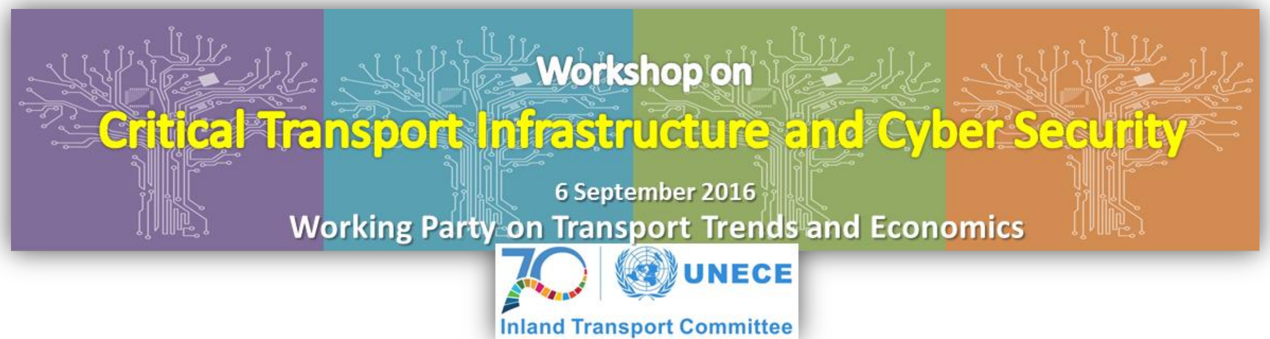


Workshop on

Critical Transport Infrastructure and Cyber Security

6 September 2016

Working Party on Transport Trends and Economics

UNECE

Inland Transport Committee

Critical Infrastructure and Cyber security
Transportation Sector

UNECE

Working Party on Transport Trends and Economcs

Senza il preventivo consenso di **SI-IES s.r.l.** non deve essere resa nota a terze parti ne riprodotta, sotto qualsiasi formato, l'informazione contenuta in questa proposta

Diary

Trasportation Sector Analysis

Critical Infrastructures LEGAL FRAMEWORK

Interdependencies

Sustainable Strategic Path

Focus on Maritime CI

Proposed approach identified by Dual Cipp

Scenarios proposed in DUAL Cipp

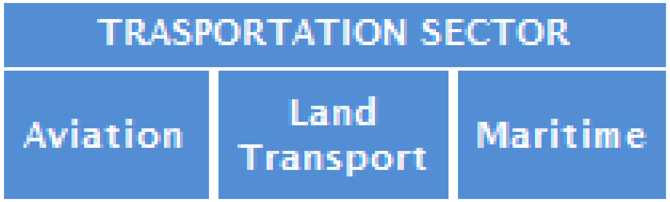
Conclusion

Contact Us

Trasportation Sector Analysis

In our mobile society transport is a key sector of the economy and sustains over 11 million jobs in EU.

- efficiency
- **safety and security**
- sustainability (green transport technologies)



TRASPORTATION SECTOR

Aviation

Land Transport

Maritime

Transportation has played a key role in the development of our society. Several changes are affecting this sector.

The question is: are we ready for this or not?

The arrival of new technologies and services that help cities and vehicles can reach a global value up to 2.5 Trillion per year in 2025.
The information everywhere World has opened up new opportunities to make the existing transportation network far more efficient and user friendly.

- Sustainable mobility
- Passenger safety and security
- Data protection and privacy
- ID management and access control
- Traffic and vehicle management
- Overload, congestion, delays
- Energy and environmental issues
- Sales, fees and charges
- Resilience management structure

