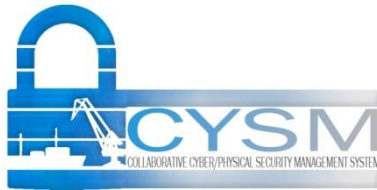


# Multi Order Dependency approaches for managing cascading effects in ports' global supply chain and their integration in risk assesment frameworks



## Approaches for assessing physical & cyber risks in ports' Supply Chain Services

**Ass. Prof. Nineta Polemi** ([dpolemi@gmail.com](mailto:dpolemi@gmail.com))

**Dr. Spyros Papastergiou** ([paps@unipi.gr](mailto:paps@unipi.gr))

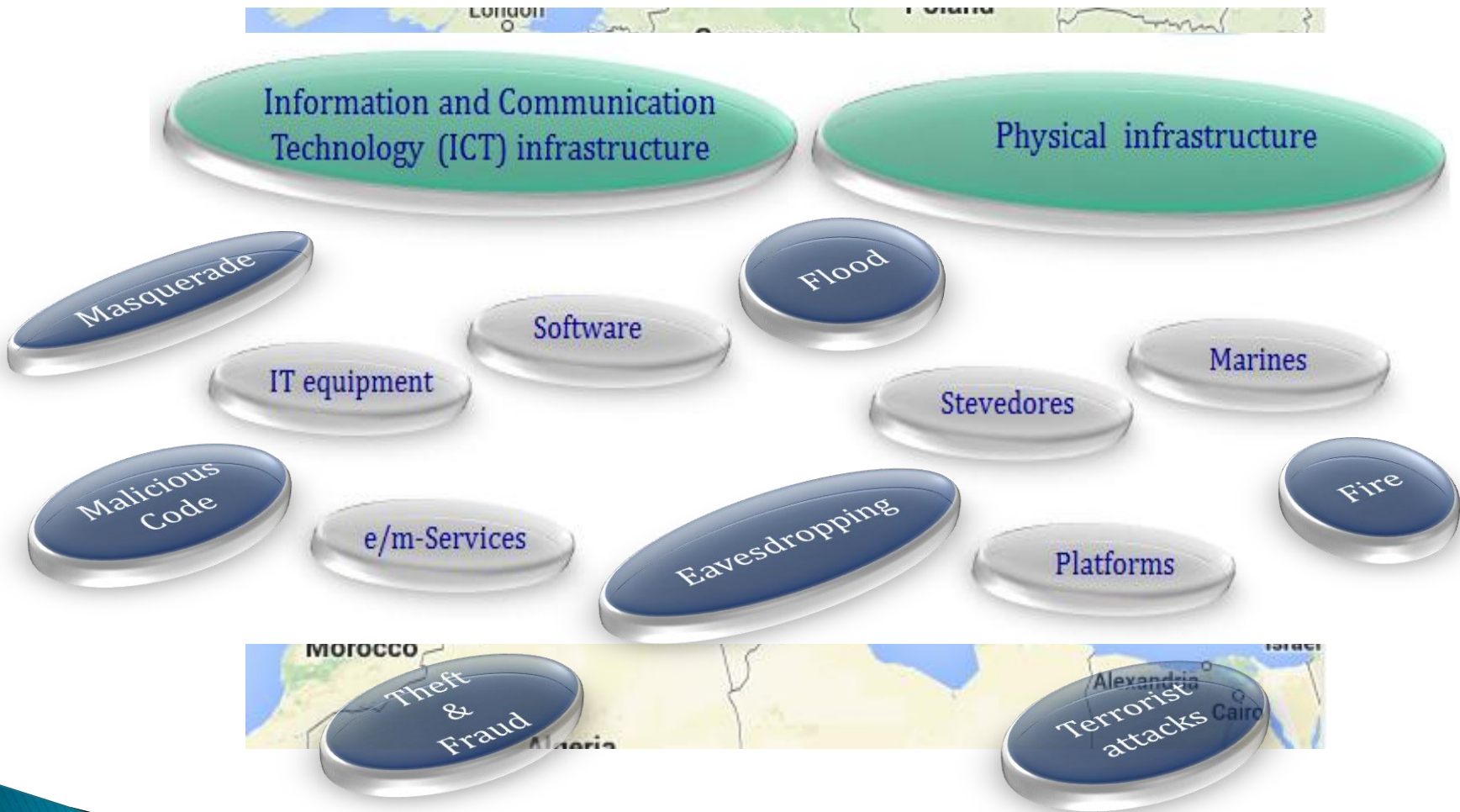
University of Piraeus (Greece)–Dept. of Informatics  
Athens– 3rd December 2015

