

The background of the slide is a light gray gradient, decorated with numerous realistic water droplets of various sizes. Some droplets are large and prominent, while others are small and subtle. They are scattered across the slide, with a higher concentration in the top and bottom areas, framing the central text.

# PORT OPERATIONS, LOGISTIC AND SUPPLY CHAIN SECURITY TOWARDS NEW TRADE TRENDS AND TECHNOLOGY DISRUPTIONS

THE NEW MARITIME SILK ROAD:

NAVIGATION AND SECURITY IN THE TECHNOLOGICAL ERA

UNIVERSITY OF MACERATA, 21 MAY 2021

PROF. FEDERICO FRANCHINA



# MARITIME SECURITY

- THE TRADITIONAL DEFINITION
- TWO ESSENTIAL FACTORS:
  - SYSTEM VULNERABILITY
  - CONSEQUENCES OF UNLAWFUL ACT
- OUTCOMES OVER SUPPLY CHAIN:
  - COST
  - TIME
  - SAFETY
  - RISK

S



# • THE DRIVING FORCES OF MARITIME SECURITY



- FREQUENCY AND VARIETY OF UNLAWFUL ACTS  
S
- SPATIAL DIMENSION
- CHANGES OF WORLD ECONOMY AND INTERNATIONAL TRADE

# MARITIME SECURITY AT INTERNATIONAL LEVEL

---

## The Consequences of 9/11

---

## The SOLAS Convention

---

## The ISPS Code

# THE ISPS CODE

## OBJECTIVES

- 1- TO ESTABLISH AN INTERNATIONAL FRAMEWORK, INVOLVING CO-OPERATION BETWEEN CONTRACTING GOVERNMENTS, GOVERNMENT AGENCIES, LOCAL ADMINISTRATIONS AND THE SHIPPING AND PORT INDUSTRIES TO DETECT AND ASSESS SECURITY THREATS AND TAKE PREVENTIVE MEASURES AGAINST SECURITY INCIDENTS AFFECTING SHIPS OR PORT FACILITIES USED IN INTERNATIONAL TRADE;
- 2- TO ESTABLISH THE RESPECTIVE ROLES AND RESPONSIBILITIES OF ALL THESE PARTIES CONCERNED, AT THE NATIONAL AND INTERNATIONAL LEVEL, FOR ENSURING MARITIME SECURITY;
- 3- TO ENSURE THE EARLY AND EFFICIENT COLLATION AND EXCHANGE OF SECURITY RELATED INFORMATION;
- 4- TO PROVIDE A METHODOLOGY FOR SECURITY ASSESSMENT SO AS TO HAVE IN PLACE PLANS AND PROCEDURES TO REACT TO CHANGING SECURITY LEVELS;
- 5- TO ENSURE CONFIDENCE THAT ADEQUATE AND PROPORTIONATE MARITIME SECURITY MEASURES ARE IN PLACE.

# THE STRUCTURE OF THE ISPS CODE

- PART A:

1- THE OBLIGATIONS OF THE COMPANY, SHIP, PORT FACILITY AND OF THE CONTRACTING GOVERNMENT,

2- THE NECESSARY REQUIREMENTS WHICH RISK ASSESSMENTS AND SECURITY PLANS MUST HAVE,

3- THE WAY THAT THE RECORDS MUST BE PROVIDED AND BE KEPT,

4- THE INFORMATION ABOUT TRAINING AND EXERCISING OF THE CREW AND STAFF

5- THE REQUIREMENTS ABOUT THE CERTIFICATION AND VERIFICATION FOR SHIPS

- PART B

# ISPS CODE AND RISK ASSESSMENT

Ship Security Assessment

Port Facility Security Assessment

Ship Security Plan

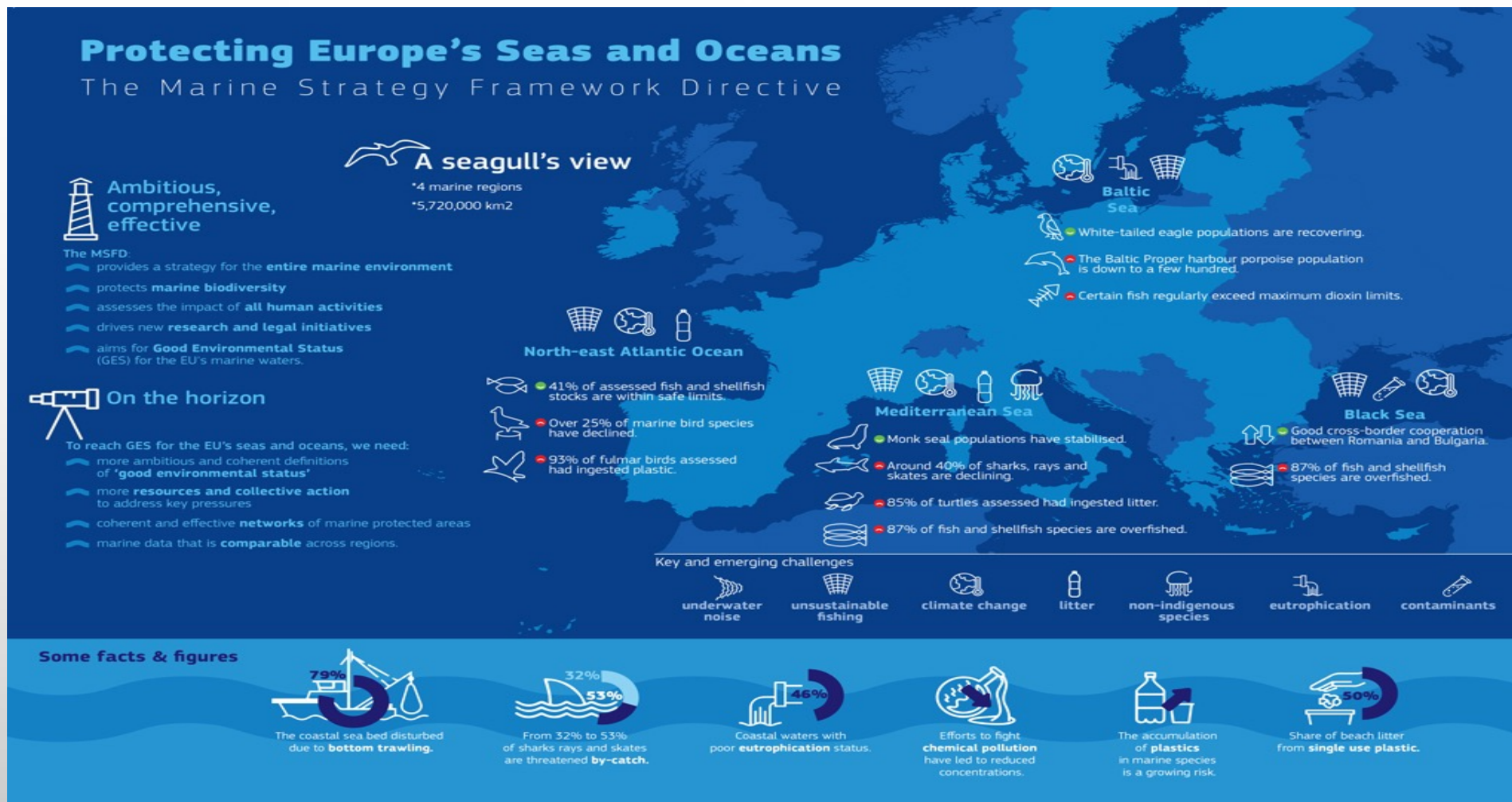
Port Facility Security Plan

# ISPS CODE AND PORT SECURITY

- PORT FACILITY SECURITY ASSESSMENT:
  - RISK ANALYSIS OF ALL ASPECTS OF A PORT FACILITY'S OPERATION IN ORDER TO DETERMINE WHICH PARTS OF IT ARE MORE SUSCEPTIBLE TO BE THE SUBJECT OF ATTACK
- PORT FACILITY SECURITY PLAN
  - PLAN TO ENSURE THE APPLICATION OF MEASURES DESIGNED TO PROTECT THE PORT FACILITY AND SHIPS, PERSONS, CARGO, CARGO TRANSPORT UNITS AND SHIP'S STORES WITHIN THE PORT FACILITY FROM THE RISKS OF A SECURITY INCIDENT
- PORT FACILITY SECURITY OFFICER



# THE EU MARITIME SECURITY STRATEGY



# PRINCIPLES OF EU MARITIME SECURITY STRATEGY

- THE FOUR PRINCIPLES:
  - A CROSS-SECTORAL APPROACH (INCLUDING CIVIL-CIVIL, CIVIL-MILITARY AND MILITARY-MILITARY COOPERATION);
  - FUNCTIONAL INTEGRITY;
  - RESPECT FOR RULES AND PRINCIPLES (INCLUDING THE RULES AND PRINCIPLES SET OUT IN INTERNATIONAL LAW AND THE UNITED NATIONS CONVENTION ON THE LAW OF THE SEA (UNCLOS));
  - MARITIME MULTILATERALISM (INCLUDING THE EU'S DECISION-MAKING AUTONOMY).



