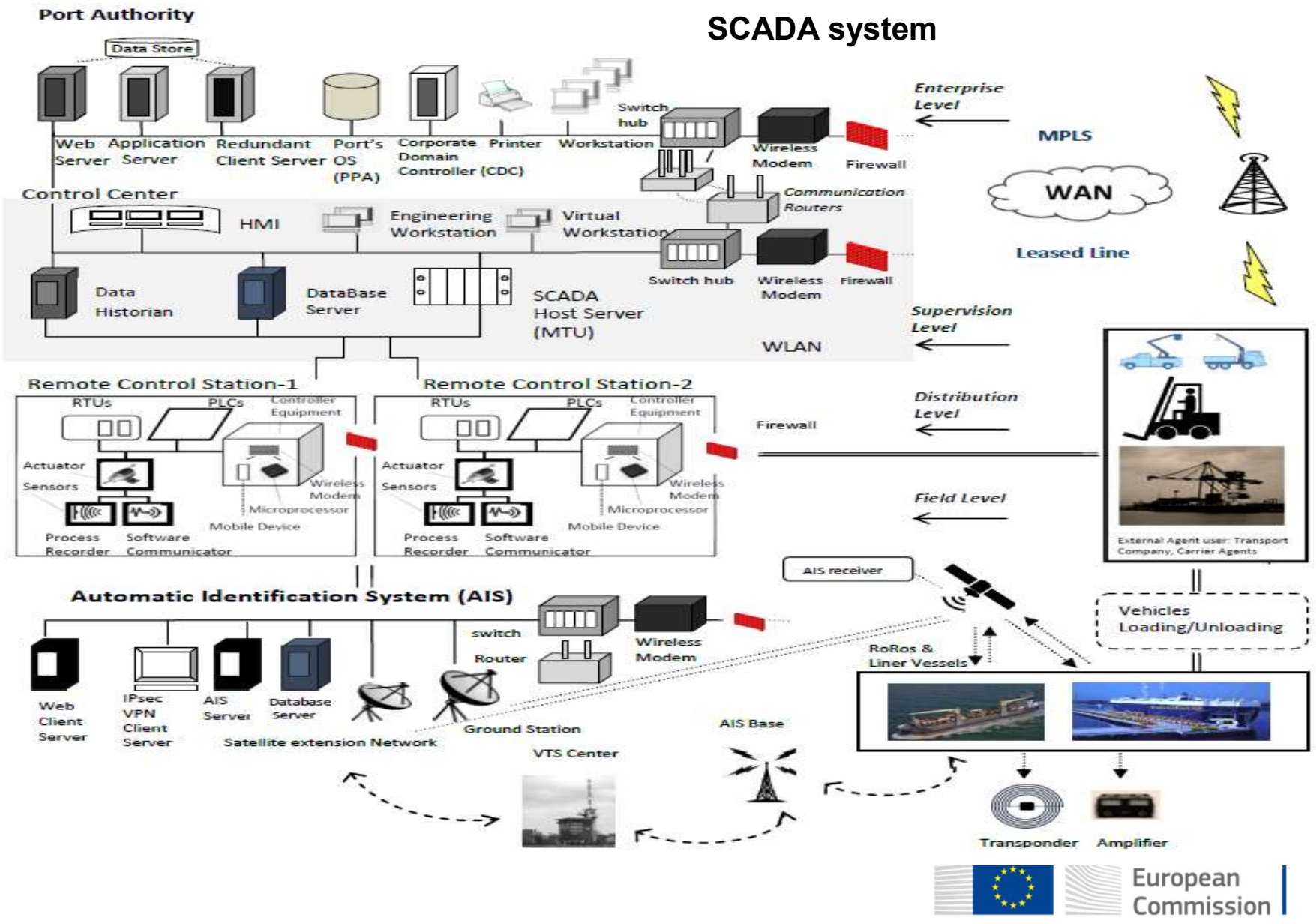
EC efforts in securing the maritime ecosystem

