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

Conseil économique et social

Distr. générale
28 octobre 2021
Français
Original : anglais, français et russe

Commission économique pour l'Europe

Comité des transports intérieurs

Groupe de travail des transports par voie navigable

Soixante-cinquième session
Genève, 3–5 novembre 2021
Point 4 de l'ordre du jour provisoire
Atelier sur la cybersécurité dans le transport par voie navigable

Atelier sur la cybersécurité dans le transport par voie navigable

Note du secrétariat*, **

Mandat

1. Le présent document est soumis conformément au projet de budget-programme pour 2021, titre V (Coopération régionale pour le développement), chapitre 20 (Développement économique en Europe), programme 17 (Développement économique en Europe) (A/75/6, sect. 20, par. 20.51).

2. Lors de sa soixante-quatrième session (ECE/TRANS/SC.3/213, par. 87), le Groupe de travail des transports par voie navigable (SC.3) a décidé que le thème de sa cinquante-neuvième session serait la cybersécurité dans le transport par voie navigable.

3. Le présent document donne un bref aperçu du cadre réglementaire pour la cybersécurité dans la navigation maritime et intérieure, les activités de la Commission économique pour l'Europe (CEE) dans ce domaine et les sujets proposés pour la discussion lors de l'atelier.

II. Aperçu du cadre réglementaire

4. La cybersécurité est un défi en pleine croissance au sein de la communauté de navigation intérieure, car la numérisation du secteur progresse rapidement, pour réussir la transition numérique. En outre, il est impératif de sensibiliser le public concerné sur ce sujet, de développer les concepts de la cyber-résilience pour assurer la continuité du service en navigation intérieure et minimiser les risques affectant la fiabilité de l'environnement numérique. La recommandation nº 8 du Livre blanc sur les progrès, les succès et les perspectives d'avenir dans le transport par voie navigable souligne la nécessité de développer

* Le présent document est soumis après la date prévue pour que l'information la plus récente puisse y figurer.

** Le présent document n'a pas été revu par les services d'édition.

la coopération entre les acteurs clés au niveau international et de s'appuyer sur l'expérience et les bonnes pratiques des autres modes de transport et elle propose des actions concrètes pour la CEE dans ce domaine.

5. Compte tenu de l'importance croissante de la cybersécurité et de la nécessité d'une approche pragmatique et pratique pour faire face aux cybermenaces, des règlements et des normes ont été adoptées dans ce domaine aux niveaux national et international, telles que :

- Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union
- Standard ISO/IEC 27001 « Management de la sécurité de l'information »
- Cybersecurity Framework 2018 (Le cadre de cybersécurité 2018) du National Institute of Standards and Technology (NIST) du Département du Commerce des États-Unis d'Amérique.

6. Dans le secteur maritime, le principal cadre réglementaire de la cybersécurité a été défini par l'OMI dans les documents suivants :

- Directives sur la gestion des cyber-risques maritimes (MSC-FAL.1/Circ.3) adoptées en 2017. Ces Directives fournissent des recommandations de haut niveau sur la gestion des cyber-risques maritimes visant à protéger les transports maritimes contre les cybermenaces et vulnérabilités actuelles et émergentes
- Résolution MSC.428(98) « Gestion des cyber-risques maritimes dans le cadre des systèmes de gestion de la sécurité » adoptée par le Comité de la sécurité maritime en 2017. La résolution encourage les administrations à veiller à ce que les cyber-risques soient traités de manière appropriée dans les systèmes de gestion de la sécurité existants conformément aux objectifs et aux exigences du Code international de gestion de la sécurité au plus tard lors de la première vérification annuelle du document de conformité de l'entreprise après le 1er janvier 2021.

7. Les règlements de l'OMI ont été développés et soutenus par un certain nombre de directives et de recommandations telles que :

- Port Cybersecurity – Good practices for cybersecurity in the maritime sector (Cybersécurité portuaire – Bonnes pratiques de cybersécurité dans le secteur maritime) (novembre 2019) et Guidelines – Cyber Risk Management for Ports (Lignes directrices – Gestion des cyber-risques pour les ports) (décembre 2020) de l'Agence européenne pour la cybersécurité (ENISA)
- Directives sur la cybersécurité à bord des navires, publiées par BIMCO, Chamber of Shipping of America, Digital Container Shipping Association, Association internationale des transporteurs de marchandises solides (INTERCARGO), InterManager, Association internationale des armateurs pétroliers indépendants (INTERTANKO), Chambre internationale de la marine marchande (ICS), Union internationale d'assurances transports (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association et World Shipping Council
- Lignes directrices sur la cybersécurité pour les ports et les installations portuaires par l'Association internationale des ports (IAPH) (septembre 2021)
- Recommandation sur la cyber-résilience (n° 166) de l'Association internationale des sociétés de classification (IACS) (juillet 2020).

8. Dans le domaine de la navigation intérieure, l'Association mondiale pour les infrastructures de transport maritimes et fluviales (AIPCN) a publié en 2019 le document « Awareness Paper on Cybersecurity in Inland Navigation » (document d'information sur la cybersécurité en navigation intérieure).

III. Activités de la Commission économique pour l'Europe dans le domaine de la cybersécurité

9. En juin 2020, le Forum mondial de l'harmonisation des règlements concernant les véhicules (WP.29) a adopté le Règlement ONU sur la cybersécurité et les systèmes de gestion de la cybersécurité, qui est entré en vigueur en janvier 2021. Le règlement fournit un cadre permettant au secteur automobile de mettre en place les processus nécessaires pour :

- Identifier et gérer les risques de cybersécurité dans la conception des véhicules
- Vérifier que les risques sont gérés, y compris les tests
- Veiller à ce que les évaluations des risques soient tenues à jour
- Surveiller les cyber-attaques et y répondre efficacement
- Soutenir l'analyse des attaques réussies ou des tentatives d'attaques
- Évaluer si les mesures de cybersécurité restent efficaces compte tenu des nouvelles menaces et vulnérabilités.

10. En 2017, le Groupe de travail des politiques de coopération en matière de réglementation et de normalisation (WP.6) a approuvé la proposition relative à une nouvelle initiative sectorielle sur la cybersécurité. Cette initiative sectorielle vise à favoriser la convergence des réglementations techniques nationales dans ce domaine vers un cadre commun sur la base d'une approche fondée sur les risques et d'autres bonnes pratiques internationales.

IV. Objectif de l'atelier et sujets de discussion

11. Conformément à la recommandation n° 8 du Livre blanc sur les progrès, les succès et les perspectives d'avenir dans le transport par voie navigable, l'objectif de l'atelier est de sensibiliser à la cybersécurité, aux progrès récents, aux travaux en cours et aux opportunités dans ce domaine, de partager les expériences et de mettre en avant les bonnes pratiques d'autres modes de transport qui pourraient être pertinentes pour le transport par voie navigable.

12. Les sujets proposés pour la discussion lors de l'atelier sont les suivants :

a) Bonnes pratiques et enseignements tirés du secteur maritime ;

b) Perspectives pour le transport par voie navigable ;

c) Cybersécurité dans la navigation automatisée et autonome ;

d) Évaluation des cyber-risques et mesures d'atténuation dans le domaine de la navigation intérieure ;

e) Mesures qui pourraient être prises au niveau international et national et le développement de la coopération dans ce domaine.

13. Le SC.3 souhaitera peut-être avoir une discussion sur la réalisation des actions liées à la cybersécurité proposées dans la recommandation n° 8 du Livre blanc sur les progrès, les succès et les perspectives d'avenir dans le transport par voie navigable.