European Collaboration in the Field of Cybersecurity for Inland Navigation

Gernot Pauli
Chief Engineer CCNR
What to expect?

- Introduction to European inland navigation
- Introduction to CCNR
- Safety of inland navigation
- Sustainability of inland navigation
- ICT in inland navigation
- European collaboration in inland navigation cybersecurity
- Conclusion
Freight transport in European inland navigation

North-South Axis
60 billion TKM

Traditional
Rhine

Seine
4 billion TKM

Moselle
3 billion TKM

Rhône-Saône
1 billion TKM

West Germany Canals
4 billion TKM

Mittelland Canal
3 billion TKM

Elbe
3 billion TKM

6,000 enterprises
16,000 employees
5,000 million € turnover
2.75 employees / enterprise
0.8 million € turnover / enterprise

In total
~145 billion TKM

Source: CCNR analysis, Eurostat, VNF, Destatis, Danube Commission, Moselle Commission
Introduction inland navigation

Economic weight of the Rhine States in inland navigation

- **Transport activity**: 84%
  - Rhine states: 15.5%
  - Other states: 0.5%
  - Other states: 68.5%

- **European companies**: 87%
  - Rhine states: 10%
  - Other states: 77%

- **Turnover**: 91%
  - Rhine states: 5%
  - Danube states: 4%
  - Other states: 82%

Source: CCNR based on Eurostat
CCNR

- Governs navigation on the Rhine
- Oldest international organisation (200 years)
- Based on Mannheim Convention (150 years)
- Guaranteeing freedom of navigation and promoting navigation on the Rhine
- Promoting safety of navigation
- Binding regulations (traffic/vessel operation, technical requirements for vessels, crew qualification, manning)
- Rhine regulations blueprint for others
- CCNR regulations complementary to or harmonized with EU regulations

CCNR exemplary safety regulations for inland navigation
ICT widely used to ensure safety

- Digital emission control systems...
- Natural Environment
- Cargo
- Navigation
- People
- Vessels

Cybersecurity vital for safety of inland navigation

- Electronic logbooks, tachographs...
- Automated track guidance systems, River Information Services...
- Loading computers, temperature control systems...
- Control systems for vessel and equipment...
Evolving domains of safety

1838 First regulations for dangerous goods
1850 Rhine Police Regulations (RPR)
1904 Vessel Inspections Regulations (RVIR)
1996 Waste Convention (CDNI)
2000 First regulation on emissions from IWW vessels

Safety of inland navigation

Digital environment new safety domain for inland navigation
A sustainable transport system is one that …

... allows the basic access needs of individuals and societies to be met **safely** and in a manner consistent with human and ecosystem health, and with equity within and between generations;

... is affordable, operates efficiently, offers choice of transport, and allows the basic access needs of individuals and societies to be met **safely** and in a manner consistent with human and ecosystem health, and with equity within and between generations;

... limits emissions and waste within the planet’s ability to absorb them, minimizes consumption of non-renewable resources, limits consumption of renewable resources to the sustainable yield level, reuses and recycles its components, and minimizes the use of land and the production of noise!

Ministers of Transport of the EU (2001)
ICT in inland navigation

Inland navigation highly exposed to cyber threats
Perspectives for ICT in inland navigation

**CCNR October 2018 Mannheim ministerial declaration**

“We urge the CCNR to promote the further development of **digitisation, automation and other modern technologies**, thus contributing to the competitiveness, safety and sustainability of inland navigation.”

**Digital Inland Waterway Area (DINA)**

“This research has identified three areas where digitalisation is critically important for IWT: improvement of navigation and management of traffic, integration with other modes of transport (multimodal hubs), reduction of the administrative burden.  

**Climate vision communication**

“A more efficient organisation of the entire mobility system based on **digitalisation, data sharing** and interoperable standards is of utmost importance to make mobility cleaner. 
COM(2018) 773 final

Inland navigation’s exposure to cyber threats will increase
European Collaboration - Why?

- small sector with few resources on national level
- typical small and medium enterprises
- highly international (in Rhine-Alpine corridor 50% of all cross-border freight transport)
- cross-border vessel traffic services (RIS)
- governance with international organisations
- regulation based on international legal instruments

European Collaboration - How?

Complement, not duplicate other activities and efforts
Learn from other modes of transport and from other safety domains
Be practical and strategic
European Collaboration - What?

➢ Raise awareness – f. e. PIANC TG 204 Report

➢ Explore preparedness – Ask national administrations

➢ Stimulate stakeholder exchange
  → Workshop 5 September 2019 in Bonn

➢ Develop and implement practical non-regret measures – f. e. guideline documents for administrations and enterprises

➢ Analyse entire sector – f. e. gap analysis of regulations and standards

➢ Strategize – based on the measures above
European Collaboration - *Where?*

**European Committee for drawing up standards in the field of inland navigation**

- **A** Prepare and adopt standards in the field of information technology
- **B** Support proper implementation of standards in the field of RIS and in other fields of information technology
- **C** Provide advice and analysis on information technology standards (including RIS)
Key findings

- Cybersecurity increasing importance for safety and sustainability of inland navigation
- Inland navigation faced with significant and growing exposure to cyber threats
- Particularities of inland navigation (large volumes, small enterprises, cross border) requires tailored approach to cybersecurity

Key objectives

- Support European collaboration to mitigate cyber risks for inland navigation
- Develop regulatory and administrative framework to keep inland navigation running when major ICT systems are compromised
Thanks for your attention!

Gernot Pauli  g.pauli@ccr-zkr.org  www.ccr-zkr.org
Chefingenieur  Tel.: +33 3 88 52 20 10  www.cesni.eu