EU policies for cybersecurity in inland navigation

Dr Nineta Polemi

Programme Manager- E.U. Policies
DG CNECT/H1: Cybersecurity
Technology & Capability Building

Maritime: Backbone for economy

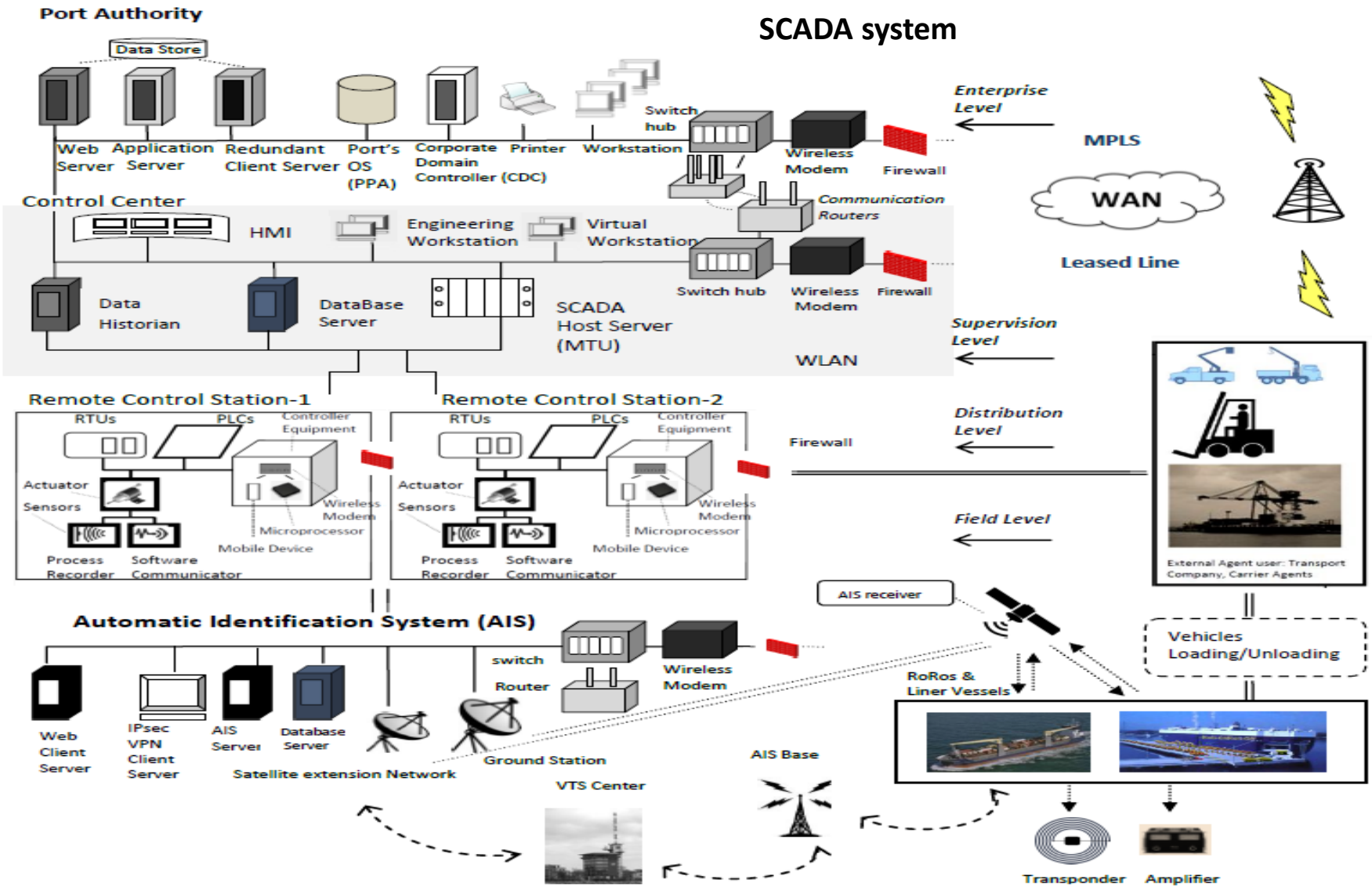
Maritime transport is . . .