Dr Nineta Polemi

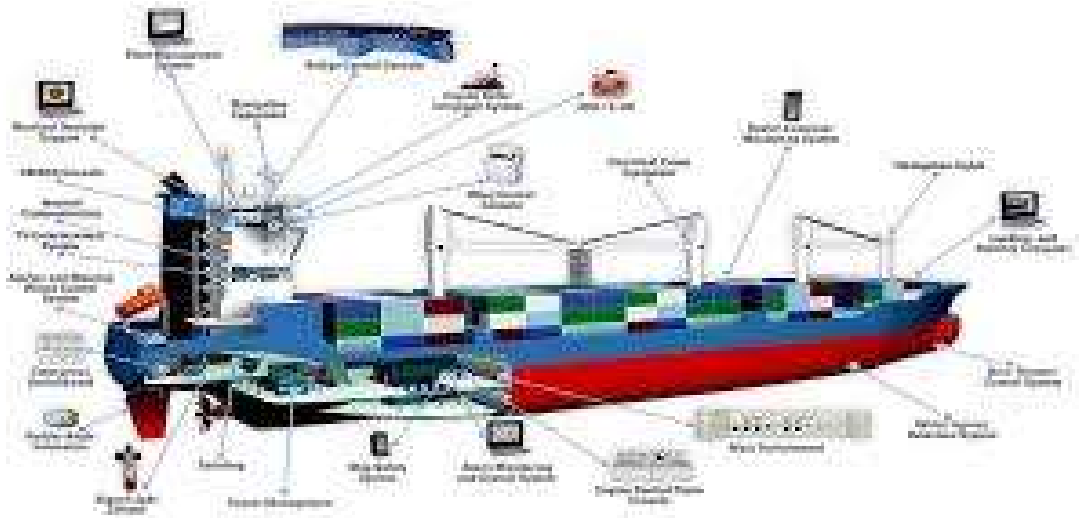
Programme Manager- E.U. Policies
DG CNECT/H1: Cybersecurity Technology & Capability Building