Κυβερνο-Ασφάλεια & Ναυτιλία – Ένα σύγχρονο πρόβλημα



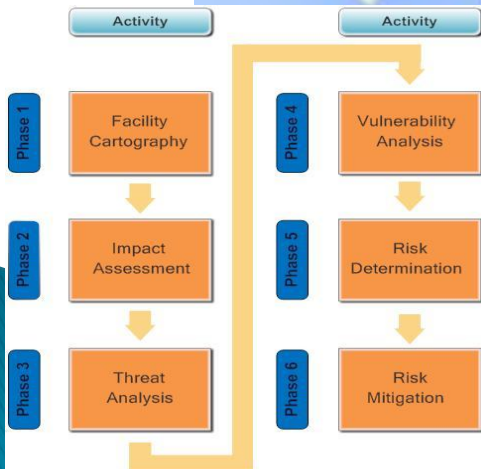
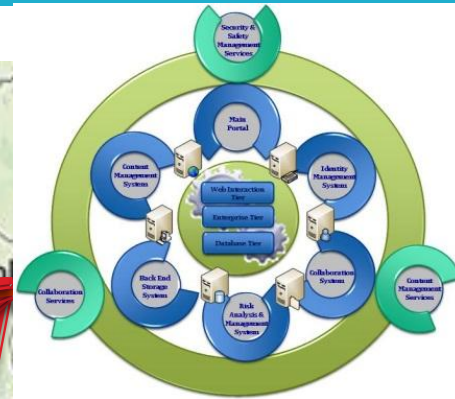
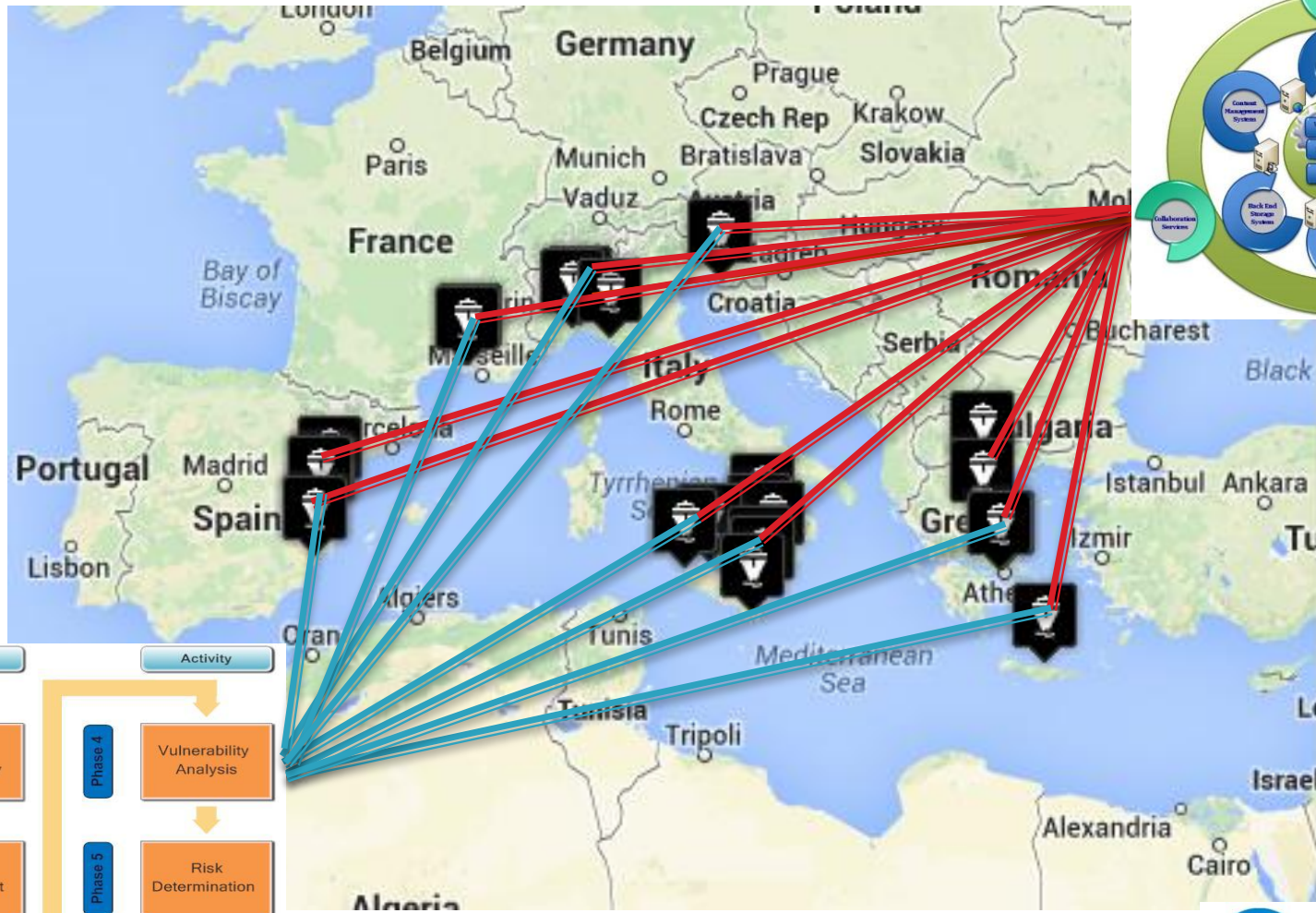


