Challenges in Maritime and Supply Chains' Security

MITIGATE

1st NMIOTC CYBER SECURITY CONFERENCE

Associate Professor N. Polemi, Director of UNIPI Security Lab

…the evolution (2009-2018)….

- **S-Port (**national project**)** and E.C. project **CYSM**: Static Ports' RM methodology and tool (ISO27001, 27005, ISPS, CIIP)
- E.C. project **MEDUSA**: Static SC RM' methodology and tool (ISPS, CIIP, ISO28000)
- E.C. project **MITIGATE**: Dynamic evidence-driven Maritime SC RM environment (simulation, crowd-sourcing, open data) (ISO27001, 27005, ISPS, CIIP, ISO28000)
- E.C. project **FASTPASS** on Automated Board Control systems

The Policy / Legislation Challenge

MITIGATE

- **IMO: MARPOL** for the *sea protection;* **SOLAS** for the *safety* of the ships, passengers and cargo and the **ISPS** (formulated in 2004) address the organisational aspect of security.
- WCO SAFE Framework of standards (2015) to Secure and Facilitate Global Trade
- **USA**, 2016 House of Representatives H.R. 3878, "Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2015"

- CIIP Directive (2012) Critical information infrastructure protection: towards global cyber-security
- The Cybersecurity Strategy for the European Union (2013) and the European Agenda on Security (2015) provide the overall strategic framework for the EU initiatives on cybersecurity and cybercrime.
- eIDAS Regulation (2014) on electronic identification and trust services for electronic transactions in the internal market
- European Parliament 2015 concerning measures to ensure a high common level of network and information security across the Union
- NIS Directive 2016 applies only to those public administrations which are identified as operators of essential services
- cPPP Initiative 2015 ensures that Europe will have a dynamic, efficient and effective market in cybersecurity products and services.
- Enhanced Privacy Directive, 2016 Mandatory reporting of security breaches

PLETHORA OF STANDARDS

MITIGATE

- ISO/IEC 27001:2005 / ISO/IEC 27001:2013 (building a SM system)
- ISO/IEC 27005:2011 guidelines for information security risk management
- NIST SP 800-128, 2011 Guide for Security-Focused Configuration Management of Information Systems
- ISO 31000:2009 - Principles and Guidelines on Implementation
- ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques
- ISO/IEC 27002:2005 (best practice recommendations)
- AS/NZS 4360:2004 (Australian/New Zeland standard for RM)

The above standards are supported by a variety of methodologies (see ENISA repository)

- ISO 28000:2007 ISO 28001:2007, ISO 28003:2007, ISO 28004:2007 for supply chain security

- IMO 2016 cyber security guidelines for maritime companies and ships

THE SECURITY AWARENESS CHALLENGE

MITIGATE

- We have enough security standards/policies/regulations, we need targeted Market-driven **"easy to use" risk assessment tools** for maritime operators assessing and mitigating their physical/cyber risks. **Insurance companies** and auditors may require risk assessment and mitigation of cyber risks in their insurance policies.
- **Collaboration** among maritime and security regulators standardization bodies and associations (IMO, NATO, EMSA, IPCA, EPCSA, ENISA, DGMARE, DGMOVE, DGCONNECT etc.)
- **Enhanced academic programs** in the maritime academies and universities
- **Open IMO/NATO/EMSA cyber/physical exercises** targeted to the commercial maritime sector (ports, maritime companies, ships, industry etc).

