Critical Infrastructure and Cyber security
Transportation Sector
UNECE
Working Party on Transport Trends and Economics
Transportation 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)

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.
Transportation Sector Analysis

Transportation Attacks in a Digital Age:

- Increasing dependence on technology and web-based communication has amplified cyber threats.
- 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

3° Target

[Bar chart showing frequency of various industries, with Transportation being the highest.]
In the 2014 Cyber sec entered the top 10 global risk on the Allianz risk barometer.

More than 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 cyber sec in mind.
EU Critical Infrastructure includes the ocean and short shipping ports as indicated in the Directive 114/2008, and concurrently critical part of the supply chains and transport routes, transferring goods and passengers.

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

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 disruptions of critical automation systems such as stuxnet, prove that cyber attacks have a significant impact on CI.
Security and Emergency Management

Security Model

Governance
- Identify vulnerabilities and gaps, prioritize and implement protection programs
- Securing transport infrastructure in a structured consistent way.

Cyber Protection
- 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

Governance and Management
- Security Service
- Infrastructure
- Network
- Peripherals

Analysis and process

Control Room
- a) Analysis
- b) Decision making

PORT HYBRID SECURITY SYSTEMS – REAL TIME ALERT
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,
<table>
<thead>
<tr>
<th>SUSTAINABLE STRATEGIC PATH</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECURITY PROFESSIONAL SERVICES</td>
</tr>
<tr>
<td>Multi-expertise and knowledge towards sophisticated analytic tools and enhanced protection functionalities</td>
</tr>
<tr>
<td>CYBER INTELLIGENCE PRODUCTS</td>
</tr>
<tr>
<td>Design of advanced security systems – Intelligent Security Platform</td>
</tr>
<tr>
<td>Updating, tailored and coordinated solutions</td>
</tr>
<tr>
<td>CULTURE, ROLES, DUTIES AND RESPONSIBILITIES</td>
</tr>
<tr>
<td>Distribution of responsibilities, Interaction among relevant bodies on national and European scale, Information sharing</td>
</tr>
<tr>
<td>GOVERNANCE AND POLICY ROADMAP</td>
</tr>
<tr>
<td>Short, medium and long time planning</td>
</tr>
<tr>
<td>- People</td>
</tr>
<tr>
<td>- Process</td>
</tr>
<tr>
<td>- Technology</td>
</tr>
</tbody>
</table>
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

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

Ports and Hinterland

PORTS

- Cargo handling equipment at the port/railway interface
- Container Cranes (for 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
- Commercial Long-Haul Trucks
- Port Security and Access Controls (physical, CCTV, gates, TWIC, ID cards)
- Automated cargo handling equipment, vehicles and similar conveyances
- Automated Cargo Container Tracking Systems
- Terminal Operating Center (financial, communications, customs, security and other back office functions)

SHIPS

Survey Piloting Standard Incident Response
Maritime Security Plans do not fully address cyber sec related threats, vulnerability and other considerations and the ports that carried out a cyber security and vulnerability assessment are EXTREMELY LIMITED.

Definition of competencies: The coast guard officials are in charge for the management of the VTS and not for the cyber threats.

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

Human Capital: Cyber sec training

Process: Cyber Incident response plan

Organization: Institution of a Port Coordination Center, Security maintenance programme,

Institution / Stakeholders: Lack of Cyber sec awareness and culture

Public Private Partnership

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