# THE IMPLEMENTATION OF EU MARITIME SECURITY STRATEGY

- AIMS

- (i) FIT FOR CURRENT AND FUTURE CHALLENGES;
- (ii) IN LINE WITH EVOLVING POLITICAL PRIORITIES;
- (iii) (III) CONSISTENT WITH ONGOING WORK AND LEGISLATION IN THE AREA OF SECURITY AND DEFENCE

- ACTIONS

- i) THE EU GLOBAL STRATEGY;
- ii) THE RENEWED EU INTERNAL SECURITY STRATEGY 2015-20204;
- iii) THE COUNCIL CONCLUSIONS ON GLOBAL MARITIME SECURITY;
- iv) THE JOINT COMMUNICATION ON INTERNATIONAL OCEAN GOVERNANCE

# THE EU REG. 725/2004

## Legal Framework

## Essential Provisions

- - Implementation of ISPS Code in the EU
  - Coordination and Monitoring of Security Measures at National Level
  - Security arrangements

## Economic Impact

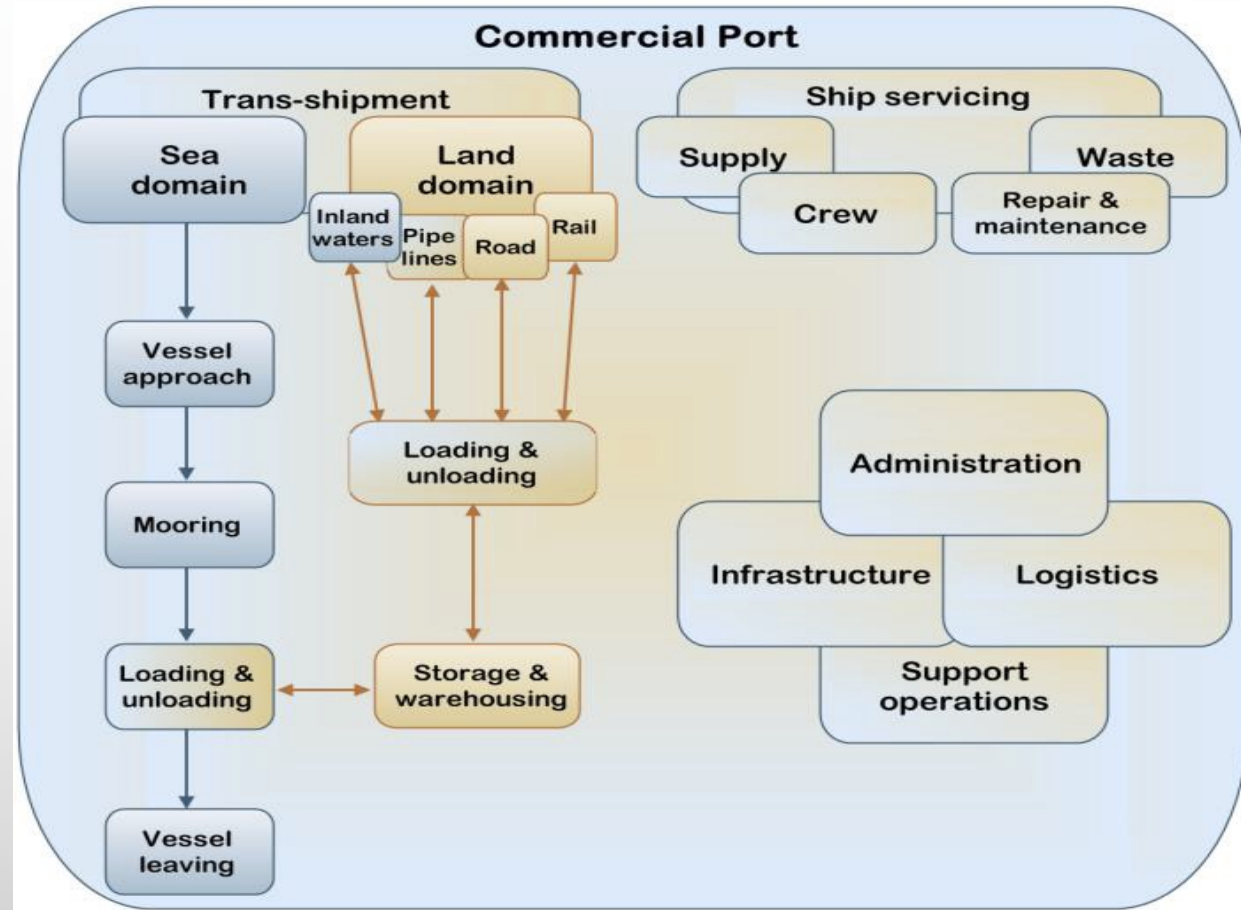
# THE EU DIRECTIVE 2005/65

- ESSENTIAL PROVISIONS:

1. DESIGNATION OF PORT SECURITY AUTHORITY
2. MANDATORY PORT SECURITY ASSESSMENT
3. PROVISION ON PORT SECURITY PLAN
4. DESIGNATION OF PORT SECURITY OFFICER

- THE DOMESTIC IMPLEMENTATION: THE LEGISLATIVE DECREE 203/2007:
  - THE RELEVAN ROLE OF THE ITALIAN PORT SYSTEM AUTHORITY

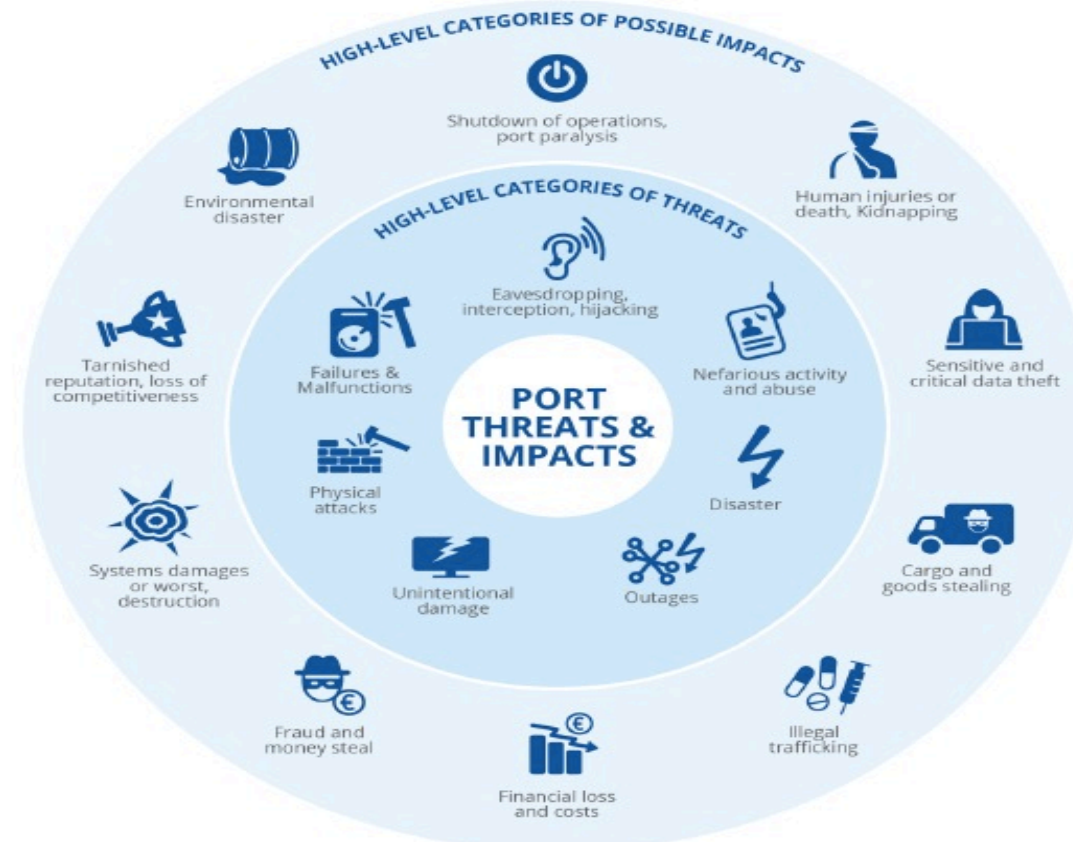
# MARITIME SECURITY AND SUPPLY CHAIN



Source: F. Andritsos

# MARITIME SECURITY AND CYBER RISK

Figure 5: High-level categories of threats and possible impacts of cybersecurity incidents







