Include cyber security in your governance model in order to define liabilities
- Ensure you consider cyber security in all stages of the life cycle of products and services
- Consider network connectivity and interdependencies and cascading effects
- Start reusing existing good practices from other sectors, for example for SCADA

The road ahead

Network and Information Security Directive



The Network and Information Security Directive



Operators of Essential Services in the context of the NIS Directive for water transport

- Inland, sea and coastal passenger and freight water transport companies (Annex I to Regulation (EC) No 725/2004)
- Managing bodies of ports (point (1) of Article 3 of Directive 2005/65/EC), including their port facilities (point (11) of Article 2 of Regulation (EC) No 725/2004), and entities operating works and equipment contained within ports.
- Operators of vessel traffic services (point (o) of Article 3 of Directive 2002/59/EC)

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

NISD, a great opportunity for you to impact cyber security in Europe

Current open surveys on:

- Incident reporting
- Security requirements
- Dependencies of Operators of Essential Services (OES) on Digital Services Providers (DSPs)

If you are a potential OES and you are interested to contribute, just contact me.

Goals

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

Thank you,

Rossella Mattioli

resilience@enisa.europa.eu

https://www.enisa.europa.eu/