- ✓ the backbone of international trade around 80% of global trade by volume and over 70% by value is carried by sea and is handled by ports worldwide
- ✓ 74% of goods entering or leaving Europe go by sea
- ✓ More than 37,000 kilometres of waterways connect hundreds of EU cities
- ✓ 13 Member States have an interconnected waterway network of cities and industrial regions.
- ✓ Attractive target: 50% of all shipping companies word-wide were victims of cyber-attacks in 2018 (NATO-NMIOTC 2019)

Maritime Cyber Activities depend upon:

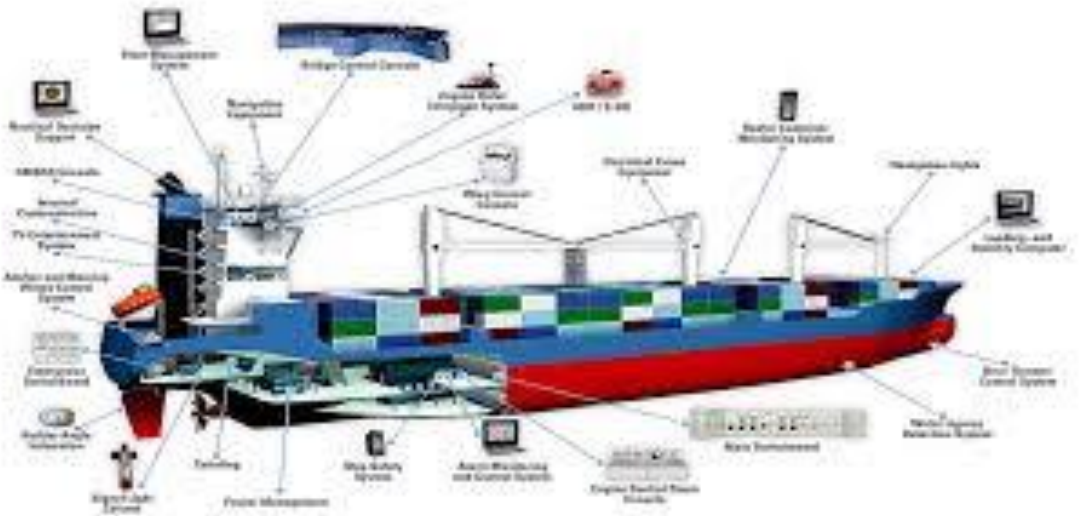
- Critical Infrastructures –CIs- (Information and Space CIs)
- Common cyber assets e.g. networks, ICT components, technical capabilities
- EU & international policies and agreements
- Supply Chains

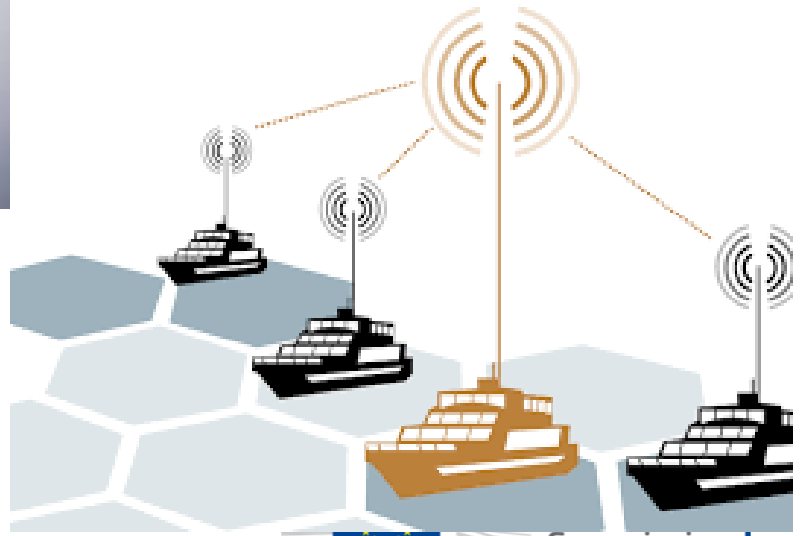
Ports' complex ICT



European Commission

Digitalization





Ships are expensive assets (more than 20 million euros is the value of a cargo ship)