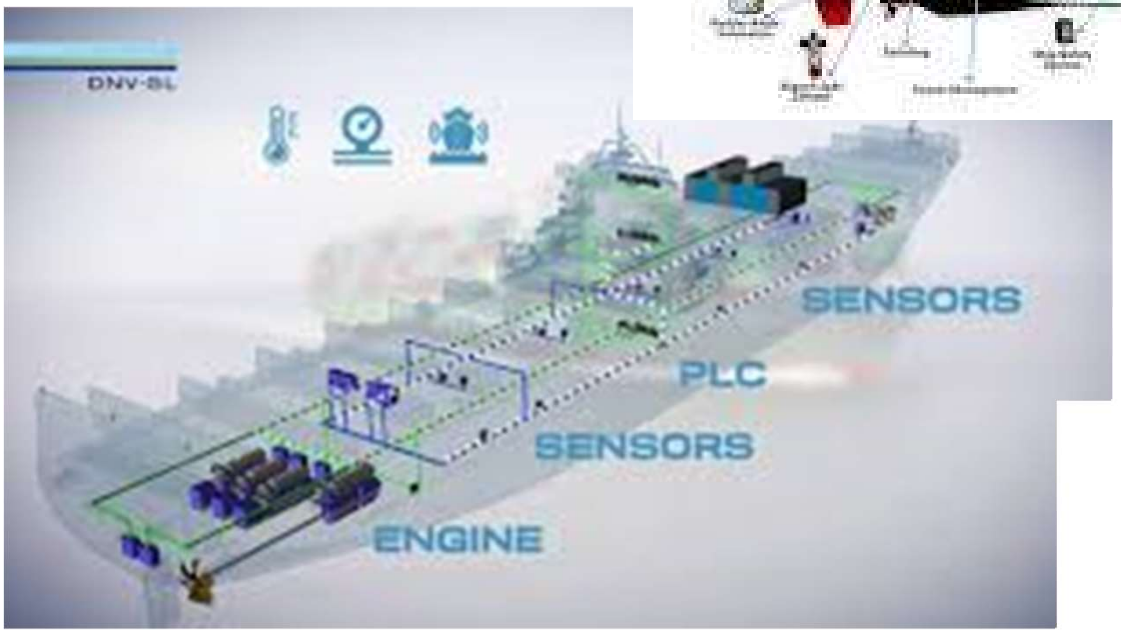
Ports' complex ICT



European Commission

Digitalization in shipping





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

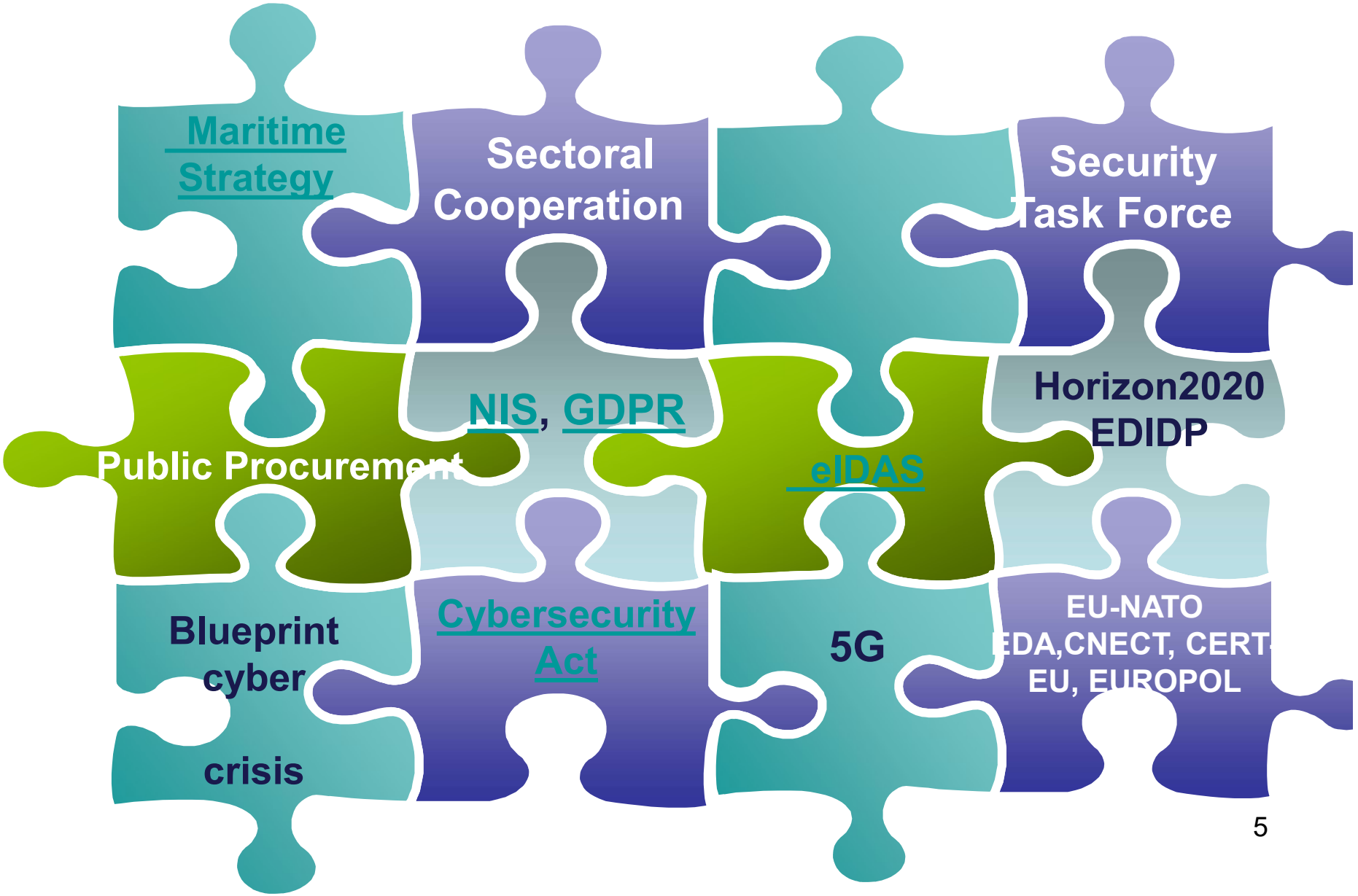
