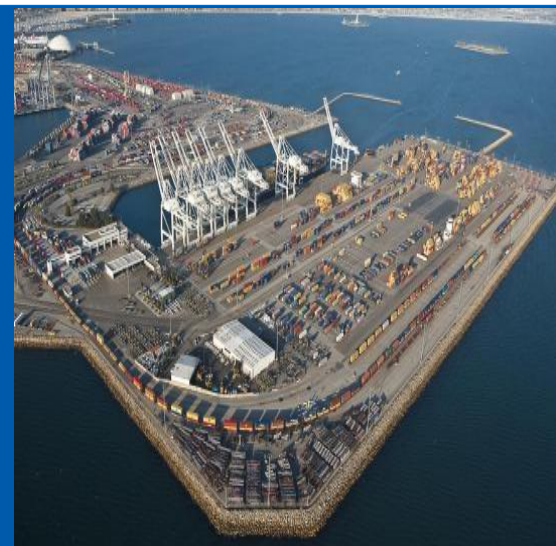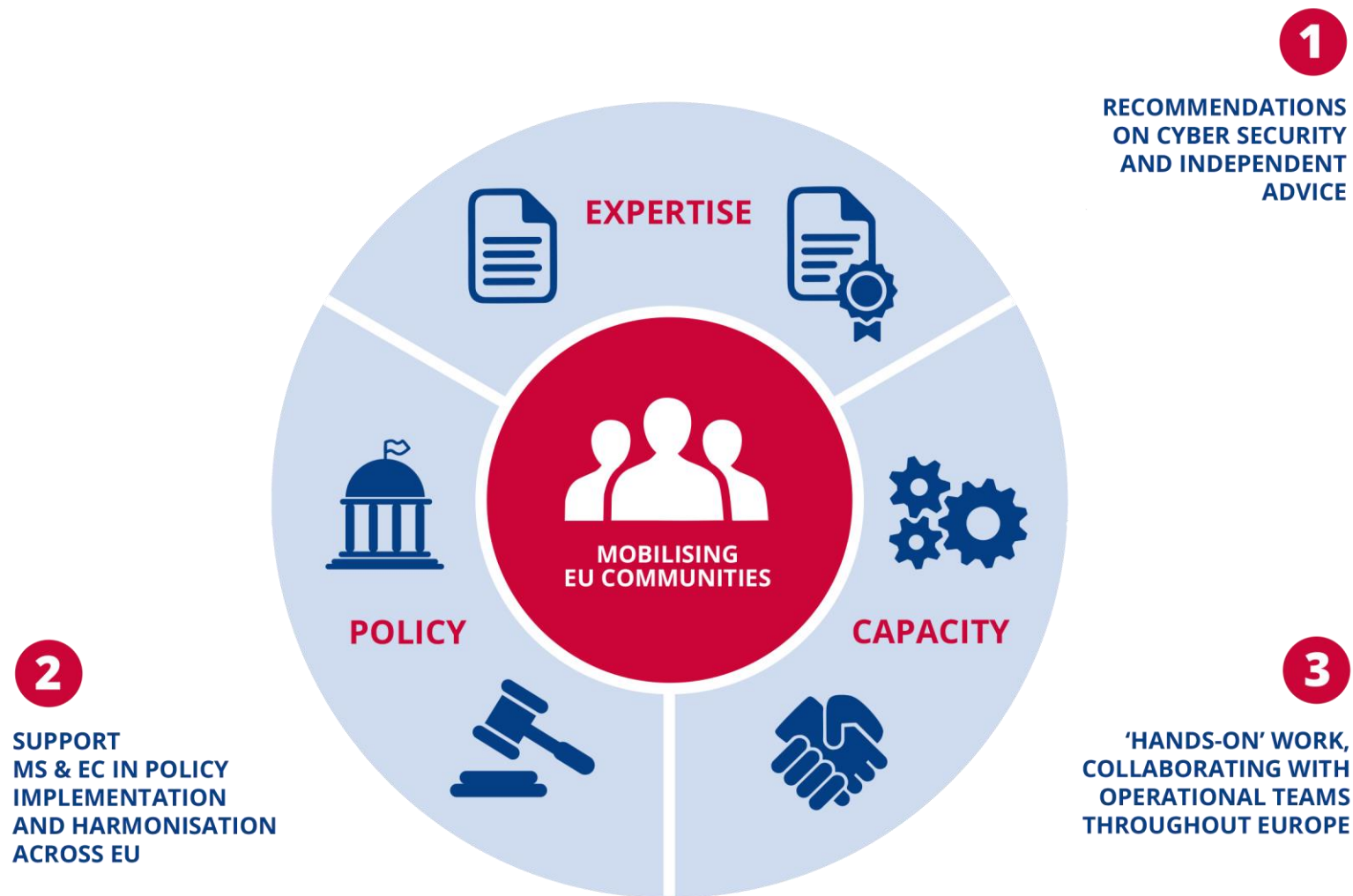# THE NIS DIRECTIVE AND CYBERSECURITY IN MARITIME

