The Baltic Seas International Maritime Conference
24th – 25th of September in Turku

Improving Cybersecurity Preparedness in the Maritime Logistics Industry

Harri Pyykkö, Research Scientist VTT

10/10/2019 VTT – beyond the obvious

Cybersecurity challenges in Maritime logistics industry

- The Port systems and maritime supply chains are very complex including various stakeholders and data transfers between different ICT systems

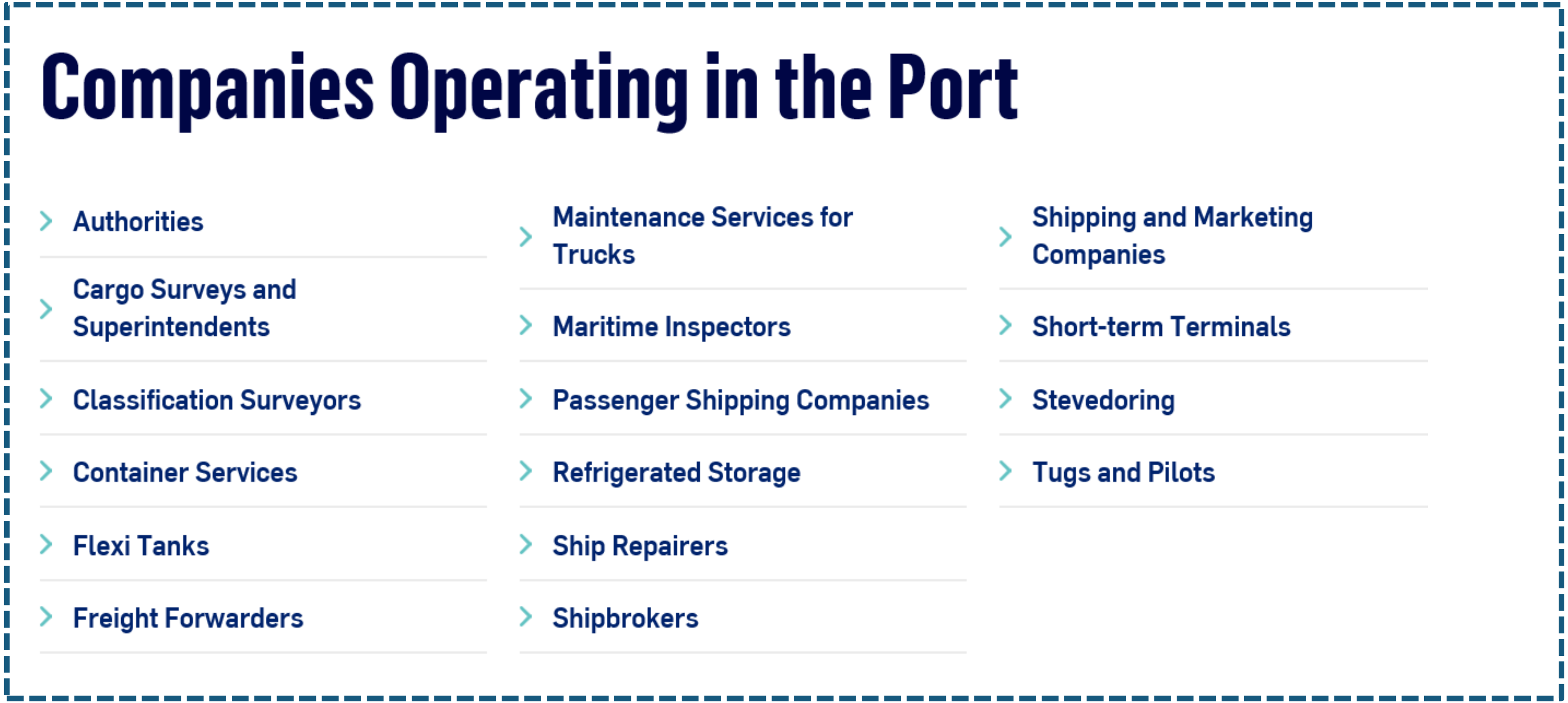
- Empirical research (ref. Ahokas & Laakso 2017; Ahokas 2019 etc.) indicates that the level of cyber threat preparedness and regulation in maritime industry should be improved

- Cyber attackers could simply by shutting down the port ICT systems could endager emergency responses and cause different types of accidents (Kouwenhoven et al. 2016; Polemi 2018)

- The cybersecurity specialists should have a deep understanding of maritime logistics operations and IT infrastructure in order to provide the most sufficient prevention models. Also the end users within maritime industry should be trained to prevent unintentional security breaches

- As the reliance on ICT systems grows, aspects of physical security need to be updated to a sufficient level in terms of security of ICT and physical-related components of the maritime sector (Fitton et. Al. 2014)