Common maritime attacks

- ✓ 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,…….

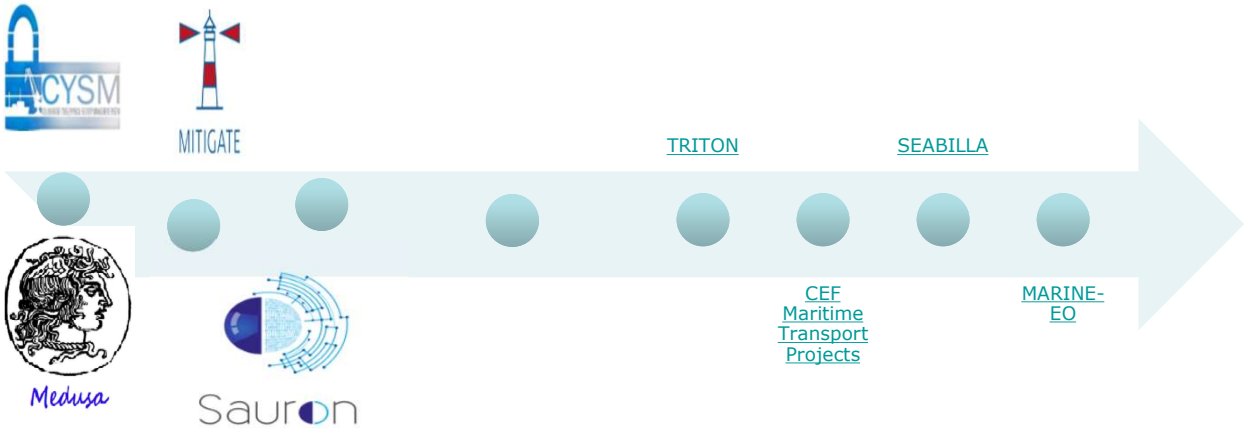
2018 attacks: Maersk, Port of Barcelona
US Ports (Long Beach, San Diego),
Austal, Royal Navy of Oman