Dr. Athanasios Drougkas
Expert in Network and Information Security
European Union Agency for Network and Information Security

06 | 03 | 2019

POSITIONING ENISA'S ACTIVITIES

1 RECOMMENDATIONS ON CYBER SECURITY AND INDEPENDENT ADVICE

2 SUPPORT MS & EC IN POLICY IMPLEMENTATION AND HARMONISATION ACROSS EU

3 'HANDS-ON' WORK, COLLABORATING WITH OPERATIONAL TEAMS THROUGHOUT EUROPE

EXPERTISE

POLICY

CAPACITY

MOBILISING EU COMMUNITIES

enisa

THE MARITIME SECTOR IS UNDER ATTACK!

Hackers took 'full control' of container ship's navigation systems for 10 hours – IHS Fairplay

by Editor | Nov 25, 2017 | Blog |

Shipping firm warns that hackers may leak confidential information

Global shipbroker says it fell victim to a 'cybersecurity incident' and is contacting those who might have had their information stolen by attackers.

By Danny Palmer | November 29, 2017 -- 16:06 GMT (16:06 GMT) | Topic: Security

CNBC

MENU | MARKETS | BUSINESS NEWS | INVESTING | TECH | POLITICS | CNBC TV

ENTERPRISE

TECH | MOBILE | SOCIAL MEDIA | ENTERPRISE | CYBERSECURITY | TECH GUIDE

Shipping company Maersk says June cyberattack could cost it up to $300 million

COSCO Shipping Lines Falls Victim to Cyber Attack

COSCO Shipping Lines confirmed that it has been hit by a cyber attack impacting its internet connection within its offices in America.

COSCO SHIPPING

Police warning after drug traffickers' cyber-attack

By Tom Bateman
Reporter, Today programme

🕐 16 October 2013

f 💬 🐦 ✉ ⬥ Share

The head of Europe's crime fighting agency has warned of the growing risk of organised crime groups using cyber-attacks to allow them to traffic drugs.

The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking business.

His comments follow a cyber-attack on the Belgian port of Antwerp.

Drug traffickers recruited hackers to breach IT systems that controlled the

Earlier this year drug traffickers hacked into the computer controlling shipping containers at the port of Antwerp

Seatrade Maritime News

Building Globa

Home | News ▾ | Regions ▾ | Sectors ▾ | Live From ▾ | Jobs | Downloads ▾ | Magazine | E

Home > News > Europe > 69% of Danish shipping companies hit by cyber crime in 2017

69% of Danish shipping companies hit by cyber crime in 2017

A survey by Danish Shipping of its ceo panel showed that 69% of companies had been hit

Port of Barcelona Suffers Cyberattack

By **Ionut Ilascu**   📅 September 21, 2018   🕐 05:15 PM   💬 0

enisa

…AND VULNERABLE

Backdoor Account Found in Popular Ship Satellite Communications System

By Catalin Cimpanu

October 26, 2017   08:00 AM   0

Naval Dome exposes vessel vulnerabilities to cyber attack

More onboard cyber vulnerability has been revealed, with maritime cyber defence firm Naval Dome demonstrating yet more ways hackers can compromise ship safety.

BLOG: MARITIME CYBER SECURITY

Making prawn espressos, or hacking ships by deciphering BAPLIE EDIFACT messaging

Hackers can easily target container ships by hacking load plans due to its vulnerable messaging system

