United Nations ECE/TRANS/SC.3/2021/3

Economic and Social Council

Distr.: General
28 October 2021
English
Original: English, French and Russian

Economic Commission for Europe

Inland Transport Committee

Working Party on Inland Water Transport

Sixty-fifth session
Geneva, 3–5 November 2021
Item 4 of the provisional agenda
Workshop "Cybersecurity in inland water transport"

Workshop "Cybersecurity in inland water transport"

Note by the secretariat*, **

I. Mandate

1. This document is submitted in line with the Proposed Programme Budget for 2021, part V, Regional cooperation for development, section 20, Economic Development in Europe. Programme 17, Economic Development in Europe (A/75/6 (Sect.20), para. 20.51).

2. At its sixty-fourth session (ECE/TRANS/SC.3/213, para. 87), the Working Party on Inland Water Transport (SC.3) decided that the theme topic for its sixty-fifth session would be cybersecurity in inland water transport.

3. The present document provides a brief overview of the regulatory framework for cybersecurity in maritime and inland shipping, the activities of the Economic Commission for Europe (ECE) in this field and the topics proposed for discussion at the workshop.

II. Overview of the regulatory framework

4. Cyber security is a fast-growing challenge within the inland water transport community, since the digitalization of the sector is progressing rapidly, in order to succeed in the digital transition of inland navigation. Furthermore, there is a strong need to raise cybersecurity awareness, develop the concepts of cyber resilience to ensure the continuity of service in inland navigation and minimize the risks that impact the reliability of inland navigation's digital environment. Policy Recommendation No. 8 of the White Paper on the Progress, Accomplishments and Future of Sustainable Inland Water Transport stresses the need to develop cooperation between the key stakeholders at the international level and build on the experience and good practice of other transport modes and proposes concrete actions for ECE in this field.

* The present document was submitted after the deadline in order to reflect the most recent information.
** The present document is being issued without formal editing.

5. Given the growing importance of cybersecurity and the need for a pragmatic and practical approach to dealing with cyber threats, regulations and standards have been adopted in this field at the national and international level, such as:

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- Standard ISO/IEC 27001 “Information Security Management”
- Cybersecurity Framework 2018 of the National Institute of Standards and Technology (NIST) of the Department of Commerce of the United States of America.

6. In the maritime sector, the main regulatory framework for cybersecurity has been laid down by IMO in:

- Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3), approved in 2017. The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities
- Resolution MSC.428(98) “Maritime Cyber Risk Management in Safety Management Systems”, adopted by the Maritime Safety Committee in 2017. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems in accordance with the objectives and requirements of the International Safety Management Code no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

7. The IMO regulations have been further developed and supported by a number of guidelines and recommendations such as:

- Port Cybersecurity – Good practices for cybersecurity in the maritime sector (November 2019) and Guidelines – Cyber Risk Management for Ports (December 2020) of the European Union Agency for Cybersecurity (ENISA)
- Guidelines on Cyber Security Onboard Ships, version 4 (December 2020), published by BIMCO, Chamber of Shipping of America, Digital Container Shipping Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of Marine Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association and World Shipping Council
- Cybersecurity Guidelines for Ports and Port Facilities by the International Association of Ports and Harbors (IAPH) (September 2021)
- Recommendation on Cyber Resilience (No. 166) of the International Association for Classification Societies (IACS) (July 2020).

8. In the field of inland navigation, the World Association for Waterborne Transport Infrastructure (PIANC) issued in 2019 the Awareness Paper on Cybersecurity in Inland Navigation.

III. Activities of the Economic Commission for Europe in the field of cybersecurity

9. The World Forum for Harmonization of Vehicle Regulations (WP.29) adopted in June 2020 the UN Regulation on Cyber Security and Cyber Security Management Systems, which entered into force enter into force in January 2021. The Regulation provides a framework for the automotive sector to put in place the necessary processes to:

- Identify and manage cyber security risks in vehicle design
- Verify that the risks are managed, including testing
- Ensure that risk assessments are kept current

- Monitor cyber-attacks and effectively respond to them
- Support analysis of successful or attempted attacks
- Assess if cyber security measures remain effective in light of new threats and vulnerabilities.

10. In 2017, the Working Party on Regulatory Cooperation and Standardization Policies (WP.6) approved the proposal for a new sectoral initiative on cybersecurity. This sectoral initiative is aimed to promote the convergence of national technical regulations in this field towards a shared framework on the basis of a risk-based approach and other international best practices.

IV. Purpose of the workshop and topics for discussion

11. In accordance with Policy Recommendation No. 8 of the White Paper on the Progress, Accomplishments and Future of Sustainable Inland Water Transport, the purpose of the workshop is to raise awareness of cyber security, the recent progress, the ongoing work and opportunities in this field, share experience and highlight the best practices of other modes of transport that could be relevant for inland water transport.

12. Proposed topics for discussion at the workshop are:

(a) Best practice and lessons learned from the maritime sector;

(b) Opportunities for inland water transport;

(c) Cybersecurity in automated and autonomous navigation;

(d) Assessment of cybersecurity risks and mitigation actions in inland navigation;

(e) Measures that could be undertaken and the international and national level and the development of cooperation in this field.

13. SC.3 may wish to have a discussion on the realization of actions related to cyber security proposed under Policy Recommendation No. 8 of the White Paper on the Progress, Accomplishments and Future of Sustainable Inland Water Transport.