Implications of addressing the needs of cybersecurity in the conduct of the European Commission's maritime security inspections

Christian Dupont

Senior Expert / DG Mobility and Transport A5
European Commission

Cybersecurity workshop, **Lisbon 26 November 2019**

Transport

European Commission

EU MARSEC LEGISLATION APPLIES TO :

* 23 coastal States & 26 Flag States
* 8377 flagged vessels (to which Regulation 725/2004 applies)
* 4300 maritime companies
* 1087 ports (as per Directive 2005/65)
* 3688 port facilities (to which Regulation 725/2004 applies)
* 80 RSOs appointed by the MS
* More than 10.000 Non-EU flag ships calling EU ports a year

EU maritime transport security related legislation

1. Regulation (EC) n° 725/2004 maritime & port facility security

-> IMO/Solas – ISPS transposed into the EC law

-> extended to inner EU traffic

-> European inspection regime

2. Directive Port Security EC n° 65/2005

-> Based on the ILO/IMO Code of Conduct

-> Security measures extended to the whole port area

-> Monitoring system

3. Commission regulation 324/2008 as amended on inspections

4. Regulation (EC) 952/2013 Union Customs Code

Integrated management of external border (cargo)
Authorized Economic Operator

Implementation and conformity check

Article 9 of Regulation (EC) No 725/2004

*1. **Member States** shall carry out the administrative and control tasks required. They shall ensure that all necessary means are allocated and effectively for the implementation.*

*4. **The Commission** conducts inspections, including inspections of a suitable sample of port facilities and relevant companies, to monitor the application by Member States of this Regulation.*