European Commission

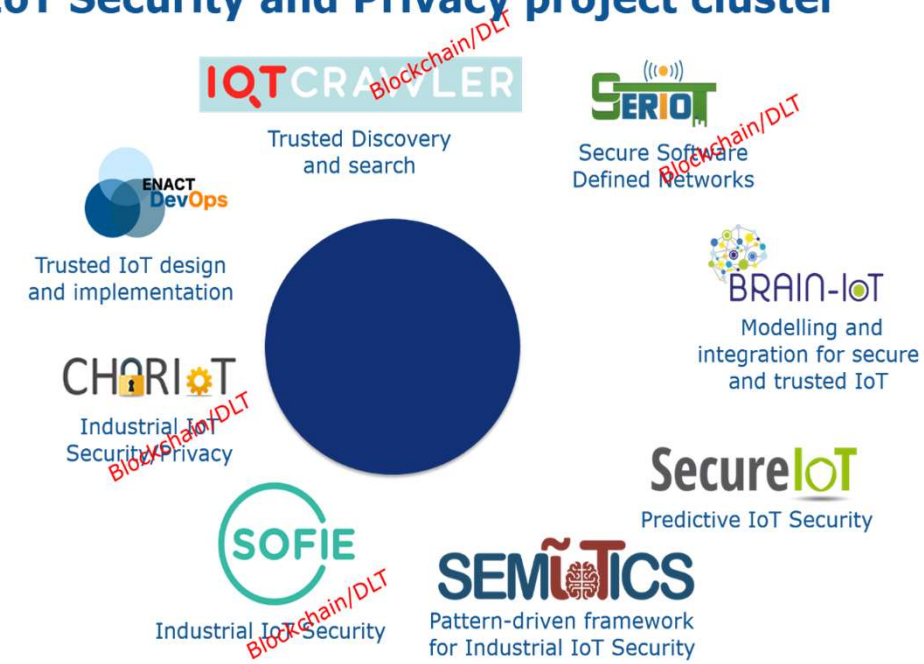
E.U. in Action


Maritime Strategy
Sectoral Cooperation
Security Task Force
Horizon2020
EDIDP
NIS, GDPR
Public Procurement
eIDAS
Blueprint cyber
crisis
Cybersecurity Act
5G
EU-NATO
EDA,CNECT, CERT-EU, EUROPOL

E.U. Maritime Cyber Security R&D



IoT Security and Privacy project cluster



AI ethics Guidelines:

- Human agency and oversight
- Technical Robustness and Safety
- Privacy and data governance
- Transparency
- Diversity, non-discrimination and fairness
- Societal & environmental well-being
- Accountability

Source: https://ec.Europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

European Commission

Co

enisa

THE EU CYBERSECURITY AGENCY

ENISA THREAT LANDSCAPE FOR 5G NETWORKS

Threat assessment for the fifth generation of mobile telecommunications networks (5G)