CRITICAL FUNCTIONS

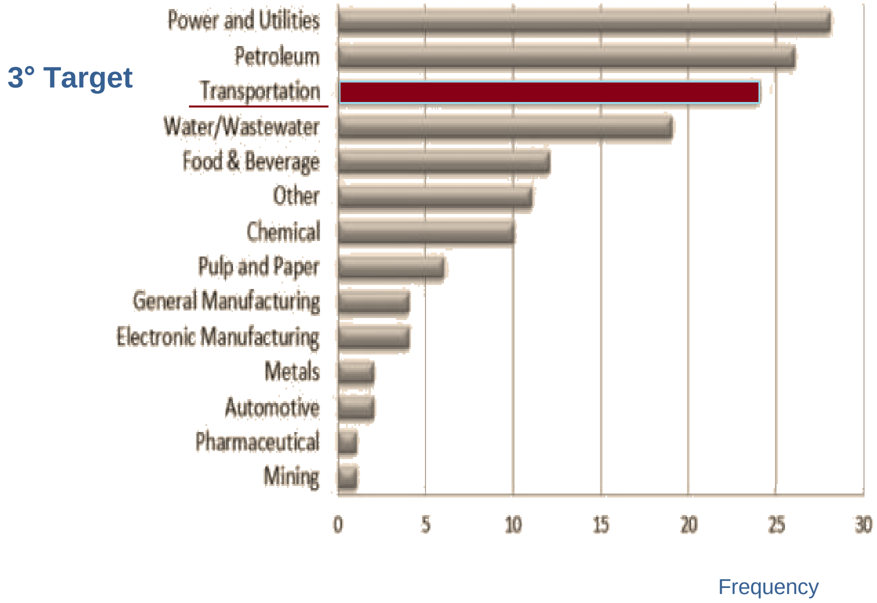
Trasportation Sector Analysis

Trasportation Attacks in a Digital Age*:*

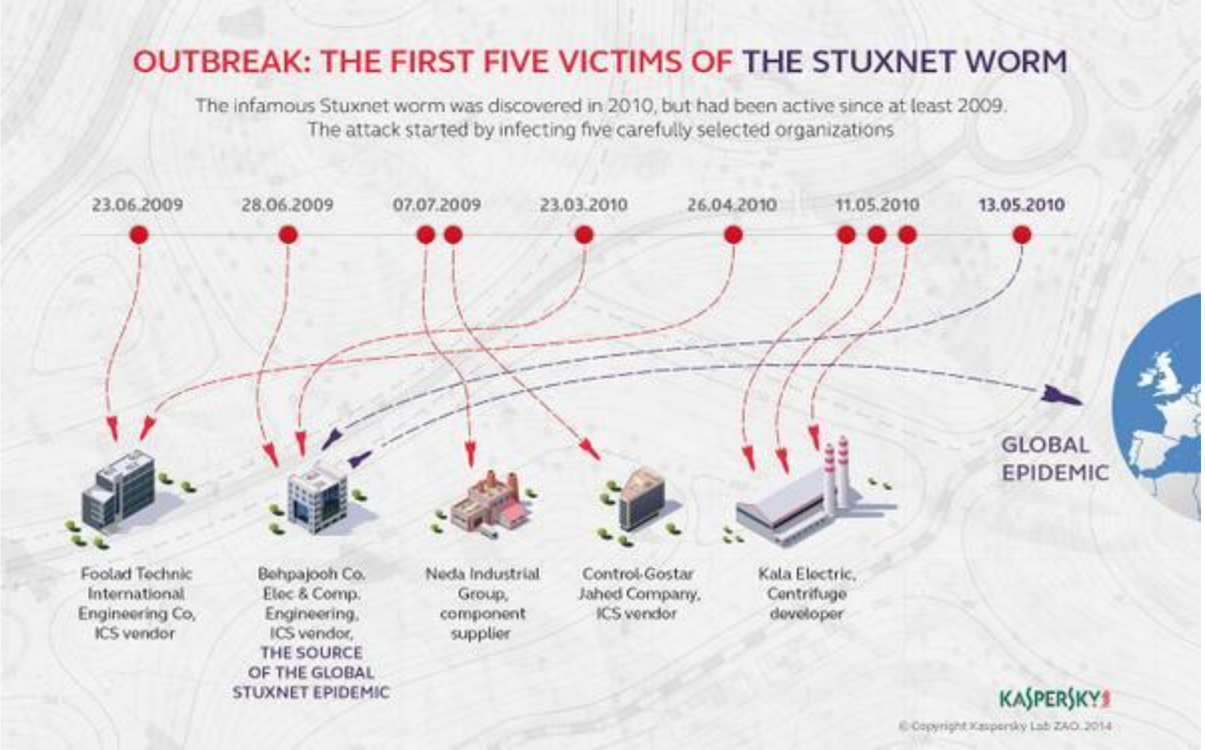
- Increasing dependence on technology and web-based communication has amplified cyber threaths.
- It is fundamental to protect transport infrastructures because of the rising number and increasing complexity of cyber attacks.
- It is essential to provide reliable and safe transport infrastructure solutions and to guarantee that transportation remains open, operating and safe for people depending on it

SECURITY THREATS

- Crimeware
- Cyber business/industrial Espionage
- Insider Misuse
- Web App Attacks
- Network-damaging attempts
- Manipulation of access control and monitoring systems
- Point-of-Sale Intrusions
- Software Errors
- Data Theft/Loss
- Payment Card Skimmers
- Denial of Service
- Natural hazards and impairments
- Terrorism