# ENISA GUIDELINES ON MARITIME CYBER RISK



---

## Objectives

---

Phase 1: Identifying cyber-related assets and services (ISPS Code Section 15.5.1: Identification and evaluation of important assets and infrastructure it is important to protect)

---

Phase 2: Identifying and evaluating cyber-related risks (ISPS Code Section 15.5.2: Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures, ISPS Code Section 15.5.4: Identification of weaknesses, including human factors in the infrastructure, policies and procedures)

---

Phase 3: Identifying security measures (ISPS Code Section 15.5.3: Identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability)

---

Phase 4: Assessing cybersecurity maturity



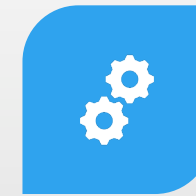
# ENISA GUIDELINES ON MARITIME CYBER RISK



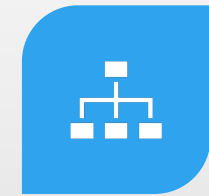
ACTIONABLE GUIDELINES TO ASSIST PORT OPERATORS IN THEIR EFFORTS TO PERFORM EACH PHASE. THESE INCLUDE SPECIFIC GUIDANCE IN HOW TO EFFECTIVELY APPLY THE VARIOUS TAXONOMIES PRESENTED IN ENISA'S PORT CYBERSECURITY REPORT OF 2019.



CHALLENGES ASSOCIATED WITH THE PERFORMANCE OF ACTIVITIES AS REPORTED BY PORT STAKEHOLDERS WHO WERE INTERVIEWED/SURVEYED FOR THIS REPORT.



GOOD PRACTICES THAT CAN BE READILY ADOPTED AND CUSTOMISED BY INDIVIDUAL ORGANISATIONS AND EASILY TAILORED AND INTEGRATED INTO ANY RISK ASSESSMENT METHODOLOGY UTILISED BY PORT OPERATORS.