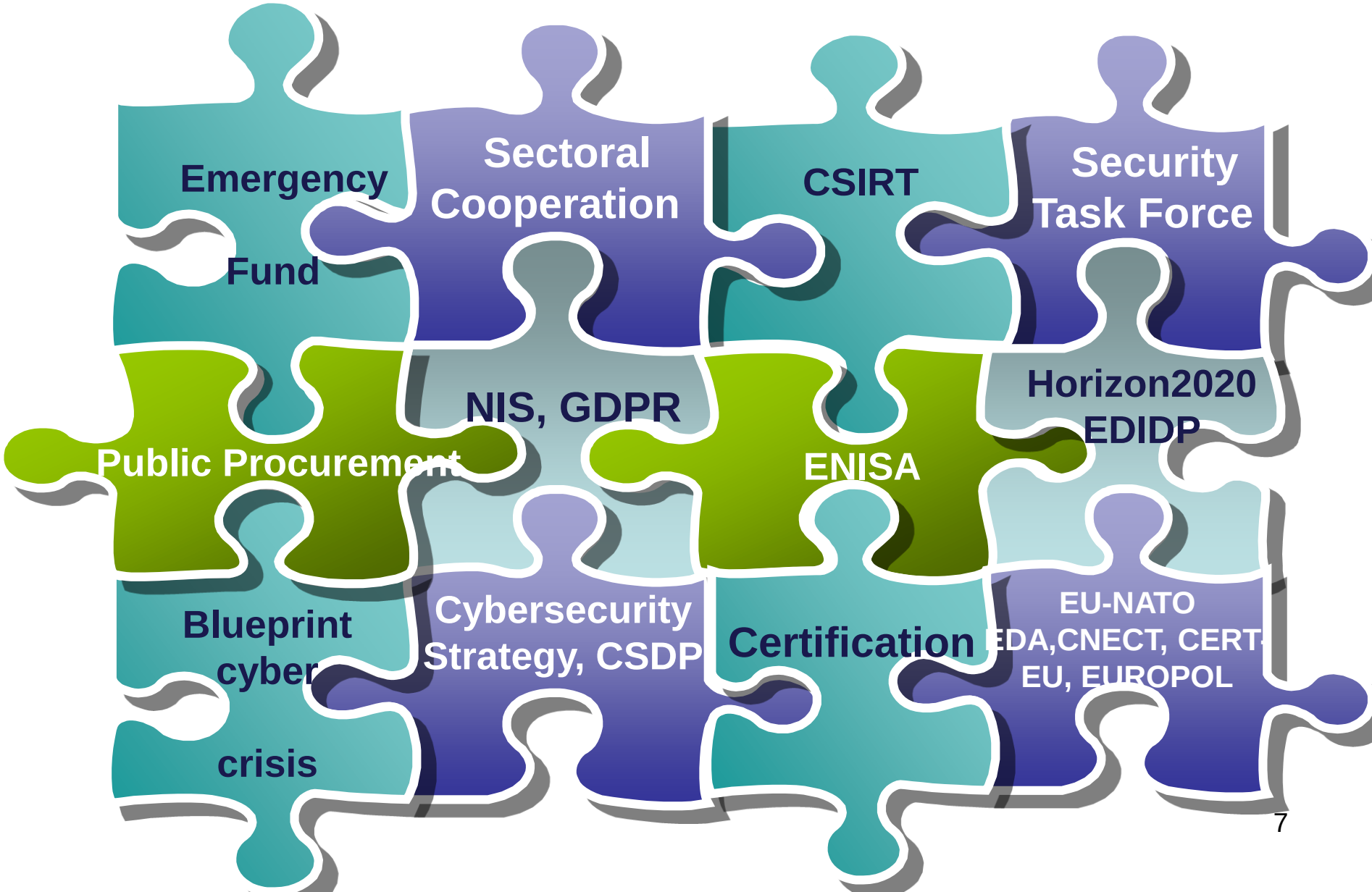
Common maritime attacks

- ✓ GPS spoofing
- ✓ Unauthorized access to on-board mobile devices
- ✓ manipulation of Bill of lading
- ✓ signals jamming, monitoring
- ✓ targeted access on automated terminal infrastructures (e.g. electronic gates, RFIDs in containers, cameras, surveillance systems)
- ✓ spear phishing, DoS,…….

2018 attacks: Maersk, Port of Barcelona
US Ports (Long Beach, San Diego),
Austal, Royal Navy of Oman

European Commission

E.U. in Action


Emergency
Fund
Sectoral
Cooperation
CSIRT
Security
Task Force
Public Procurement
NIS, GDPR
ENISA
Horizon2020
EDIDP
Blueprint
cyber
crisis
Cybersecurity
Strategy, CSDP
Certification
EU-NATO
EDA,CNECT, CERT-
EU, EUROPOL