Implementation and conformity check

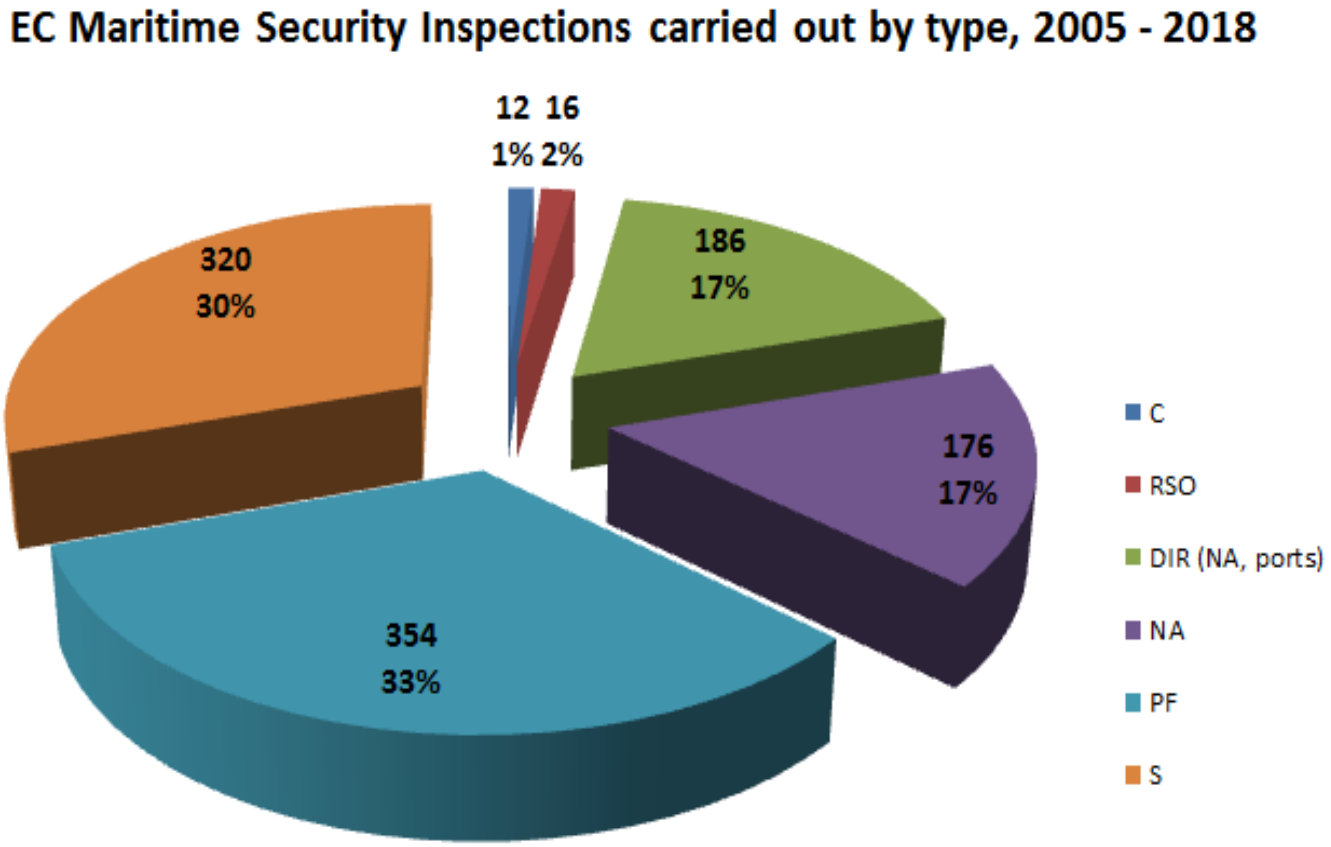
Article 13 of Directive 2005/65/EC

1. **Member States** shall set up a system ensuring adequate and regular supervision of the port security plans and their implementation.

2. **The Commission shall**, in cooperation with the focal points referred to in Article 12, **monitor the implementation of this Directive by Member States.**

3. **This monitoring shall be conducted jointly with the inspections** provided for in Article 9(4) of Regulation (EC) No 725/2004.