# Maritime Sector





# CYSM Outputs ([cysm.eu](http://cysm.eu))





# Cysm Security Management System

<http://cysm.cs.unipi.gr/>

The screenshot shows the CYSM website interface. At the top, there is a blue header with the CYSM logo and navigation links: Home, e-Library, and Collaboration. Below the header, there is a sidebar menu with the following items: Sites (CYSM Pilot Port, CYSM, Port of Carrara, Port of Valencia, Port of Mykonos), Asset Identification (Register Infrastructure (Physical), Register Physical (Non ICT) Assets, Register HW Assets, Register Software Assets, Register Information Data), and a Back button.

MARITIME SAFETY COMMITTEE  
95th session  
Agenda item 4

MSC 95/INF.19  
14 April 2015  
ENGLISH ONLY

## MEASURES TO ENHANCE MARITIME SECURITY

### Cyberphysical relationship in port security

#### CYSM project – "Collaborative Cyber/Physical Security Management System"

Submitted by the European Commission

#### SUMMARY

**Executive summary:** This document provides information on a project funded by the European Commission which aims to address potential gaps in security related to the cyberelements of port infrastructure

**Strategic direction:** 6.1

**High-level action:** 6.1.1

**Planned output:** 6.1.1.1

**Action to be taken:** Paragraph 9

**Related document:** MSC 94/21, paragraph 4.7

#### Reporting

Help

Vulnerability	Vul. Level	Controls
of software	5	+
ensive security	5	+
aining program	5	+
or controlling copyrights	5	+
as of sensitive files	5	+
as of files	5	+
te control of outbound	5	+
ntitlement review process	5	+
ess rights of the	5	+
organization's premises	5	+
entication	5	+
ty training	5	+
Lack of application safeguards leading to	5	+
fraudulent payments being made	5	+
Inadequate monitoring of the organization	5	+
premises	5	+

Telecommunication Room	Theft and Fraud	3	Lack of application safeguards leading to	5	+
Telecommunication Room	Theft and Fraud	3	fraudulent payments being made	5	+
			Inadequate monitoring of the organization	5	+
			premises	5	+