EU Maritime Cybersecurity Regulation/Policies

- *Regulation **No 725/2004** on enhancing ship/port facility security*
- *Directive **2005/65** on enhancing port security*
- *Regulation **324/2008**: inspections in the field of maritime security.*
- *Directive (EU) 2016/1148 sets cybersecurity obligations –**NIS**-*
- *2016 **EU-NATO Joined Declaration** (…enhance coordination, complementarity and cooperation in the maritime domain)*
- *eIDAS Regulation (2014) on electronic identification*
- *2016 Directive **85/374**/EEC on **product liability***
- *Regulation 2016/679 on protection of privacy –**GDPR**-*
- Space Strategy for Europe 2016/2325(INI)
- *Regulation COM(2017)477 **Cybersecurity Act***
- *2018 Revised EU Maritime Security Strategy (emphasizes the need for improving the integration of cybersecurity)*

European Commission

MARITIME CYBERSECURITY GUIDELINES

- SOLAS XI-2 and the ISPS Code
- Guidelines on maritime cyber risk management (IMO)
- ETSI TR 103 456 CYBER; Implementation of the NIS COM(2017) 476 final "Making the most of NIS"
- C(2017)6100 final Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (**blueprint**)
- Cyber Diplomacy Toolbox
- The Tanker Management/ Self Assessment - TMSA (OCIMF)
- The Guidelines on Cyber Security Onboard Ships (supported by: BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI)
- Cyber Security Awareness -AMMITEC
- IACS Cyber Panel Systems (2015)

E.U. Initiatives

- ✓ cPPP-**ECSO** (2016)
- ✓ Digital European **Industry** Initiative (2016)
- ✓ Electronic Components and Systems (**ECSEL JU**)
- ✓ Supercomputers (**EuroHPC JU**)
- ✓ **5G** Action Plan (2016)
- ✓ Framework for screening foreign investment
- ✓ Strategic Forum for Important Projects of common European Interest (**IPCEI**)
- ✓ Digital Skills and Jobs Coalition
- ✓ Space Programme (2018)
- ✓ **AI** Declaration/ AI Communication (2018)
- ✓ Communication on **online disinformation** (April 2018)

E.U. Maritime Cyber Security R&D

CYSM, MEDUSA: Static SC RM' methodology and tools

MITIGATE: Dynamic evidence-driven Maritime SC RM environment (simulation, crowd-sourcing, open data) (ISO27001, 27005, ISPS, CIIP, ISO28000)

SAURON: Situational Awareness platform

TRITON Trusted Vessel Information from Trusted On-board Instrumentation SEABILLA Sea Border Surveillance)

MARINE-EO Bridging Innovative Downstream Earth Observation and Copernicus enabled Services for Integrated maritime environment, surveillance and security

