Ports’ Critical Information Infrastructure Protection

P-CIIP

Associate Professor N. Polemi
University of Piraeus–Dept. of Informatics
dpolemi@gmail.com
http://athina.cs.unipi.gr/security-lab/
EU’s over 1 000 individual ports handle 90% of EU external trade and 40% of internal trade. The 'blue' economy represents 5.4 million jobs.

Only the Greek 16 international and 140 regional ports served 15.5 million people in 2012. The direct contribution of the core Greek shipping cluster is €7.6B (3.5% of the Greek GDP).

Maritime Ecosystem

Ships
Banks
Maritime Companies
Ports
Ministries
Ship Industry
Customs
Port Authorities
Other Providers
IT Providers
Critical Infrastructures
The importance of port security

Port cyber security breaches cause serious economic damage, 3299 supply chain related attacks (PWC2013 report) e.g. 2013 port of Antwerp hackers accessed secure data causing theft cargo.

Existing maritime related efforts concentrate on the safety ignoring the cyber security. “the awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent” ENISA (2011)

2011-2014: slow progress in protecting the dual nature of the ports (physical, cyber)
Ports’ ICT System

1. **Users/Procedures**
   - Internal, external, cargo, vessels

2. **Information/data**
   - Marine, coastal, trade, ...

3. **e/m-Services**
   - Vessels, cargo, inland logistics, ...

4. **IT equipment/Software**
   - Servers, navigation, RFID, cameras, ERP, ...

5. **Telecom**
   - Networks, routers, optical fibers, ...

6. **Infrastructure**
   - Port facilities, buildings, terminals, gates, data centers
Existing efforts in P-CCIP

Port of Valencia -Spain
**International Maritime Organization (IMO) legislation:**

SOLAS ISPS code for the **safety** of the ships, passengers and cargo

**Port safety related EU legislation:**

* EC port security
* E.C. Regulation **324/2008** on procedures for conducting Commission inspections in the field of maritime security
* E.C. Directive **2010/65** on ships arriving/departing from EU Regulation **No 725/2004** on enhancing ship and port facility security
* EC Directive **2005/65** on enhancing ports

**CYBER SECURITY IS NOT ADDRESSED PROPERLY in the maritime legislation**
Existing port risk management methodologies (MSRAM, MARISA, CMA) are ISPS compliant but they do not deal with cyber internal or external threats, they do not estimate the cascading effects of interconnected threats from the ports’ supply chain.

Most EMSA and JRC systems concentrate on the safety and surveillance of the ports, vessels and containers (e.g. CISE, SafeSeaNet) or 7th FP E.C. maritime security related projects (SUPPORT, CONTAIN) do not address properly the dual nature of the ports.

.....are compliant with the safety maritime legislation but....

CIIP existing methodologies and tools (e.g. ATHENA, CIPMA, FAIT) concentrate on railways, airports and energy.

ICT risk management methodologies and tools (CRAMM, eBIOS, OCTAVE) are too generic.
Combining Management Approaches

Maritime Safety Approaches

CI Security Management Approaches

ICT Security Management Approaches
A HOLISTIC APPROACH TO PORT SECURITY

Holistic P-CLIP

- ISPS
- ISO
- CIIP
The National project:

S-port: http://s-port.unipi.gr/
### Security Impact Categories

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td></td>
</tr>
</tbody>
</table>

#### Organizational Impact Categories

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Losses</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Value</th>
<th>Assigned Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legal Consequences</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th></th>
</tr>
</thead>
</table>

### Organizational Impact Categories

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Losses</td>
<td></td>
</tr>
<tr>
<td>Legal Consequences</td>
<td></td>
</tr>
</tbody>
</table>

### Availability

<table>
<thead>
<tr>
<th>Organizational Impact Categories</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Losses</td>
<td></td>
</tr>
<tr>
<td>Legal Consequences</td>
<td></td>
</tr>
</tbody>
</table>
Upcoming security directives and actions

* **Directive 2013/40/EU** of 12 August 2013 on attacks against information systems
* **NIS Proposed Directive** COM 2013/0027 (COD) concerning measures to ensure a high common level of network and information security across E.U.
* **eIDAS** proposed directive on electronic identification and trusted services for electronic transactions in the internal market
* **NIS platform, ENISA**
Port Supply chain security

Well protected ports have an advantage in Global Supply Chains

Certified operators

C-TPAT / AEO

ISPS Port Directive
CSI / 24 hour rule

Certified Operators
AEO / GTPAT

Factory
Road/rail transport
Consolidation / distribution center
Port of loading
Vessel
Transit port
Vessel
Port of discharge
Road/rail transport
Consolidation / distribution center

W.C.O. SAFE framework of standards
New Policy and Standardisation Initiatives

Support FP7 project
E.U. trustworthy CIIs

- Privacy
- Accountability
- Security
Conclusions

Port of Carrara-IT
- Not new standards are needed, we only need targeted P-CIIP methodologies and tools compliant with standards, addressing the ports’ supply and be included in the NIS platform;
- The current E.C. actions, as reported in the 28/2/2014 “High level Conference on the EU Cybersecurity Strategy” for implementing the "Cyber security Strategy of the E.U. JOIN(2013)" do not cover sufficiently the P-CIIP. Further collaborative actions need to be undertaken with relevant stakeholders (e.g. United Nations, IMO, EMSA, IALA, SMDG, ITIGG, PROTECT, DG-MOVE);
- The cyber security strategy and directives (e.g. NIS, eIDAS) need to be implemented by the ports;
- In our democratic societies the E.U. ports’ and all other CIIs need to undertake not only security but also privacy and accountability measures. This 3-tier approach can become the E.U. competitive advantage to trustworthiness.
Thank you

dpolemi@gmail.com

Mykonos-GR