More than 1.000 EU COM inspections from 2005 to 2018



LEGEND
C - Companies 12

RSO - Recognised Security Organisations 16

DIR - ports, NA ports 186

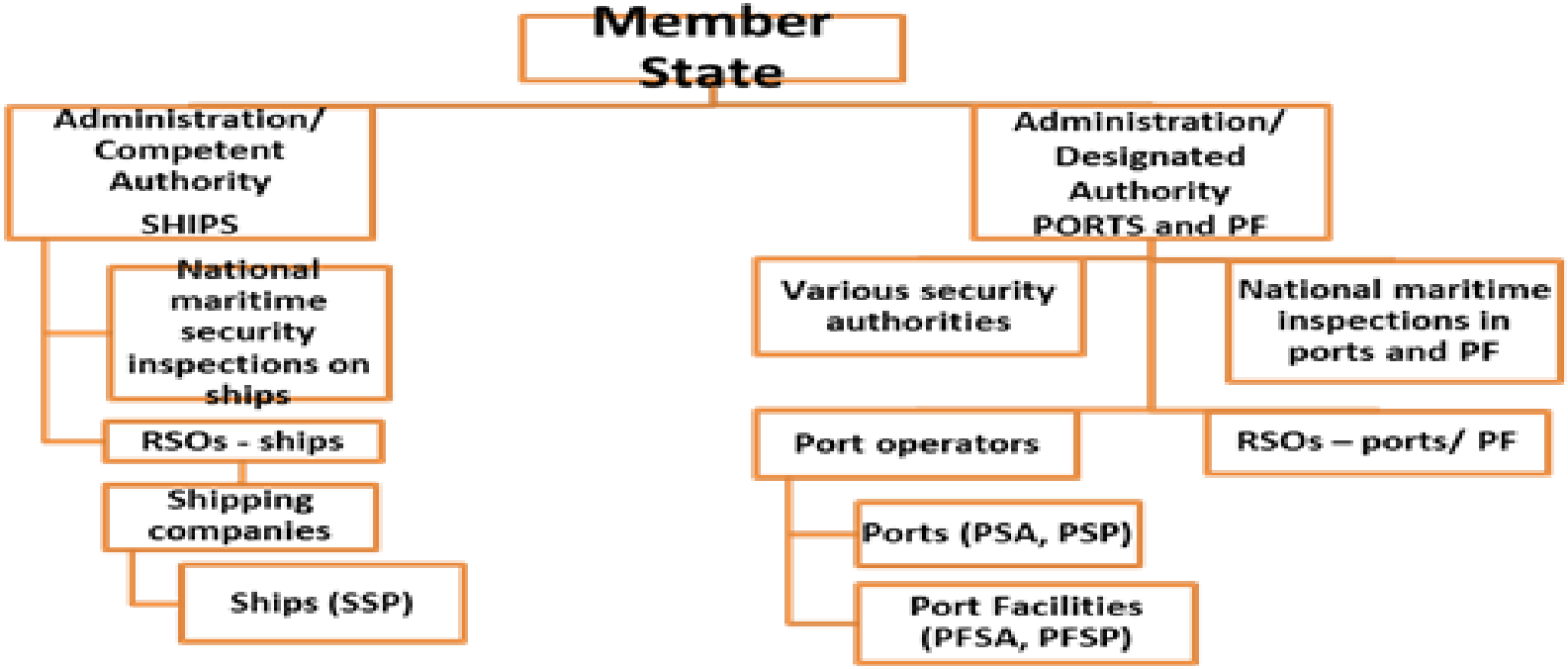
NA - National Administrations 176

PF - Port Facilities 354

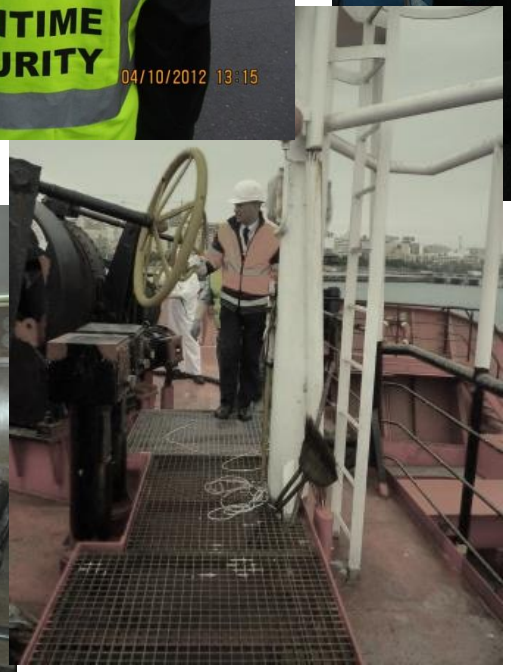
S - Ships 320

TOTAL: 1064

System-based approach of Commission inspections



There are different types of inspections



Types of COM inspections (1)

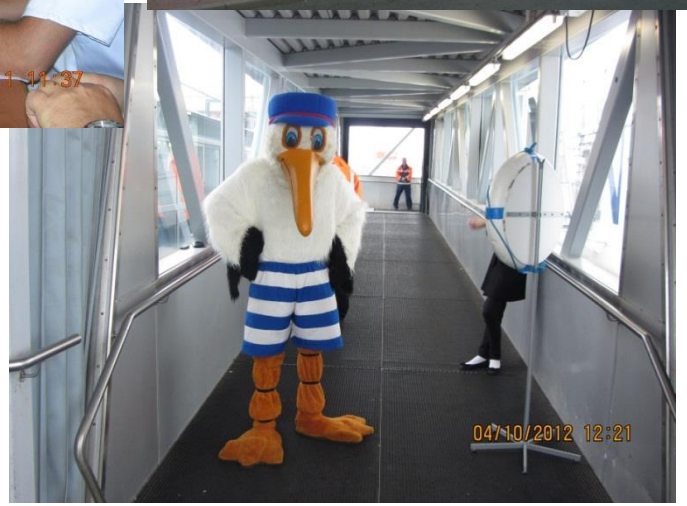
- ✓ **National Administration (N. A.)– Reg.725: general application at the national level**
- ✓ **National Administration – Dir.65: Ports at the national level**
- ➢ **Caution : "N.A." may well mean from 1 to 10 different bodies to inspect…**