October 2019

EU coordinated risk assessment of the cybersecurity of 5G networks

Report

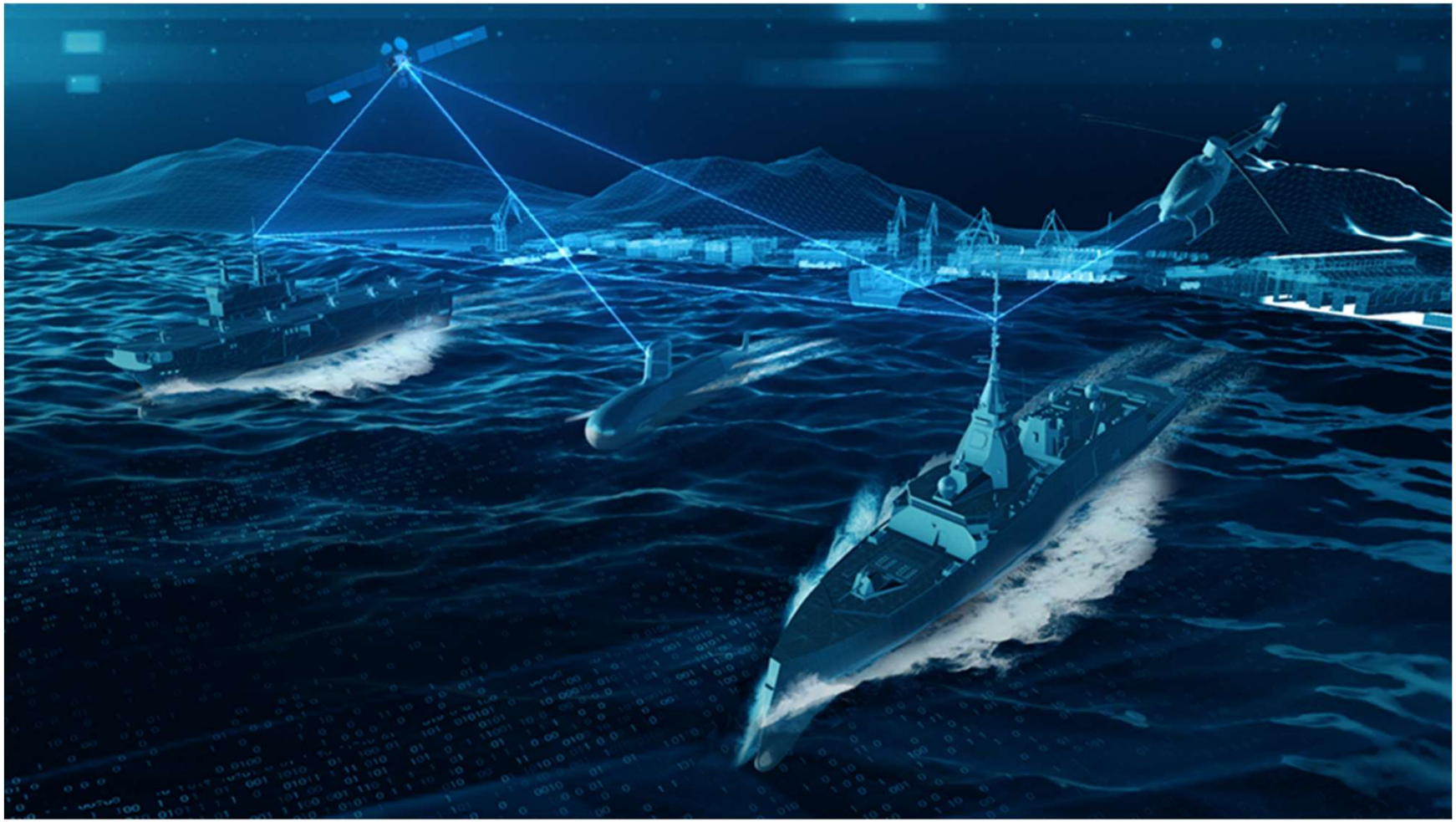
9 October 2019

NIS COOPERATION GROUP

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)

THE FUTURE



European Commission

"Third Generation" of IoT Systems

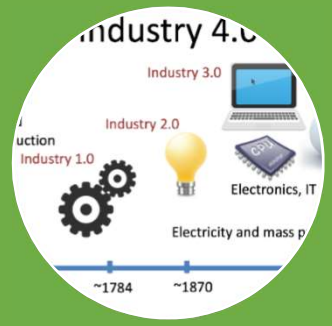
- From Distributed Sensing & Massive IoT/Cloud Systems to Smart Objects with (Semi)Autonomous Behavior
- From Passive Data Analytics to Field Actuation and Cyber-Physical Systems (CPS)

IoT Platforms Interoperability (incl. Security Interoperability)

- Cross-Platform Interoperability Scenarios (e.g., Supply Chain Management)

Alignment to On-Going Evolution and Regulatory Compliance

- Artificial Intelligence, Distributed Ledger Technologies (DLT)
- GDPR into force as of May 2018
- Cybersecurity Act into force as of June 2019



Foundation for Dynamic Massively Scalable & Autonomous IoT Systems

- Supporting Industry 4.0
- Leveraging AI and Blockchain Technologies
- Secure on board and off shore services