November 28, 2017 By Pierluigi Paganini

Hackers Could Sink a Bulk Carrier Says Pen Test Partners

December 19, 2017

Security

Crappy IoT on the high seas: Holes punched in hull of maritime security

Researchers: We can nudge ships off course

By John Leyden 6 Jun 2018 at 12:18   32   SHARE ▼

Why 50,000 ships are so vulnerable to cyberattacks
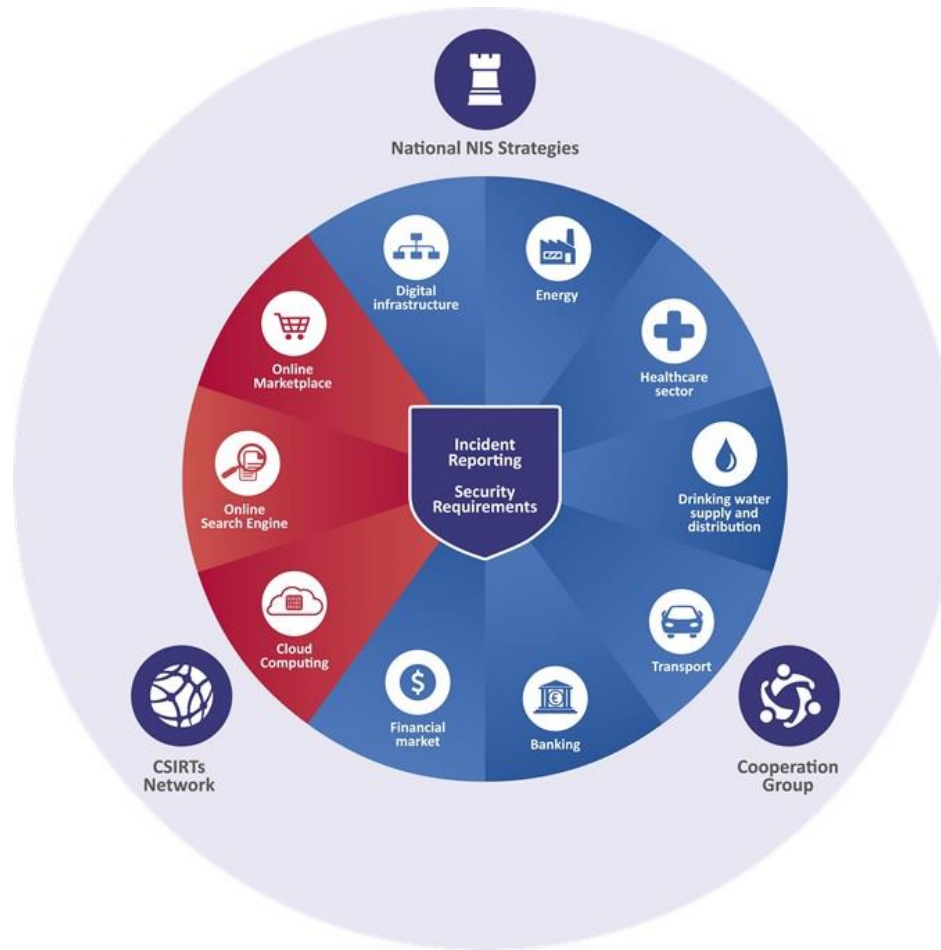
June 13, 2018 2.15pm BST

enisa

CYBER SECURITY IN THE MARITIME SECTOR – SITUATIONAL ANALYSIS

- Cybersecurity gaining more attention but still relatively **low awareness** and focus on maritime cyber security

- **Emerging standards/guidelines** from IMO, industry etc.

- **Complexity** of the maritime ICT environment including SCADA and emerging IoT usage

- Fragmented maritime **governance context**

- No holistic approach to **maritime cyber risks** and **diversity between different actors** in maritime

- Overall **lack of direct economic incentives** to implement good cyber security in maritime sector

enisa

THE NETWORK AND INFORMATION SECURITY DIRECTIVE

OBLIGATIONS FOR MS ON OES

- **<u>Identification of operators of essential services</u>**

- **<u>Minimum security measures</u> to ensure a level of security appropriate to the risks**

- **<u>Incident notification</u> to prevent and minimize the impact of incidents on the IT systems that provide services**