# CYSM Consortium



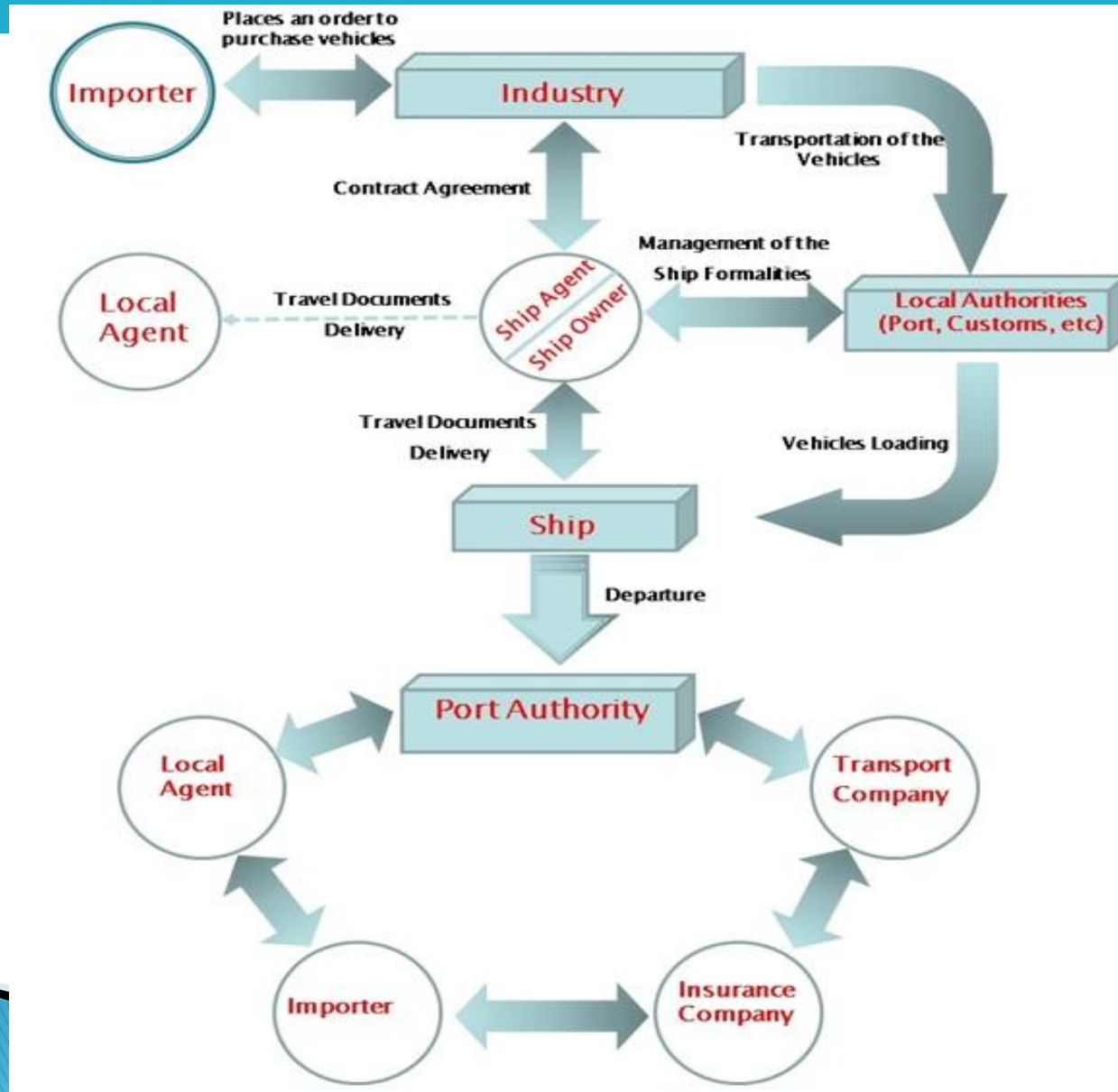


# Commercial Ports





# Port's Supply Chain Services



Medusa

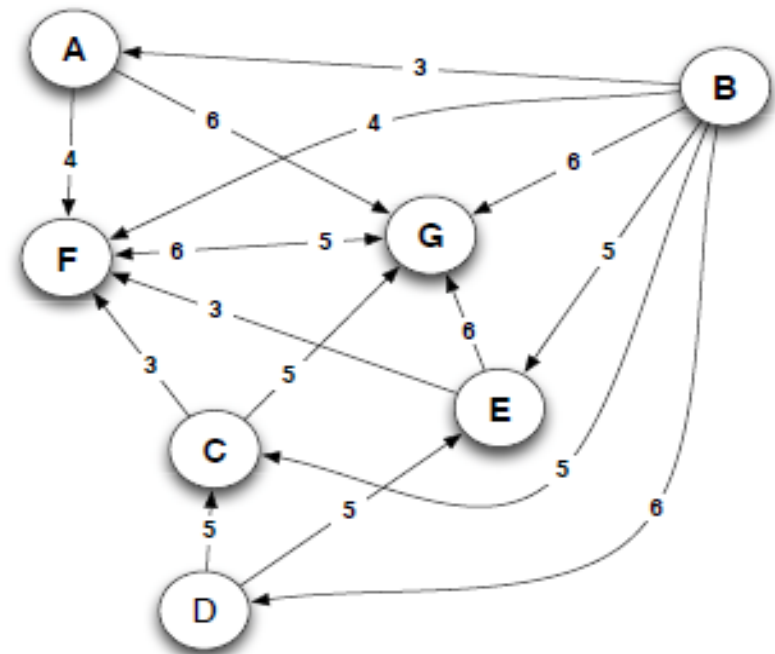


# Identifying dependencies:

## Dependency graphs

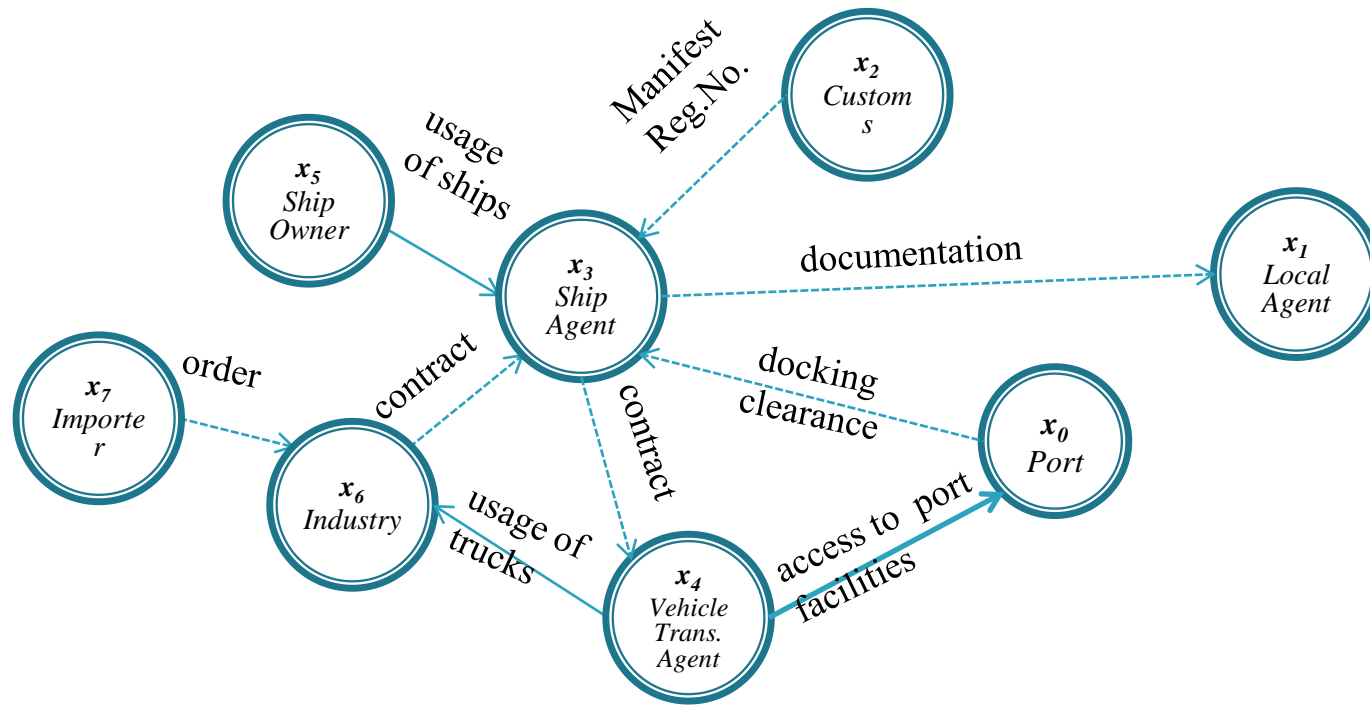
Dependent	Dep. Type	Description	SImp	IImp	IImp Type	Scale $I_{j,s}$	LH $L_{j,s}$	Risk $R_{j,s}$
<b>CI<sub>A</sub> (Finance Sector)</b>								
CI <sub>F</sub>	C	Provides payment services	UA	UA	Public Confidence	L	L	4
CI <sub>G</sub>	C	Provides payment Services	UA	UA	Public Confidence	H	L	6
<b>CI<sub>B</sub> (Energy Sector)</b>								
CI <sub>A</sub>	P	Depends for power	UA	UA	Economic Impact	VL	L	3
CI <sub>C</sub>	P	Depends for power	UA	UA	Public Confidence	H	VL	5
CI <sub>D</sub>	P	Depends for power	UA	UA	Economic Impact	VH	VL	6
CI <sub>E</sub>	P	Depends for power	UA	UA	Economic Impact	H	VL	5
CI <sub>F</sub>	P	Depends for power	UA	UA	Public Confidence	L	L	4
CI <sub>G</sub>	P	Depends for power	UA	UA	Public Confidence	H	L	6
<b>CI<sub>G</sub> (Government Sector)</b>								
CI <sub>F</sub>	S	Industrial action	UA	UA	Economic Impact	M	M	6