A MAPPING OF THE LISTED GOOD PRACTICES FOR EACH PHASE WITH THE RESPECTIVE CHALLENGES THEY ADDRESS

# ENERGY TRANSITION AND MARITIME SECURITY

## EMSA GUIDELINES

EMSA Guidance on LNG Bunkering to Port Authorities/Administrations

European Maritime Safety Agency

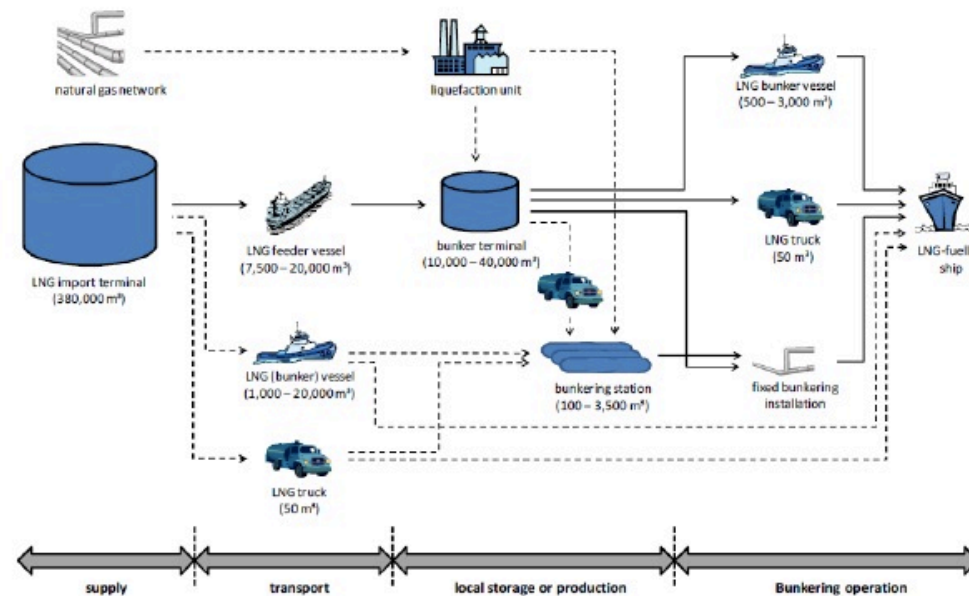
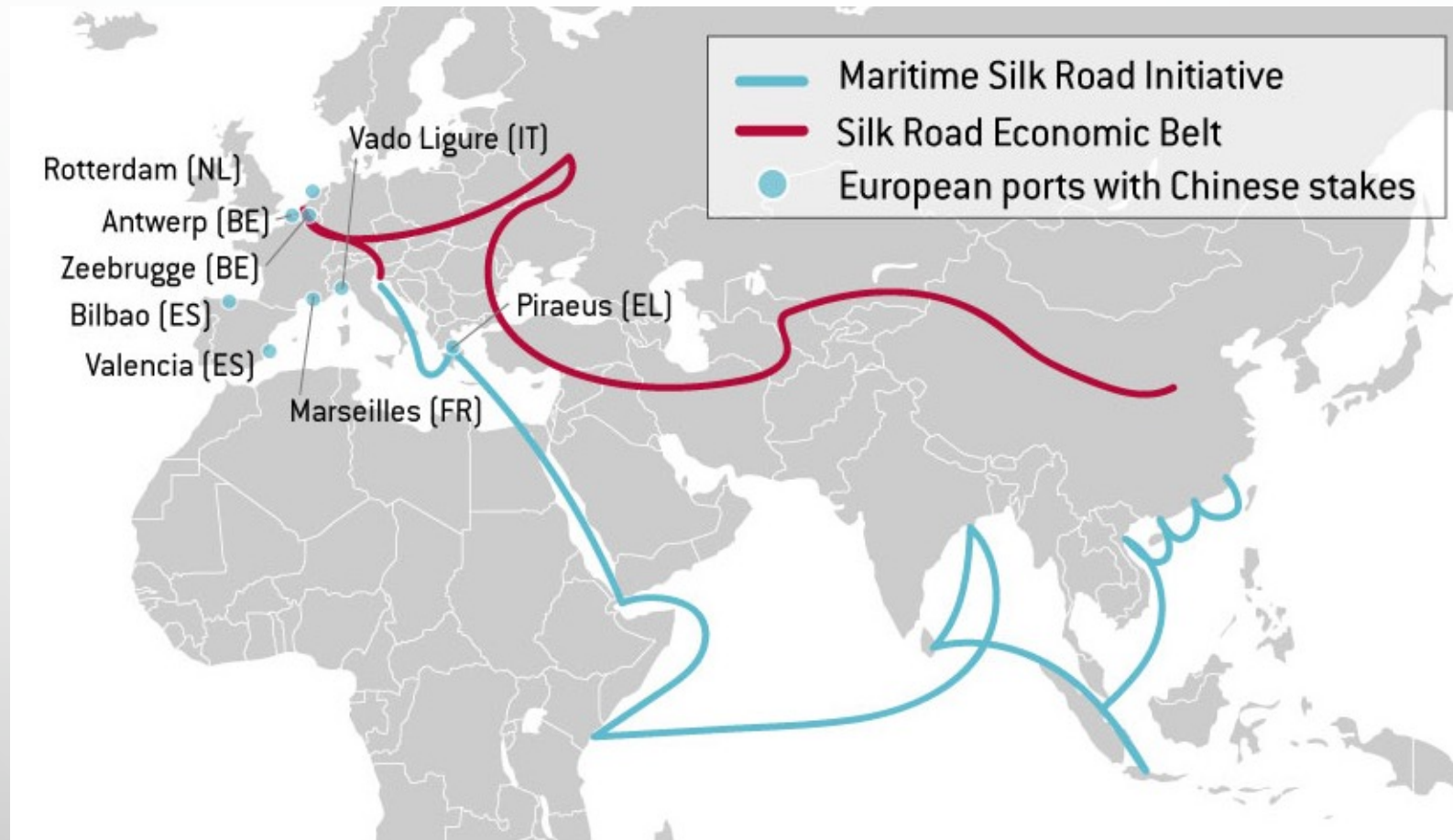


Figure 2.16 – Schematic representation of the different supply routes for the delivery of LNG as a ship fuel [21]

# FDI AND MARITIME SECURITY







## REMARKS

---

Meaning of Maritime Security evolution: from 9/11 to digital transformation

---

Different and New Threats (FDI, BRI, etc.)

---

Are the current legal tools and the Port Authority able to deal with them?