- **Make sure <u>authorities have the powers and means</u> to assess security and check evidence of compliance for OES**
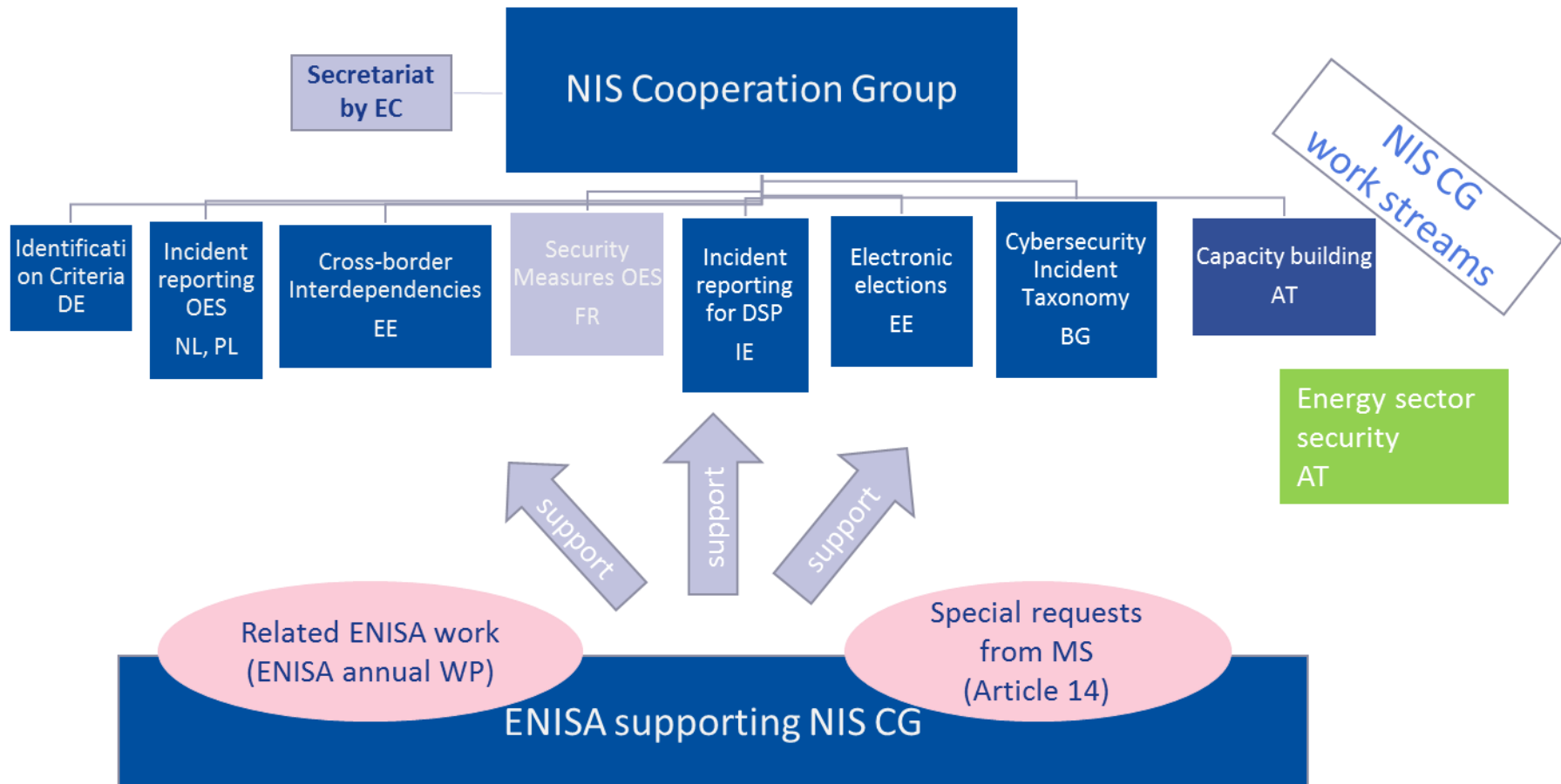
enisa

IDENTIFICATION OF OES IN THE WATER TRANSPORT SECTOR

MS shall define the criteria for the identification of OES and identify the OES among the following:

- **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)

enisa

WORKING GROUPS UNDER THE NIS DIRECTIVE

NIS DIRECTIVE - TIMELINE

August 2016	-	Entry into force
February 2017	6 months	Cooperation Group starts its tasks
August 2017	12 months	Adoption of implementing on security and notification requirements for DSPs
February 2018	18 months	Cooperation Group establishes work programme
9 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 - consistency of Member States' identification of OES
May 2021	57 months (i.e. 3 years after transposition)	Commission review

enisa

ENISA'S WORK – HOW YOU CAN HELP!

2019 Study: Port Cybersecurity

- Port CISOs/CIOs
- Input from competent authorities

NIS Directive Transposition

- National Approaches
- OES identification, Security Measures, Incident Reporting

ENISA TRANSSEC Group

- Looking for maritime cybersecurity experts!

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europe.eu