Dependency. P: Physical, C: Cyber, G: Geographic, Log: Logical, S: Social  
Source/Incoming Impact (SImp/IImp). UA: Unavailability, DS: Disclosure, MD: Modification  
Scale/Likelihood. VH: Very High, H: High, M: Medium, L: Low, VL: Very Low





# Vehicle Transport Service



---> (1) Access to Cyber systems

-----> (2) Interaction with Cyber systems

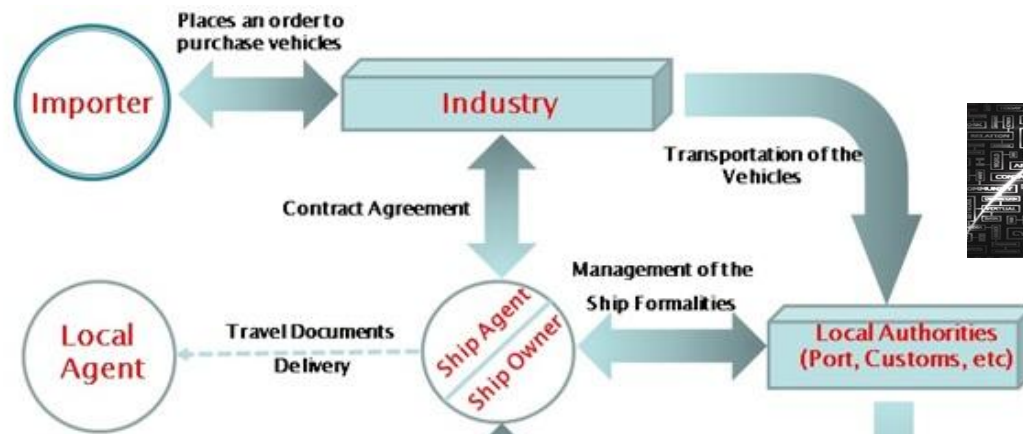
—> (3) Access to Physical facilities

—> (4) Usage of physical facilities/goods

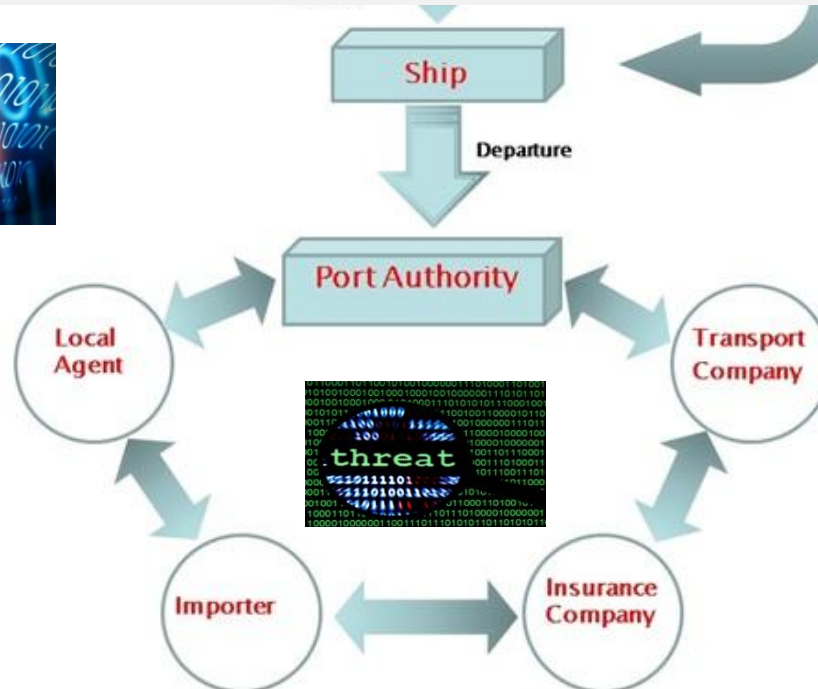




# Risks of Port's Supply Chain Services



**QUESTION:** How can we estimate risks of a supply chain ???



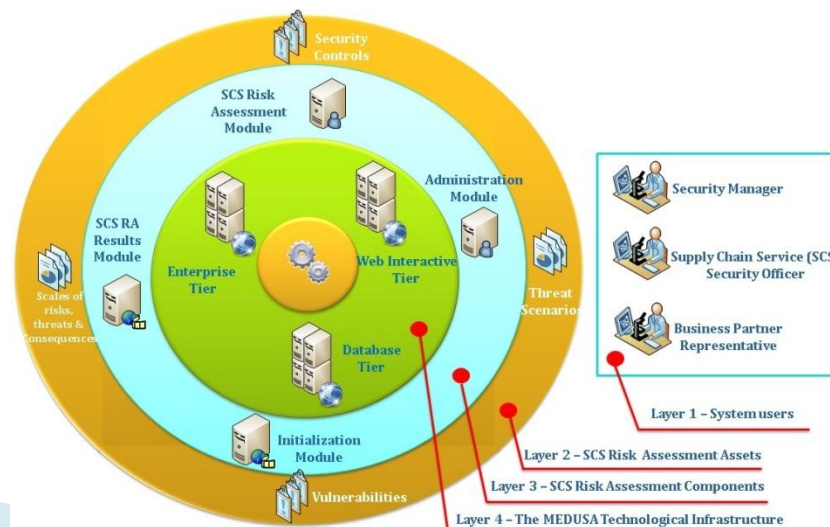


# Medusa Objectives ([medusa.cs.unipi.gr](http://medusa.cs.unipi.gr))

**Obj. 1:** techniques for capturing multi-order dependencies between port infrastructures and other CIs comprising the global supply chain

**Obj. 2:** algorithms for identifying and assessing the critical path of the inter-dependencies across the global supply chain

**Obj. 3:** approach for identifying and analyzing the cascading effects of security incidents on port infrastructures, given their various dependencies.





# Medusa Consortium





# MEDUSA Risk Assessment System

<http://medusascsra.cs.unipi.gr>

**Threat Assessment** **Control in Place** **Consequence Assessment** 3 Finish Calculate

LNG SCS RA

Search

#

1

2

3

4

5

Results

Statistics

Cascading Dependency Risk

Search

Export Table Data

Code	Description	Over. Risk	R. Threshold
TS1.1	Destroy a major / critical SC Infrastructure	High	High
TS4.2	Use the supply chain as a means of smuggling.	Medium	Medium
TS1.2	Suspected or confirmed unauthorized access to SC Infrastructures	Low	Medium
TS4.1	Intrude and/or take control of an asset (including conveyances) within the supply chain.	Low	Low
TS2.1	Information tampering	Low	Medium
TS3.2	Misuse / abuse of SC procedures	Low	Medium
TS3.1	People under attack	Low	Medium
TS2.2	Information loss	Low	High
TS2.3	Communication interruption or loss	Low	Low
TS2.4	Software/system abuse	Low	High