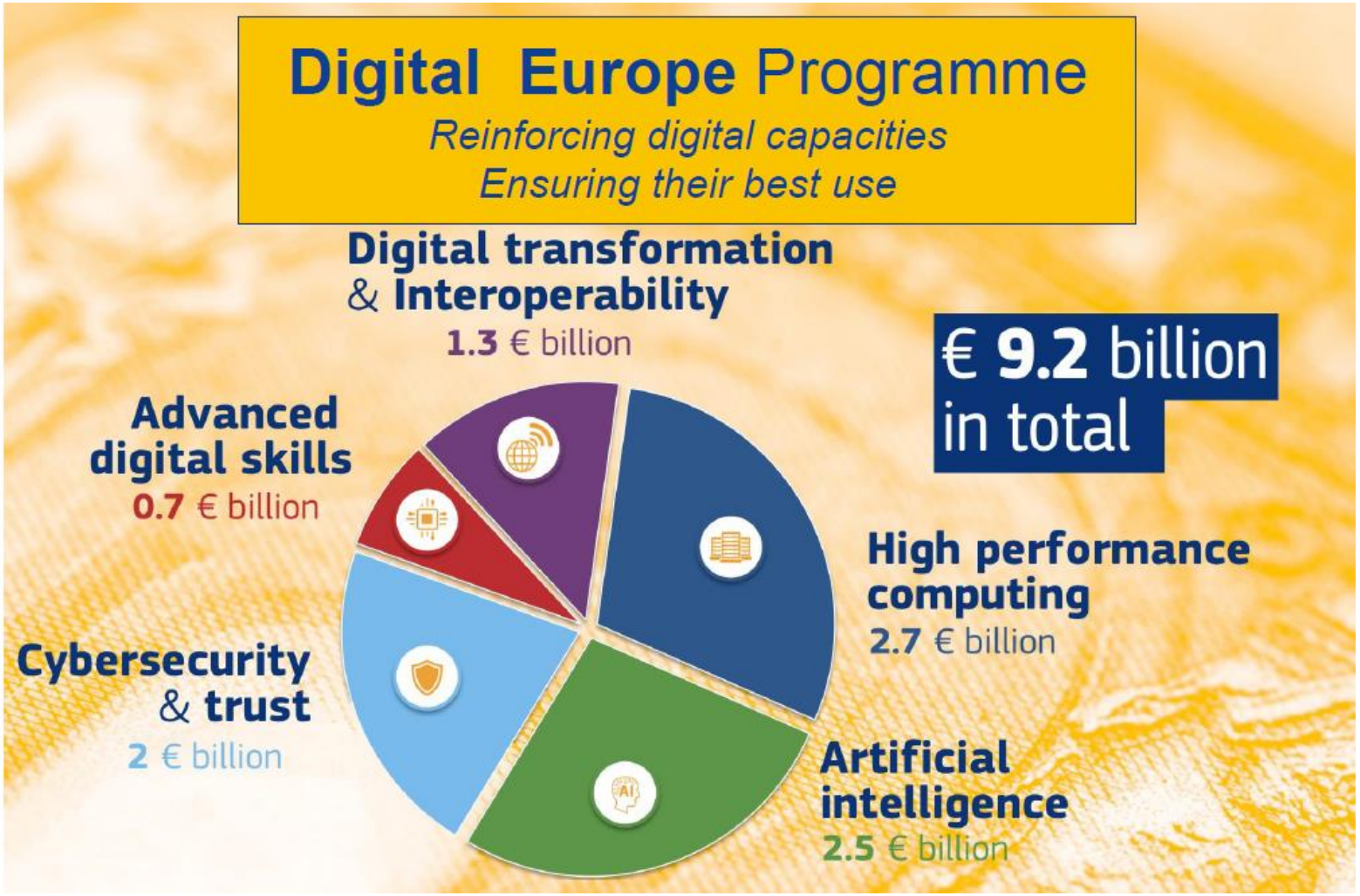
CEF Maritime Transport Projects 2014-2019

The future

Future Threats

- ✓ International **Supply chains, AI** and **5G** will bring severe attacks causing tremendous damages from making vessels invisible to destroying their fire-alarm systems to disrupting their cargo management systems.
- ✓ The on-board connected IT systems (e.g. cargo management, bridge systems, passengers servicing, communication systems etc.) more and more are provided by international suppliers with **non EU security certifications**, more vulnerable to attacks.
- ✓ The vessels are controlled by their inland shipping company, but operated by the on-board technical departments with no necessary **cyber skills.**

The Digital Europe Programme 2021-2027



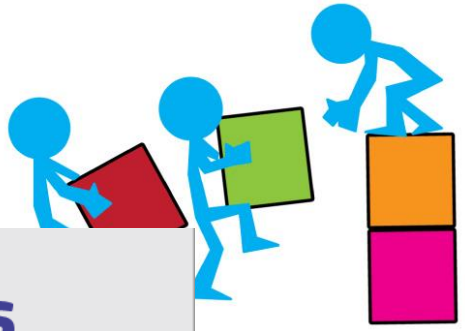
The Cybersecurity Competence Centre and Network (CCCN)

Brussels, ***12.9.2018*** *COM(2018) 630 final*

2018/0328 (COD) REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL **establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres**

European Commission

Preparing for CCCN



More than €63.5 million invested in 4 projects

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Partners: **46**

EU Member States involved: **14**

Key words
- SME & startup ecosystem
- Ecosystem for education
- Socio-economic aspects of security
- Virtual labs and services
- Threat Intelligence for Europe
- DDoS Clearing House for Europe
- AI for cybersecurity
- Post-Quantum cryptography

Cyber Security for Europe

Partners: **43**

EU Member States involved: **20**

Key words
- Cybersecurity for citizens
- Application cases
- Research Governance
- Cyber Range
- Cybersecurity certification
- Training in security

ECHO

Partners: **30**

EU Member States involved: **15**

Key words
- Network of Cybersecurity centres
- Cyber Range
- Cybersecurity demonstration cases
- Cyber-skills Framework
- Cybersecurity certification
- Cybersecurity early warning

SPARTA

Partners: **44**

EU Member States involved: **14**

Key words
- Research Governance
- Cybersecurity skills
- Cybersecurity certification
- Community engagement
- International cooperation
- Strategic Autonomy