Trasportation Sector Analysis


OUTBREAK: THE FIRST FIVE VICTIMS OF THE STUXNET WORM
The infamous Stuxnet worm was discovered in 2010, but had been active since at least 2009.
The attack started by infecting five carefully selected organizations
23.06.2009
28.06.2009
07.07.2009
23.03.2010
26.04.2010
11.05.2010
13.05.2010
Foolad Technic International Engineering Co, ICS vendor
Behpajooh Co. Elec & Comp. Engineering, ICS vendor, THE SOURCE OF THE GLOBAL STUXNET EPIDEMIC
Neda Industrial Group, component supplier
Control-Gostar Jahed Company, ICS vendor
Kala Electric, Centrifuge developer
GLOBAL EPIDEMIC
KASPERSKY
© Copyright Kaspersky Lab ZAO, 2014

In the 2014 Cybe sec entered the top 10 gloabl risk on the Allianz risk barometer.

More then 50% of Cyber Attacks are conducted on Country Critical Infrastructure like electricity, water and oil and gas. 75% of the target are industrial companies.

Most of those infrastructures were designed for resilience but never designed with cber sec in mind.

Critical Infrastructure – LEGAL FRAMEWORK

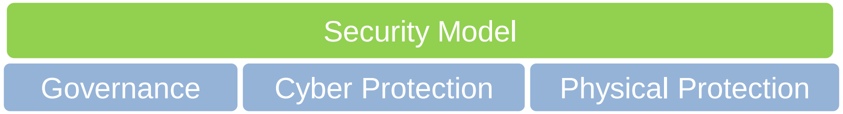
EU Critical Infrastructure includes the the ocean and short shipping ports as indicated in the **Directive 114/2008**, and concurrently critical part of the supply chains and trasport routes, transferring goods and passengers.

EU PORTS:
- serve around 3,733 mln of tons of freight flows
- 397 mln of passensger per year
- 74% of goods entering or leaving the EU by SEA
- 1.5 mln workers

enisa
European Network and Information Security Agency

Enisa Report on Cyber Sec challenges in the Maritime Sector seems evident that cyber threats are a growing menace, spreading to all industry sector that are relying on ICT systems. Recent deliberate distruptions of critical automatetion systems such as stuxnet, prove that cyber attackes have a significant impact on CI.

Security and Emergency Management



Governance

Identify vulnerabilities and gaps, prioritize and implement protection programs

Securing transport infrastructure in a structured consistent way.