Port operations include various stakeholders – Port of Helsinki contact list

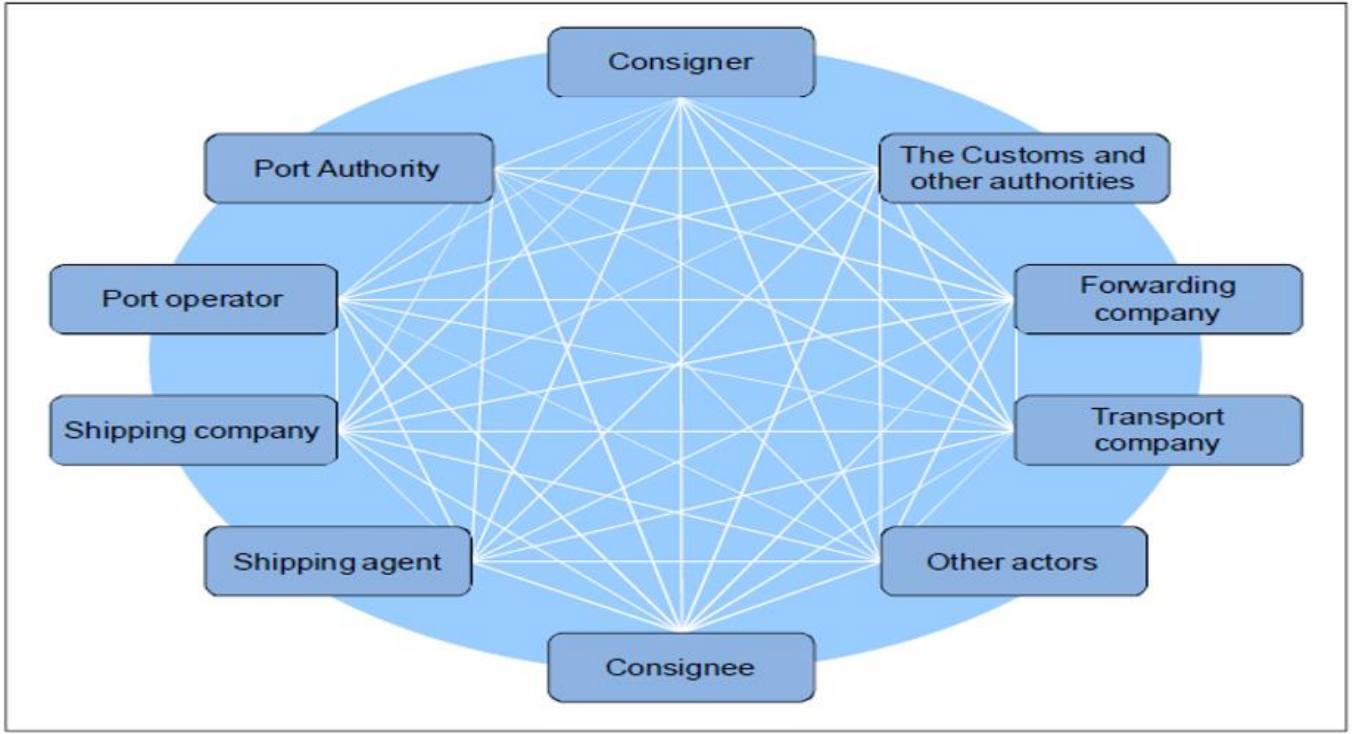


Companies Operating in the Port

- Authorities
- Cargo Surveys and Superintendents
- Classification Surveyors
- Container Services
- Flexi Tanks
- Freight Forwarders
- Maintenance Services for Trucks
- Maritime Inspectors
- Passenger Shipping Companies
- Refrigerated Storage
- Ship Repairers
- Shipbrokers
- Shipping and Marketing Companies
- Short-term Terminals
- Stevedoring
- Tugs and Pilots

Traditional communication model in a port

(REF. Milá, S. (2009). Port Community System (PCS), its present & future. Sail to the Future, Vol. 2, No. 1, May 2009.)



Different levels of data flows occuring in maritime logistics

1 Port/ Terminal operations

- Terminal operating system / TOS is used monitor and control the operations within Port/Terminal area.
- TOS has interfaces with various other ICT systems of the supply chain.
- Terminal data includes data both from the physical events and documentation.

2 Cargo Ship operations

- Vessel location information: AIS system feeds, typically provided via API or on user inferface
- Vessel performance data: Speed, bunkering etc.
- Cargo data: Freight contracts, Information about the loaded/planned cargo, planning of weight distribution, IMDG classified cargoes, risk analysis etc.
- Event data: Weather, congestion, routing changes etc.