# MITIGATE Objectives ([mitigateproject.eu](http://mitigateproject.eu))

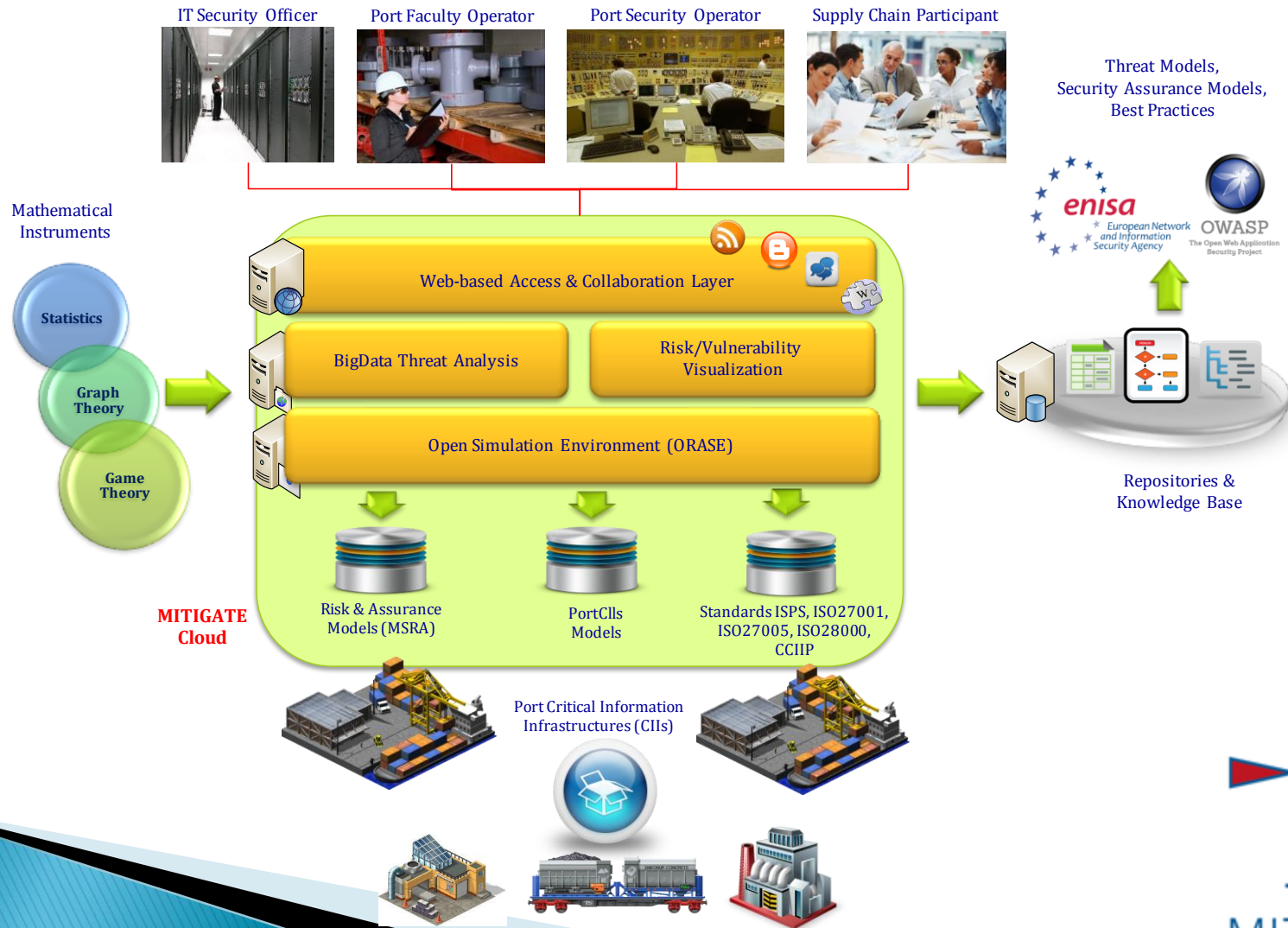
Goal of MITIGATE is to realize a **radical shift** in risk management methodologies for the maritime sector towards a **dynamic evidence-driven Maritime Supply Chain Risk Assessment (g-MSRA)** approach that alleviates the limitations of state-of-the-art risk management frameworks.

The project will develop an effective, collaborative, standards-based **Risk Management (RM) system** for port's CIIs, which shall consider all threats arising from the **global supply chain**, including threats associated with portCIIs **interdependencies** and associated **cascading effects**.





# Mitigate: Maritime SC Dynamic Risk Assessment





# MITIGATE Consortium



Instituto Portuario de Estudios y Cooperación  
de la Comunitat Valenciana





# Multi Order Dependency approaches for managing cascading effects in ports' global supply chain and their integration in risk assesment frameworks

Medusa Website  
[medusas.cs.unipi.gr](http://medusas.cs.unipi.gr)



Medusa system  
[medusascra.cs.unipi.gr](http://medusascra.cs.unipi.gr)

MITIGATE Website  
[www.mitigateproject.eu](http://www.mitigateproject.eu)



CYSM Website  
[cysm.eu](http://cysm.eu)



CYSM system  
[cysm.cs.unipi.gr](http://cysm.cs.unipi.gr)

## Thank You