To see the framework

to monitor the implementation of relevant EU **legislation by the responsible authorities of the Member States**

Types of COM inspections (2)

- ✓ **Ports**
- ✓ **Port Facilities**
- ✓ **Ships**
- ✓ **Ships with authorities**



To see how the system works

to look at **suitable sample** of ports, port facilities, ships. at **measures, procedures** and **structures**

Types of COM inspections (3)

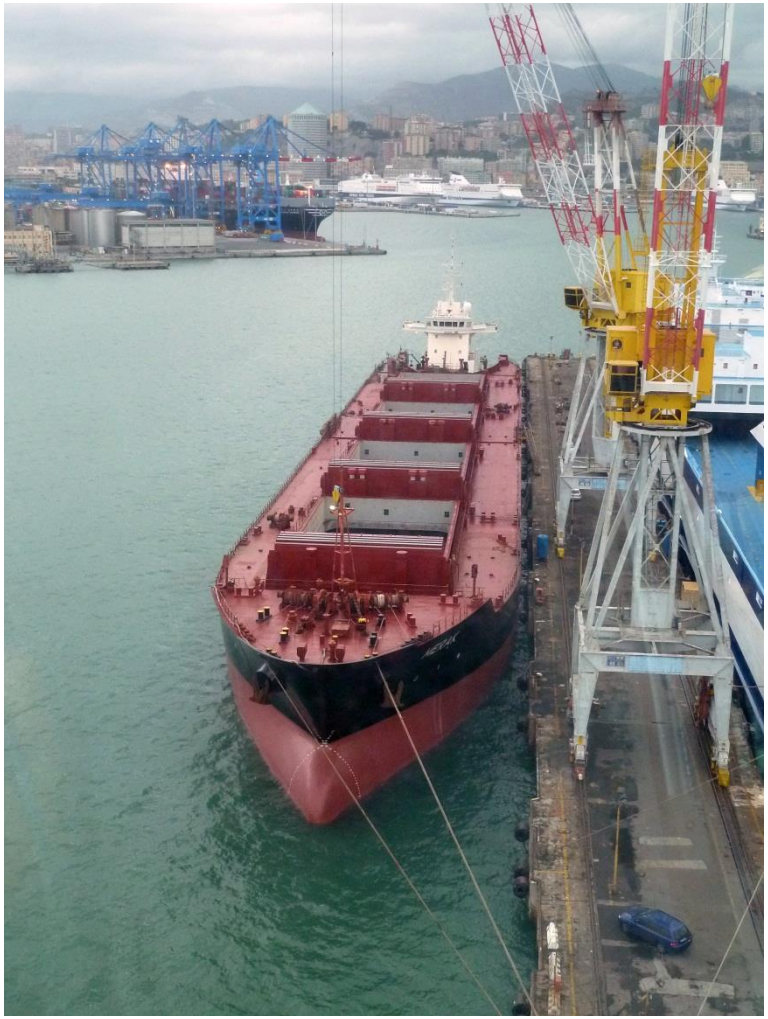
- ✓ **RSOs – ships**
- ✓ **RSOs – Port Facilities**
- ✓ **RSOs – Ports**
- ✓ **Shipping companies**

- To see how the delegation works
- How RSOs act on behalf of MS

to look at **suitable sample** of RSOs and associated companies

What does the existing EU legislation already contain without naming it expressly

“cyber security measures” ?



port facility security assessment (PFSA)(1)