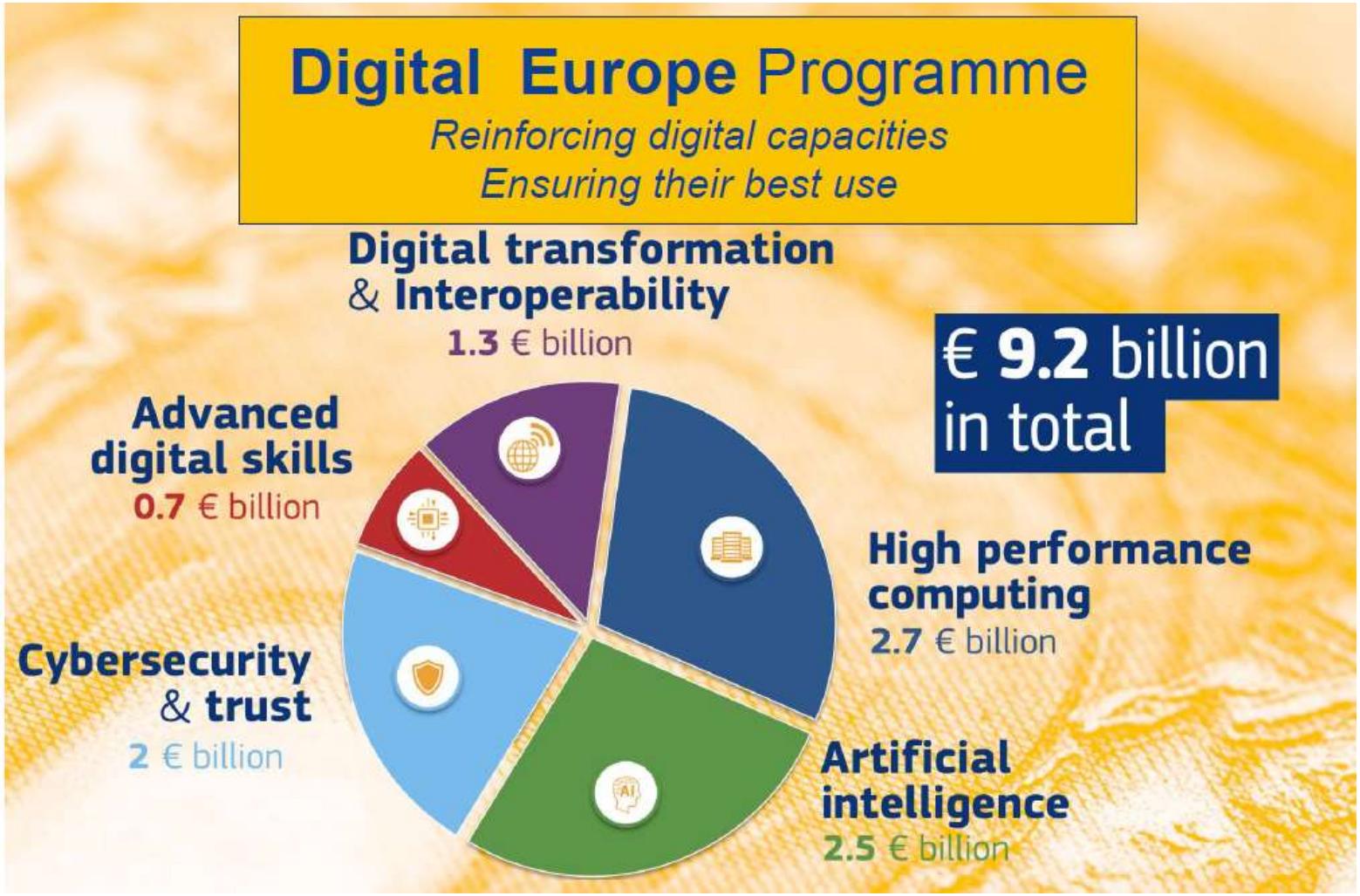
European Commission

FORTHCOMING TOPICS IN H2020

- SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems. (RIA, 47.00 MEUR 19/11/2019)
- Erasmus ++ Blue Print-Cybersecurity (26/2/19)
- SU-DS02-2020: Intelligent security and privacy management. (RIA/IA, 38.00 MEUR 27/08/2020)
- SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises. (IA, 10.80 MEUR 27/08/2020)

- ICT-56-2020: Next Generation Internet of Things (RIA, CSA 46.50 MEUR 16/01/2020)
- SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe. (IA, 20.70 MEUR 27/08/2020)
- SU-AI-2020: Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe (IA, CSA 20.00 MEUR 27/08/2020)
- SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches. (IA, 20.00 MEUR 27/08/2020)

