EU policies for cybersecurity in inland navigation

Dr Nineta Polemi

Programme Manager - E.U. Policies
DG CNECT/H1: Cybersecurity Technology & Capability Building
Maritime: Backbone for economy

Maritime transport is . . .

✓ the backbone of international trade around 80% of global trade by volume and over 70% by value is carried by sea and is handled by ports worldwide
✓ 74% of goods entering or leaving Europe go by sea
✓ More than 37,000 kilometres of waterways connect hundreds of EU cities
✓ 13 Member States have an interconnected waterway network of cities and industrial regions.
✓ Attractive target: 50% of all shipping companies word-wide were victims of cyber-attacks in 2018 (NATO-NMIOTC 2019)
Critical Infrastructures – CIs – (Information and Space CIs)

Common cyber assets e.g. networks, ICT components, technical capabilities

EU & international policies and agreements

Supply Chains

Maritime Cyber Activities depend **upon:**
Ports' complex ICT

SCADA system

Control Center

Enterprise Level

WAN

Leased Line

Supervision Level

Distribution Level

Field Level

Automatic Identification System (AIS)
Digitalization

Ships are expensive assets (more than 20 million euros is the value of a cargo ship)
Common maritime attacks

✓ GPS spoofing
✓ Unauthorized access to on-board mobile devices
✓ manipulation of Bill of lading
✓ signals jamming, monitoring
✓ targeted access on automated terminal infrastructures (e.g. electronic gates, RFIDs in containers, cameras, surveillance systems)
✓ spear phishing, DoS, ......

2018 attacks: Maersk, Port of Barcelona
US Ports ( Long Beach, San Diego),
Austral, Royal Navy of Oman
E.U. in Action

- Emergency Fund
- Sectoral Cooperation
- CSIRT
- Security Task Force
- Horizon 2020 EDIDP
- NIS, GDPR
- Emergency Fund
- ENISA
- Certification
- Blueprint Cyber
- Cybersecurity Strategy, CSDP
- EDA, CNECT, CERT
- EU-NATO
- EUROPOL
- ENISA
- EU, EUROPOL
- E.U. in Action
- Cyber Crisis
EU Maritime Cybersecurity Regulation/Policies

- Regulation No 725/2004 on enhancing ship/port facility security
- Directive 2005/65 on enhancing port security
- Regulation 324/2008: inspections in the field of maritime security.
- Directive (EU) 2016/1148 sets cybersecurity obligations –NIS-
- 2016 EU-NATO Joined Declaration (...enhance coordination, complementarity and cooperation in the maritime domain)
- eIDAS Regulation (2014) on electronic identification
- 2016 Directive 85/374/EEC on product liability
- Regulation 2016/679 on protection of privacy –GDPR-
- Space Strategy for Europe 2016/2325(INI)
- Regulation COM(2017)477 Cybersecurity Act
- 2018 Revised EU Maritime Security Strategy (emphasizes the need for improving the integration of cybersecurity)
MARITIME CYBERSECURITY GUIDELINES

• SOLAS XI-2 and the ISPS Code
• Guidelines on maritime cyber risk management (IMO)
• ETSI TR 103 456 CYBER; Implementation of the NIS COM(2017) 476 final "Making the most of NIS"
• C(2017)6100_final Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises (blueprint)
• Cyber Diplomacy Toolbox
• The Tanker Management/ Self Assessment - TMSA (OCIMF)
• The Guidelines on Cyber Security Onboard Ships (supported by: BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI)
• Cyber Security Awareness - AMMITEC
E.U. Initiatives

- cPPP-ECSO (2016)
- Digital European Industry Initiative (2016)
- Electronic Components and Systems (ECSEL JU)
- Supercomputers (EuroHPC JU)
- 5G Action Plan (2016)
- Framework for screening foreign investment
- Strategic Forum for Important Projects of common European Interest (IPCEI)
- Digital Skills and Jobs Coalition
- Space Programme (2018)
- AI Declaration/ AI Communication (2018)
- Communication on online disinformation (April 2018)
E.U. Maritime Cyber Security R&D

CYSM, MEDUSA: Static SC RM’ methodology and tools
MITIGATE: Dynamic evidence-driven Maritime SC RM environment (simulation, crowd-sourcing, open data) (ISO27001, 27005, ISPS, CIIP, ISO28000)
SAURON: Situational Awareness platform
TRITON: Trusted Vessel Information from Trusted On-board Instrumentation SEABILLA: Sea Border Surveillance
MARINE-EO: Bridging Innovative Downstream Earth Observation and Copernicus enabled Services for Integrated maritime environment, surveillance and security
CEF Maritime Transport Projects 2014-2019
The future
Future Threats

✓ International **Supply chains, AI** and **5G** will bring severe attacks causing tremendous damages from making vessels invisible to destroying their fire-alarm systems to disrupting their cargo management systems.

✓ The on-board connected IT systems (e.g. cargo management, bridge systems, passengers servicing, communication systems etc.) more and more are provided by international suppliers with **non EU security certifications**, more vulnerable to attacks.

✓ The vessels are controlled by their inland shipping company, but operated by the on-board technical departments with no necessary **cyber skills**.
The Digital Europe Programme 2021-2027

Digital Europe Programme
Reinforcing digital capacities
Ensuring their best use

Digital transformation & Interoperability
1.3 € billion

Advanced digital skills
0.7 € billion

Cybersecurity & trust
2 € billion

High performance computing
2.7 € billion

Artificial intelligence
2.5 € billion

Total
€ 9.2 billion in total
Brussels, **12.9.2018** COM(2018) 630 final

**2018/0328 (COD) REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL** establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres
**Preparing for CCCN**

More than **€63.5 million** invested in **4 projects**

<table>
<thead>
<tr>
<th>Project</th>
<th>Partners</th>
<th>EU Member States involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONCORDIA</td>
<td>46</td>
<td>14</td>
</tr>
<tr>
<td>Cyber Security for Europe</td>
<td>43</td>
<td>20</td>
</tr>
<tr>
<td>ECHO</td>
<td>30</td>
<td>15</td>
</tr>
<tr>
<td>SPARTA</td>
<td>44</td>
<td>14</td>
</tr>
</tbody>
</table>

**CONCORDIA**
- Key words: Cybersecurity for citizens, Application cases, Research Governance, Cyber Range, Cybersecurity certification, Training in security
- EU Member States involved: 14
- Partners: 46

**Cyber Security for Europe**
- EU Member States involved: 20
- Partners: 43

**ECHO**
- EU Member States involved: 15
- Partners: 30

**SPARTA**
- EU Member States involved: 14
- Partners: 44

**More than 160 partners** from **26 EU Member States**

Maritime Cybersecurity: A strategic priority

Building maritime ecosystem resilience to cyber attacks

1. Capacity Building
   - Enhanced national/inter national capabilities & Risk management requirements
   - Training
   - Industrial capabilities

2. Prevention & Response Coordination
   - Maritime CERT (ISAC)
   - Information sharing
   - International Collaboration
   - Certified Maritime cyber products
Follow us on get involved:

On:  https://twitter.com/Cybersec_EU

Subscribe to our newsletter:  http://europa.eu/!yT68Jg
Thank you for your attention!

Nineta.POLEMI@ec.europa.eu