Cyber Protection

Physical Protection

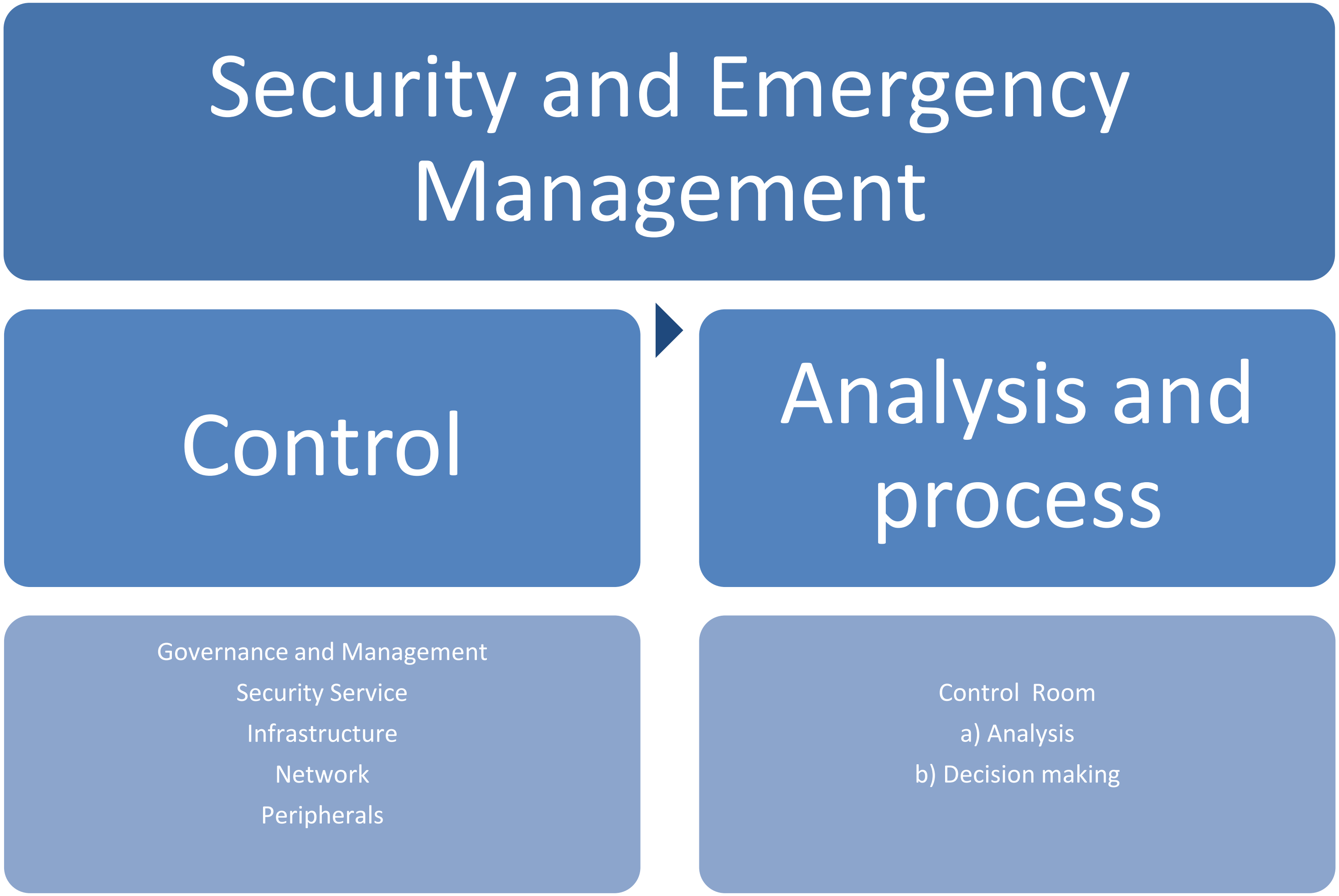
Core- implementation

- Definition of a Security and Emergency Control Room:
Structured and consistent continuous monitoring of security events detected by a centralized **control platform** for efficient **monitoring** and **prompt decision-making process**

- Design of the platform according to a risk-based criteria. Identification of Relevant indicators and sources of attack during critical cyber and physical events (e.g. potential attacks on ICS, SCADA, navigation systems, physical access, energy systems maintenance and management)

- **Advanced Analytics** and **Big data** analysis techniques for security, that guarantee new levels of protection and control via data sources analysis

Security and Emergency Management



Security and Emergency Management

Control

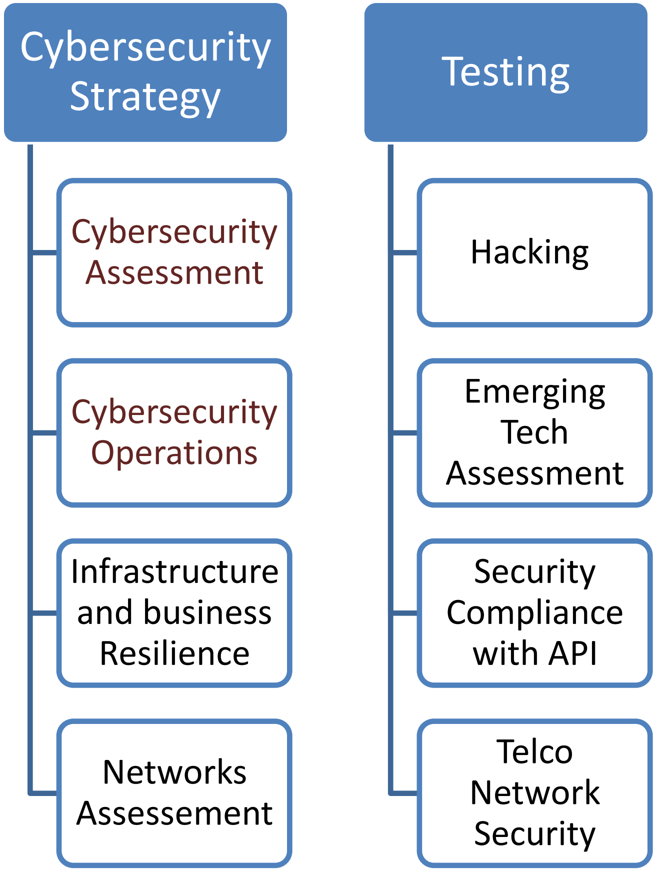
Analysis and process

Governance and Management
Security Service
Infrastructure
Network
Peripherals

Control Room
a) Analysis
b) Decision making

PORT HYBRID SECURITY SYSTEMS – REAL TIME ALERT

Security and Emergency Management



- Cybersecurity Strategy
  - Cybersecurity Assessment
  - Cybersecurity Operations
  - Infrastructure and business Resilience
  - Networks Assessement
- Testing
  - Hacking
  - Emerging Tech Assessment
  - Security Compliance with API
  - Telco Network Security