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

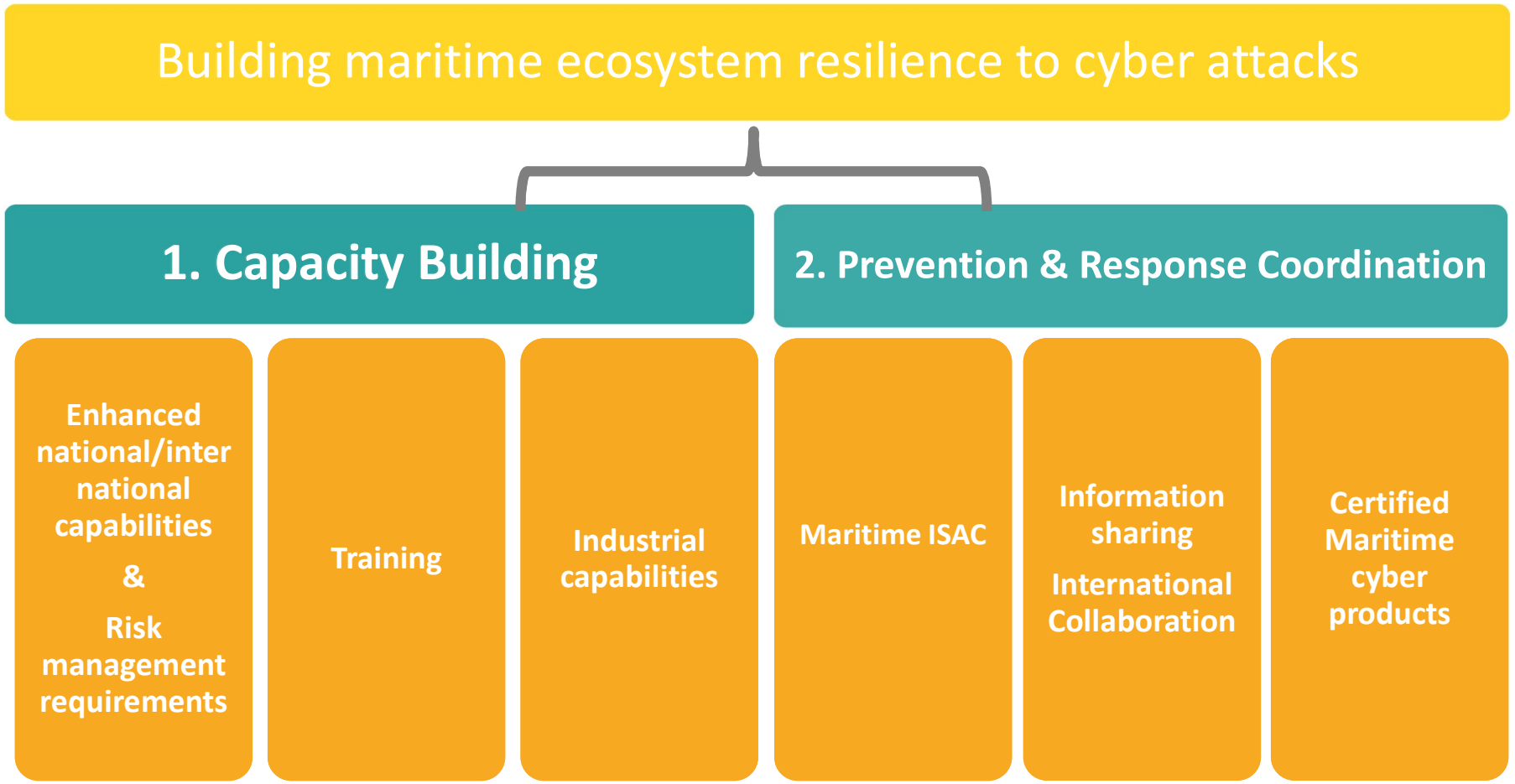
More than 160 partners from 26 EU Member States

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