Last updated 26 February 2019

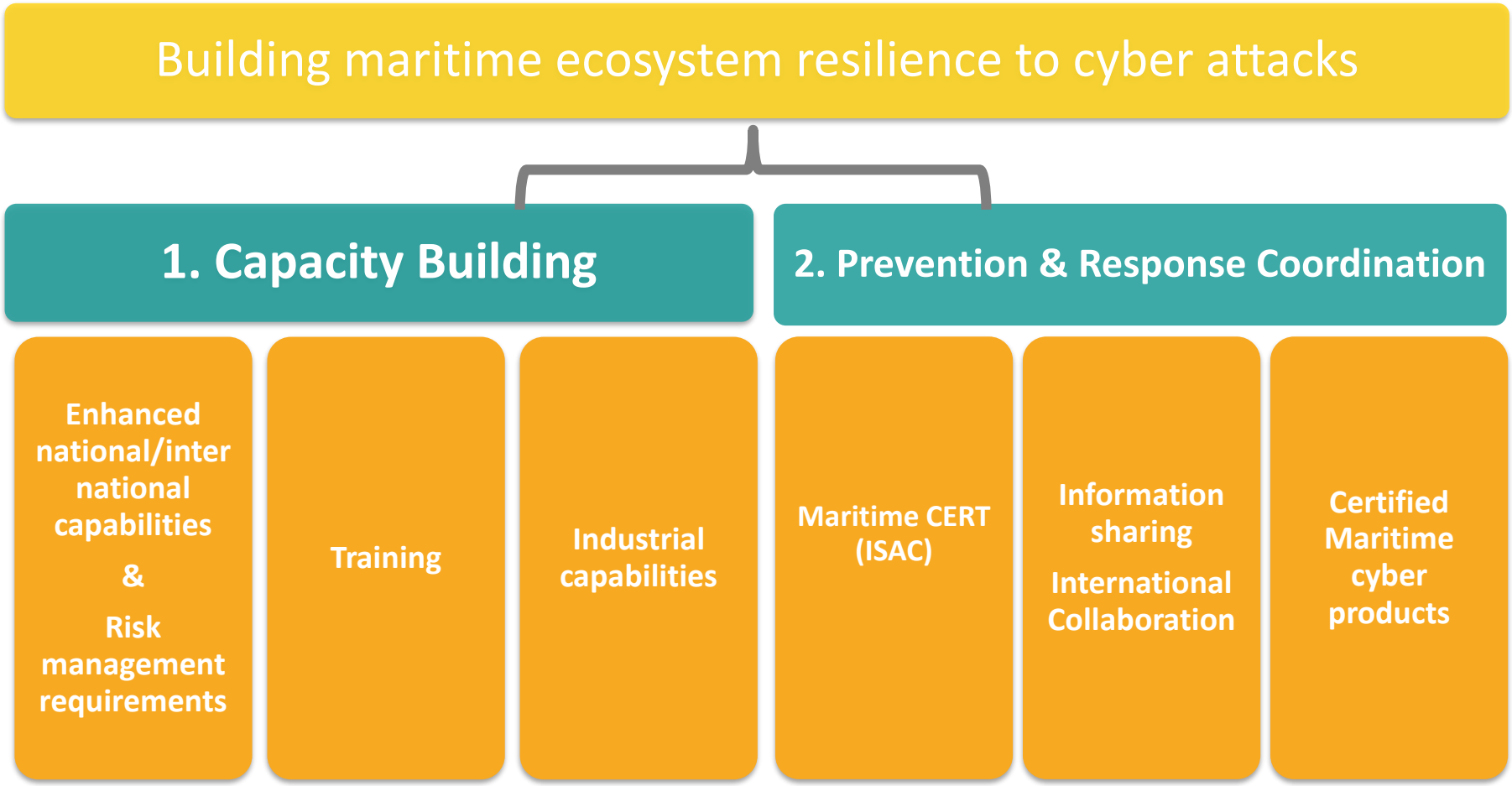
More than 160 partners from 26 EU Member States

More info at:

https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

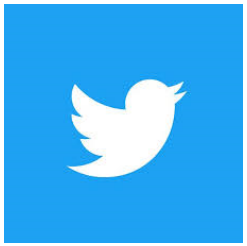
European Commission

Maritime Cybersecurity: A strategic priority



European Commission

Follow us on get involved:

On  : *https://twitter.com/Cybersec_EU*

Subscribe to our newsletter:
http://europa.eu/!yT68Jg

European Commission

Thank you for your attention!

Nineta.POLEMI@ec.europa.eu