Hackers recently shut down a floating oil rig by tilting it, while another rig was so riddled with computer malware that it took 19 days to make it seaworthy again; Somali pirates help choose their targets by viewing navigational data online, prompting ships to either turn off their navigational devices, or fake the data so it looks like they're somewhere else; and hackers infiltrated computers connected to the Belgian port of Antwerp, located specific containers, made off with their smuggled drugs and deleted the records.

Interdependencies

The state and operation of each infrastructure is correlated to the state of other infrastructures.

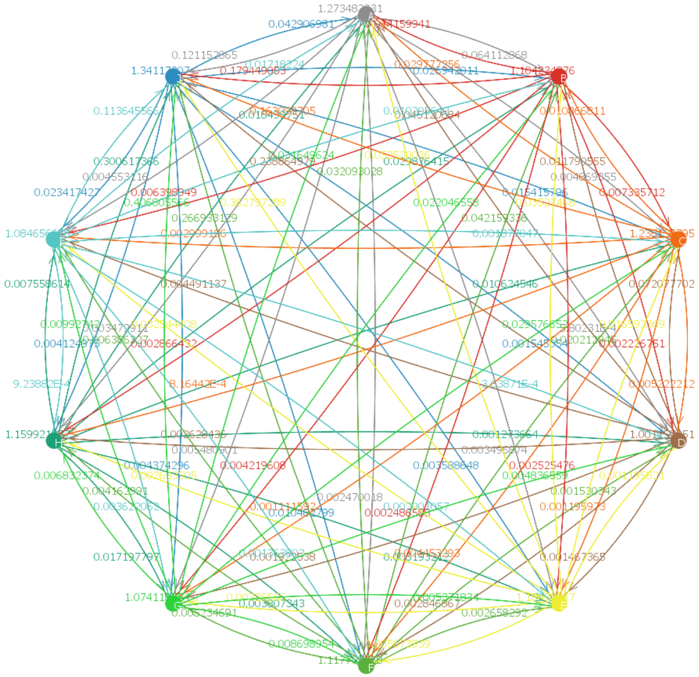
Dependency of one transport system on physical material output, transmission of information, local environmental effects, operations of other transport systems of infrastructures.

[Physical, cyber, geographical, functional dependencis]

Risk assessment methodologies must take into account cross-sectoral dependencies and events that could affect simultaneously several infrastructures.

⇨ Cascading effects

Cyberattacks could damage port operations for weeks or months, thereby dramatically affecting trade and commerce,