- (*Refer to the forthcoming EMSA presentation*);
- ISPS A15.5 : identification of assets, threats, vulnerabilities , counter-measures
- ISPS B15.3.5 (mandatory): to address radio and telecommunication systems, including computer systems and networks;

port facility security assessment (PFSA) (2)

- ISPS B 15.7: Assets and infrastructure important to protect may include :
  - **electrical distribution systems, radio and telecommunication systems and computer systems and networks**
  - **security and surveillance equipment and systems**

port facility security Plan (PFSP) (1)

- ISPS A16.3.3: *The plan shall address procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface*
- *ISPS A 16.7: The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment*

port facility security Plan (PFSP) (2)

- ISPS A 16.8: *The plan shall be protected from unauthorised access or disclosure*
- ISPS B 16.3.2 (mandatory): *the PFSP shall detail the organisation's links with other relevant authorities and the necessary communication systems to allow the effective continuous operation of the organisation and its links with others, including ships in port;*

port facility security Plan (PFSP) (3)

- ISPS B 16.8.4 (mandatory): *the PFSP shall establish the communication systems provided to allow effective and continuous communication between port facility security personnel, ships in port and, when appropriate, with national or local authorities with security responsibilities*

port facility security Plan (PFSP) (4)

- ISPS B 16.8.7 (mandatory): *the PFSP shall establish the procedures to assess the continuing effectiveness of security measures, procedures and equipment, including identification of, and response to, equipment failure or malfunction;*

port security assessment (PSA)(1)

- Article 6.2: *Each port security assessment shall be carried out taking into account as a minimum the detailed requirements laid down in Annex I.*

port security assessment (PSA)(2)

- Annex I: *The port security assessment will cover at least:*
- *identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures;*
- *identification, selection and prioritisation of counter-measures and procedural changes and their level of effectiveness in reducing vulnerability;*

port security assessment (PSA)(3)

- The assesment will at least:
  - **identify the specific characteristics of each sub-area, such as location, accesses, power supply, communication system, ownership and users and other elements considered security-relevant**

port security assessment (PSA)(4)

- identify potential threat scenarios for the port. The entire port or specific parts of its infrastructure, cargo, baggage, people or transport equipment within the port can be a direct target of an identified threat;

port security assessment (PSA)(5)

- identify the specific consequences of a threat scenario. Consequences can impact on one or more sub-areas. Both direct and indirect consequences will be identified (…)

port security assessment (PSA)(5)

- identify communication requirements for implementation of the measures and procedures;
- pay specific attention to measures to protect security-sensitive information from disclosure;

port security plan (PSP)(1)

- Article 7.3: *Each port security plan shall take into account as a minimum the detailed requirements specified in Annex II.* (…)

port security plan (PSP)(2)

- Annex II: *The port security plan will be based on the following general aspects:*
- *(…)*
- *identifying an organisational structure supporting the enhancement of port security.*

port security plan (PSP)(3)

- communication and security clearance. All relevant security information will be properly communicated according to security clearance standards included in the plan. In view of the sensitivity of some information, communication will be based on a need-to-know basis, (…). (*This is*) aimed at protecting security sensitive information against unauthorised disclosure;

port security plan (PSP)(4)

- integration with other preventive plans or activities. The plan will specifically deal with integration with other preventive and control activities in force in the port;

port security plan (PSP)(5)

- integration with other response plans and/or inclusion of specific response measures, procedures and actions. The plan will detail interaction and coordination with other response and emergency plans. Where necessary conflicts and shortcomings will be resolved;

European Commission

How do we process on inspections?

- **In the assessments: identification of threats, vulnerabilities and counter-measures**
- **In the plans: existence and effectivity of the security measures to prevent breaches of security**

As a conclusion….

“See you soon”

European Commission

Any questions?

European Commission

Thank you for your attention

Christian Dupont
Senior Expert
Maritime Security
European Commission
DG MOVE A5