THE RISK ASSESMENT CHALLENGE FOR PORTS' CIS

MITIGATE

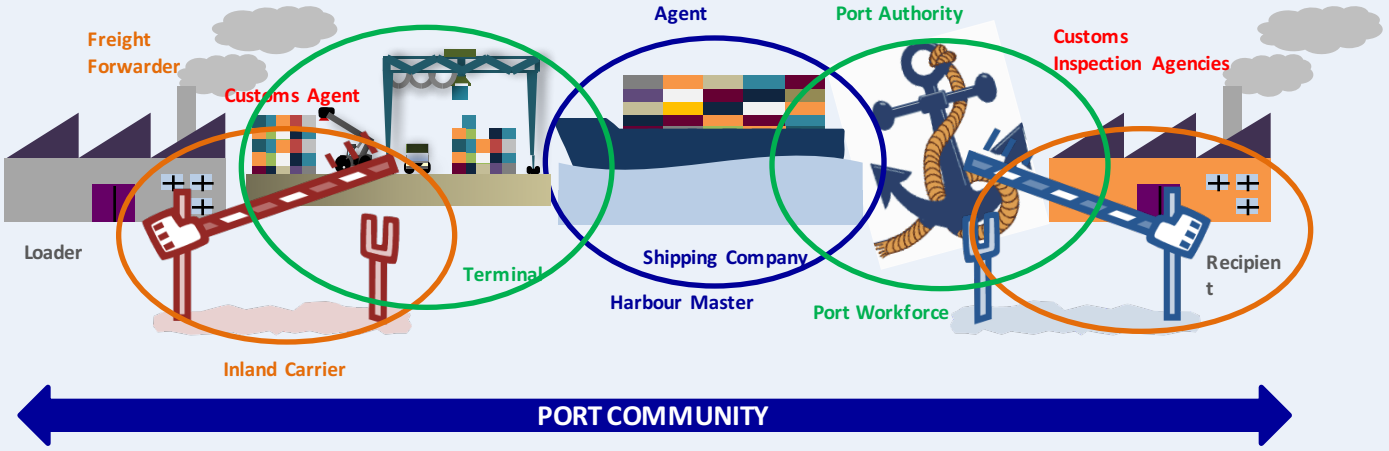
Holistic Risk Assessment

CYSM

MITIGATE

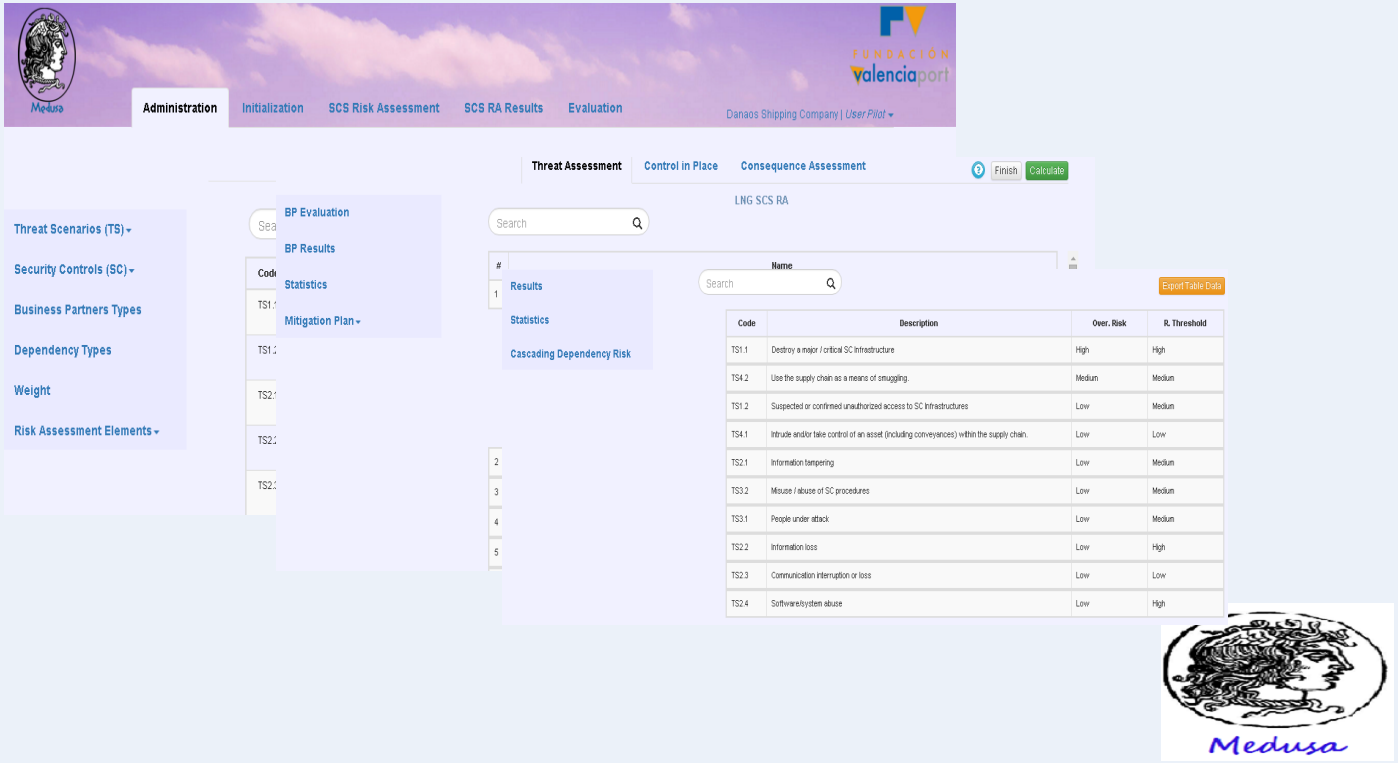
THE RISK ASSESMENT CHALLENGE FOR MARITIME SUPPLY CHAINS

MITIGATE



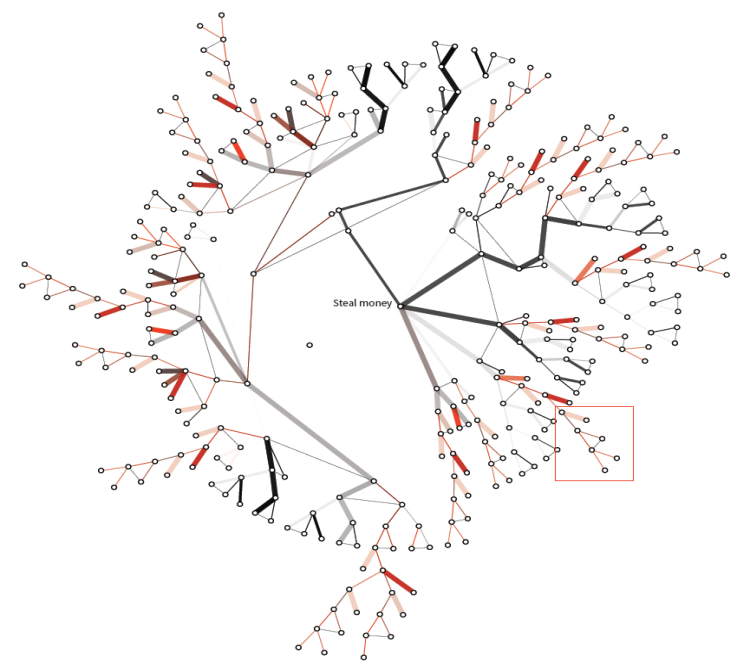
MEDUSA

MITIGATE



THE RISK ASSESMENT CHALLENGE FOR MARITIME SUPPLY CHAINS' INTERCONNECTED CYBER ASSETS

MITIGATE



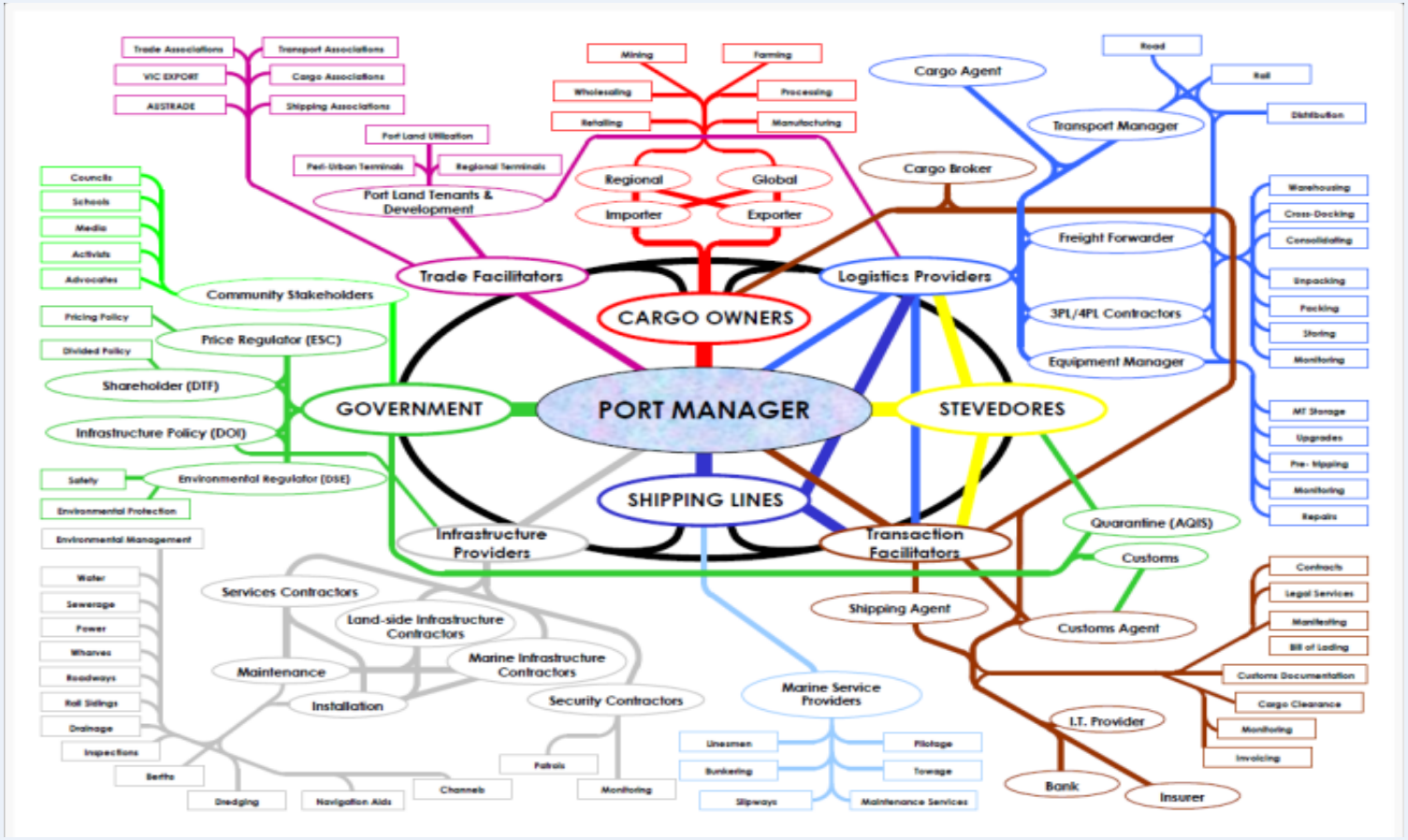
MITIGATE PROJECT

- **MITIGATE methodology** for assessing the complex, propagated risks of the interconnected supply chains' cyber assets
- MITIGATE dynamic, risk assessment **tool**
- MITIGATE forecasting, simulation, crowed sourcing and risk assessment **services** utilizing open security data

www.mitigateproject.eu

THE CHALLENGE OF PHYSICAL-CYBER MARITIME RISKS

MITIGATE



MARITIME COMPUTER INCIDENT RESPONSE CENTERS

MITIGATE

The national or European CERTs do not guide maritime operators on how to manage security incidents. A trusted body need to undertake this role in order to:

- thoroughly assess the vulnerabilities
- forecast and evaluate the probability of hybrid attacks;
- access/receive warnings for upcoming attacks and vulnerabilities;
- recreate, visualize and forecast propagation/ cascading effects;
- provide guidance on investigating and handling complex, interrelated physical/cyber maritime security incidents;
- combine and analyze all security incident
- receive guidelines, share information and warnings

AUTOMATED BORDER CONTROL SYSTEMS (ABCS)

MITIGATE

The FRONTEX requirements (FRONTEX, 2012) for the ABC systems need to be enhanced in order to address the remaining challenges:

- **Mobility**
- **Interoperability**
- **Multimodality-Interconnection**
  - Indoor ABC gates
  - Mobile ABC gates
  - ABC portable devices held by the patrol controllers
  - Large ABC gates for vehicle
  - ABC systems for cargo

The E.C. **FastPass project** is considering the above needs

FastPass

MARITIME SOFTWARE CODE AUDITING

MITIGATE

- **Innovative maritime source code auditing tools are required in order to find security flaws** (e.g. authentication, access control, cryptography problems).
- **Maritime software** (for ship management, marine navigation, shipping ERPs,..) need to be audited by certification bodies
- **Port Community Systems** / National Single Windows security is treated as a "**black box**".

COST IS A CHALLENGE

- **Accountability needs to complement Security**. Commercial maritime CIs (ports, companies etc) can not afford to become military camps. Security needs to be viewed as a shared responsibility.

(e.g. If a navigation system is vulnerable to interruption, the provider is responsible for the mitigation of its vulnerabilities and not the maritime company or the port authority)

Accountability technologies, **enhanced SLAs** and **insurance policies** are proposed measures.

- **Security & Privacy as Cloud Services** hosted and operated by a trusted party (e.g. IMO, EMSA, NATO) will minimize the security costs of the commercial maritime entities

CONCLUSIONS

MITIGATE

Thank You

N. Polemi- dpolemi@gmail.com