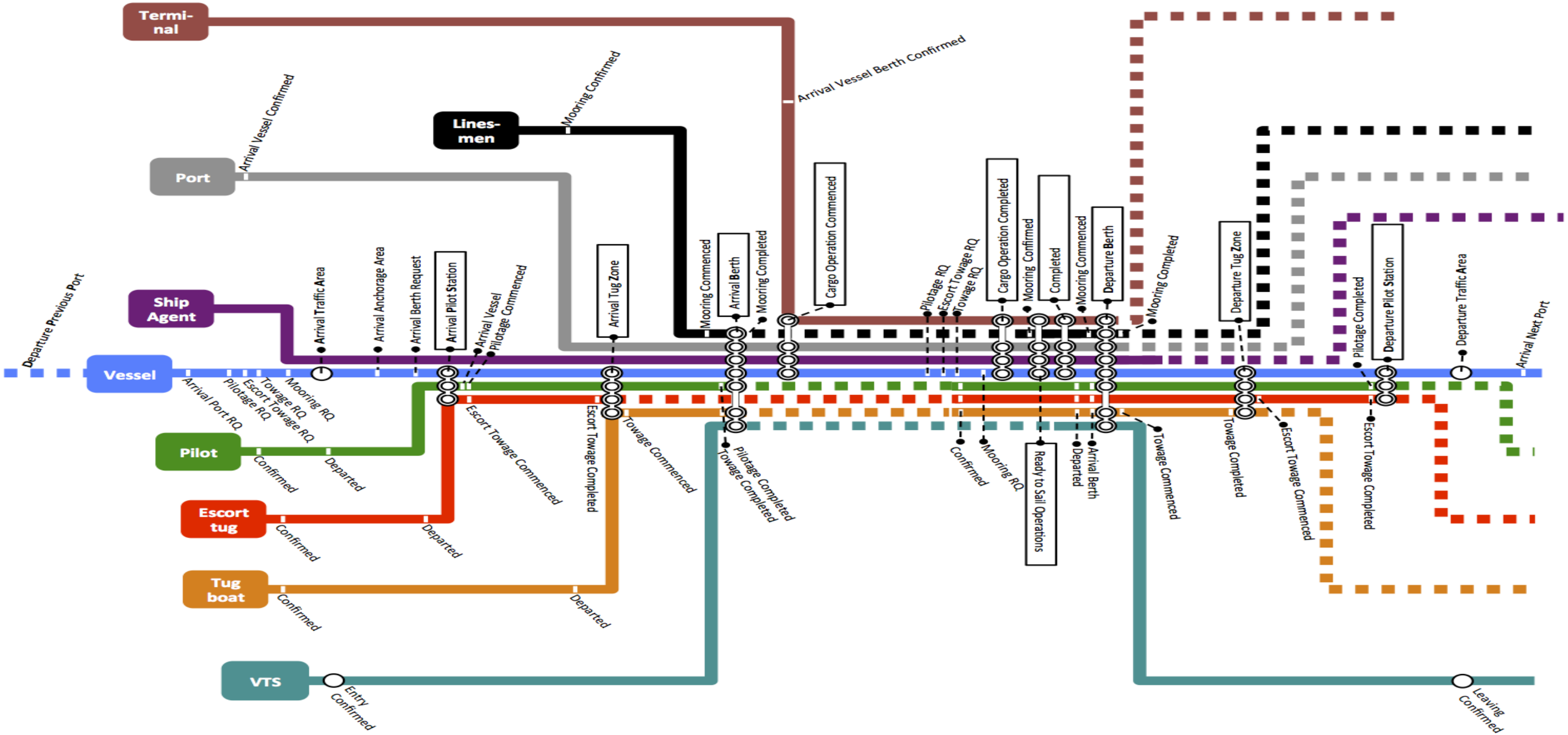
3 The Customs and other authorities

- Regulation, National/EU/IMO
- Risk analysis, physical and cyber security
- AREX, PortNET, VTS, GOFREP , ISPS, VGM, ENS
- Taxation, statistics
- Interfaces to various operational systems
- Customs is allowed to access all data if needed

4 Cargo owner/receiver, forwarder, broker, rail/road operator etc.

- Contract data: Freight, Commercial, Brokerage, Insurance,
- Document data: Cargo details, Bill of Lading, commercial invoice, declarations
- Various own ICT systems, SAP/ERP etc.
- Inttra, EDIFACT messages between systems

Cargo ship port call – Interrelationship between different actors (ref. Lind et al. (2016))



Cyber-MAR, 3 year H2020 project

- Cyber-MAR is an effort to fully unlock the value of the use of cyber range in the maritime logistics value chain via the development of an innovative simulation environment

- CSIRTs/CERTs data collected will be analysed and feed the knowledge-based platform with new-targeted scenarios and exercises.