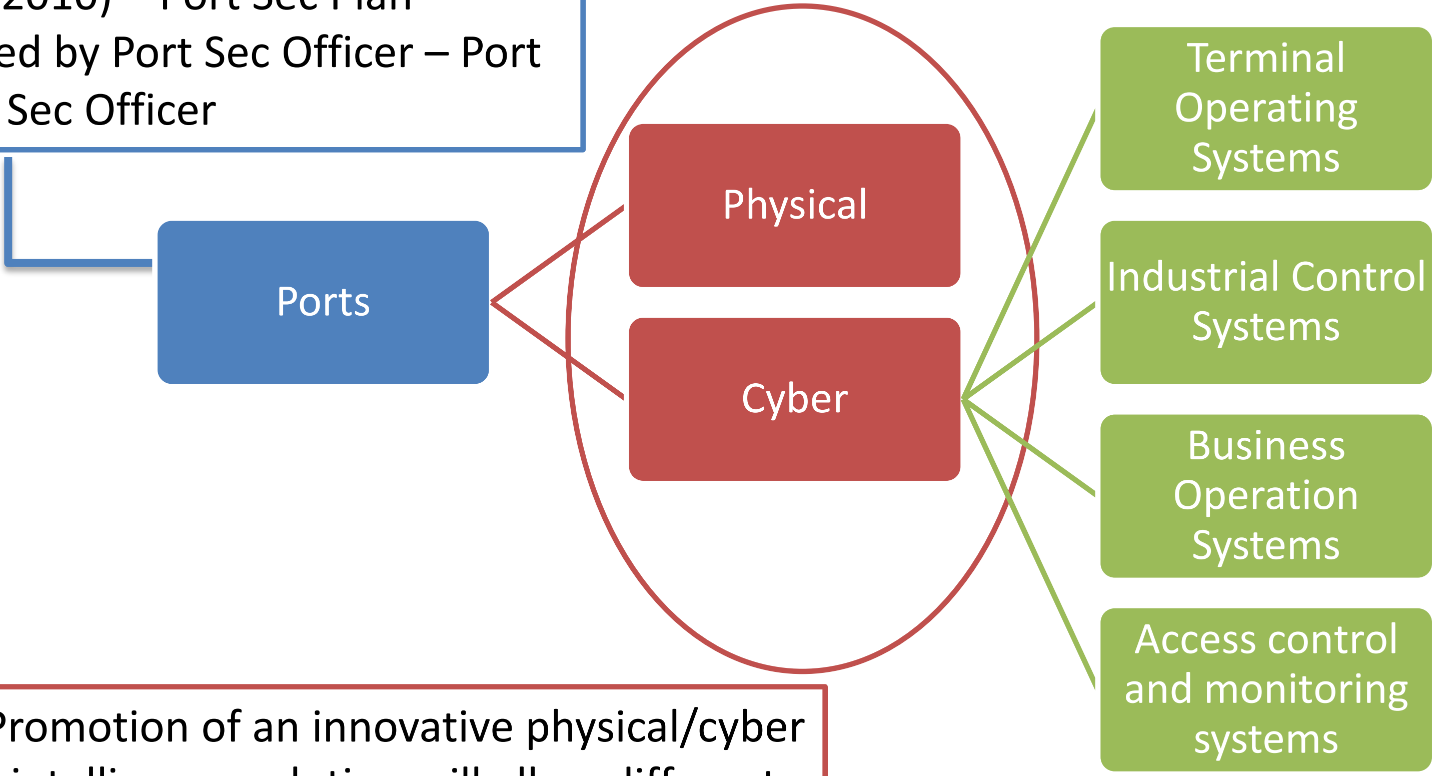
Sustainable Strategic Path

SUSTAINABLE STRATEGIC PATH

SECURITY PROFESSIONAL SERVICES	CYBER INTELLIGENCE PRODUCTS	CULTURE, ROLES, DUTIES AND RESPONSIBILITIES	GOVERNANCE AND POLICY ROADMAP
Multi-expertise and knowledge towards sophisticated analytic tools and enhanced protection functionalities	Design of advanced security systems – Intelligent Security Platform Updating, tailored and coordinated solutions	Distribution of responsabilities, Interaction among relevant bodies on national and European scale, Information sharing	Short, medium and long time planning -People -Process -Technology

Focus on Maritime CI

The relevant legislation on port sec is the ISPS Code (EU/725/2004 and EU/65/2010) – Port Sec Plan managed by Port Sec Officer – Port Facility Sec Officer


Ports
Physical
Cyber
Terminal Operating Systems
Industrial Control Systems
Business Operation Systems
Access control and monitoring systems

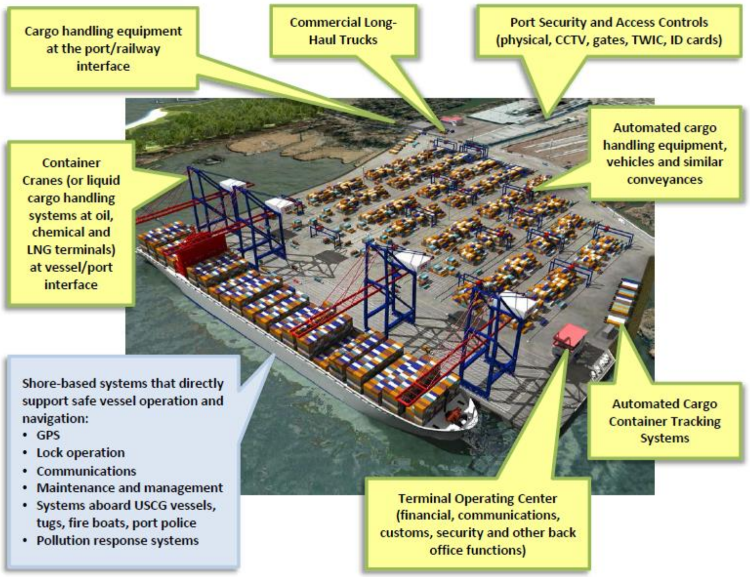
Promotion of an innovative physical/cyber intelligence solution will allow different stakeholders active in port operations to cooperate in managing the physicial and cyber sec threats