- Through Cyber-MAR, the maritime logistics value chain actors will increase their cyber-awareness level; effort to minimize business disruption potential.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Cyber-MAR methodology – three-tiered approach

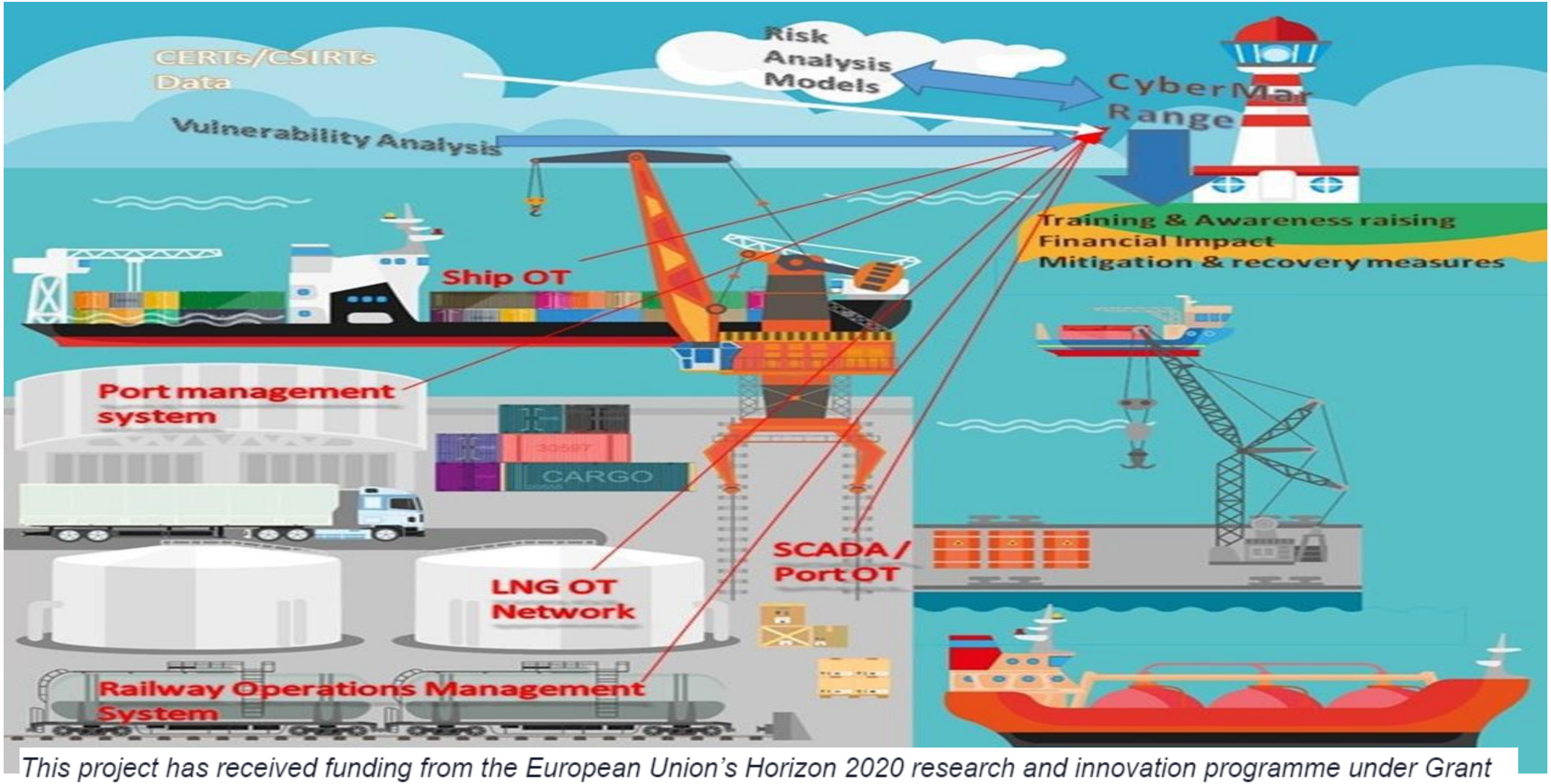
- **1. Training** systematically both cybersecurity professionals and employees to be well prepared when an attack occurs

- **2. Testing** environment for different technologies including the new emerging technologies

- **3. Measuring** procedures by using pilots and simulations which will assist to detect areas for improvement and deficiencies in the procedures followed after a cyber-attack.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Cyber-MAR in a maritime logistics environment



This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

beyond
the obvious

www.vtt.fi

10/10/2019