Focus on Maritime CI

Ports and Hinterland

PORTS

SHIPS



Cargo handling equipment at the port/railway interface

Commercial Long-Haul Trucks

Port Security and Access Controls (physical, CCTV, gates, TWIC, ID cards)

Automated cargo handling equipment, vehicles and similar conveyances

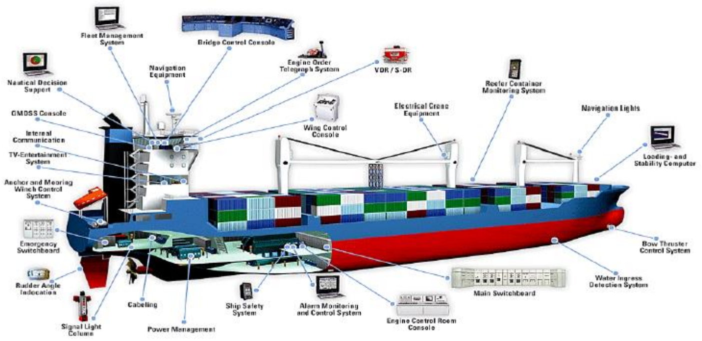
Container Cranes (or liquid cargo handling systems at oil, chemical and LNG terminals) at vessel/port interface

Shore-based systems that directly support safe vessel operation and navigation:

- GPS
- Lock operation
- Communications
- Maintenance and management
- Systems aboard USCG vessels, tugs, fire boats, port police
- Pollution response systems

Automated Cargo Container Tracking Systems

Terminal Operating Center (financial, communications, customs, security and other back office functions)


Fleet Management System
Bridge Control Console
Engine Order Telegraph System
VDR / S-DR
Navigation Equipment
Nautical Decision Support
GMDSS Console
Internal Communication
TV-Entertainment System
Anchor and Mooring Winch Control System
Emergency Switchboard
Rudder Angle Indication
Signal Light Column
Cabeling
Power Management
Ship Safety System
Alarm Monitoring and Control System
Engine Control Room Console
Main Switchboard
Wing Control Console
Electrical Crane Equipment
Reefer Container Monitoring System
Navigation Lights
Loading- and Stability Computer
Bow Thruster Control System
Water Ingress Detection System

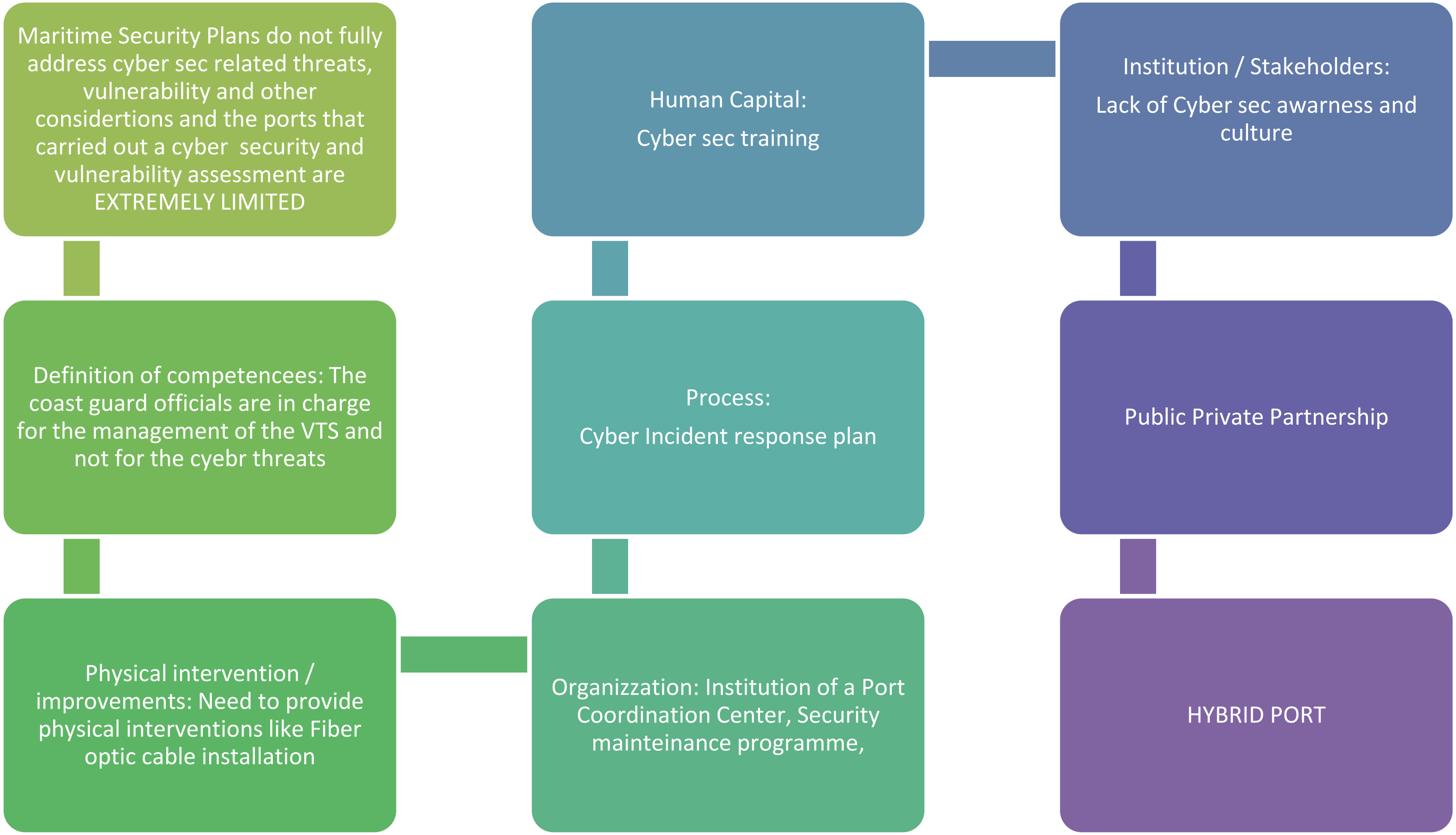
Survey

Piloting

Standard

Incident Response

PROPOSED APPROACH – IDENTIFIED BY DUAL CIPP



Maritime Security Plans do not fully address cyber sec related threats, vulnerability and other considertions and the ports that carried out a cyber security and vulnerability assessment are EXTREMELY LIMITED

Definition of competencees: The coast guard officials are in charge for the management of the VTS and not for the cyebr threats

Physical intervention / improvements: Need to provide physical interventions like Fiber optic cable installation

Human Capital:

Cyber sec training

Process:

Cyber Incident response plan

Organizzation: Institution of a Port Coordination Center, Security mainteinance programme,

Institution / Stakeholders:

Lack of Cyber sec awarness and culture

Public Private Partnership

HYBRID PORT

DUAL CIPP PROJECT – SUBMITTED BY AN INTERNATIONAL CONSORTOIUM COMPOSED BY 7 MS in the framework of H2020 CIP Call

SCENARIOS PROPOSED IN DUAL CIPP

Scenarios	*Events*
Cyber attacks on logistic transportation	Event 1: sending a PDF document to a key user that from a user's perspective contains some interesting data. However, opening this PDF triggers the execution of an attached exploit (for a publicly known vulnerability in Adobe Reader) that silently installs a remote access service on the computer .
	Event 2: the hackers handle to get access to more sophisticated attack tools capable of identifying and exploiting vulnerabilities that pertain to the in-vehicle communication interfaces, e.g., mobile communications, near field communications, wireless sensor networks, etc.
	Event 3: engage into malicious activities spanning from simple phishing attacks (targeting port authorities and key employees)
	Event 4: the hackers exploit vulnerabilities in the surveillance system of the port that controls the CCTV video cameras in order to gain access and delete video streams that show their malicious activities.

CONCLUSIONS

NEED TO ADDRESS cyber vulnerabilities in the framework of the Maritime. These potential vulnerabilities include limited cybersecurity training and preparedness (human capital), errors in software (BUG), protection of commercial technologies, network connectivity and interdependencies, foreign dependencies, global positioning system jamming-spoofing.

A cyber attack on networks at a port or aboard a ship could generate
Lost cargo, port disruptions, Physical and environmental damage.

Several mitigation measures can increase the security and resiliency of ports: setting up maritime cybersecurity standards, sharing information across the sector, conducting routine vulnerability assessments, using best practices, mitigating insider threats, and developing contingency plans for cyber attacks.

Knowledge is power - Francis Bacon

Contact Us

THANK YOU

for your attention

Director
European Services Institute
SI-IES s.r.l.
Sito web: www.si-ies.it

Andrea Chiappetta

e-mail a.chiappetta@si-ies.it