

PROGRAMME | BONN | 5 SEPTEMBRE 2019

ATELIER CONSACRÉ À LA CYBERSÉCURITÉ EN NAVIGATION INTÉRIÈRE

Lieu: Ministère fédéral allemand du transport et de l'infrastructure numérique (BMVI),
Robert-Schuman-Platz 1, Salle 0.105 (et 0.121), 53175 Bonn, Allemagne

Présidence : Nils Braunroth, Adjoint au chef de bureau (BMVI)
Langues de travail : français, allemand, néerlandais, anglais

9:00 *Inscription et café de bienvenue*

10:00 **Ouverture de l'atelier par la Présidence** (salle 0.105)
Nils Braunroth

10:10 **Introduction**
Achim Wehrmann Président de la CCNR, Allemagne
Geert Van Cappellen Secrétaire général, AIPCN

10:25 **Politiques et mesures de soutien de l'UE pour la cybersécurité en navigation intérieure**
Nineta Polemi Responsable de programme, Commission européenne, DG CNCT

Cybermenaces et cybersécurité - Conseils et soutien de l'ENISA pour le transport par voies d'eau
Athanasios Drougkas Expert en sécurité des réseaux et de l'information, ENISA

11:00 **Introduction aux sessions 1 et 2**
Nils Braunroth

11:10 *Pause-café*



Atelier consacré à la cybersécurité en navigation intérieure

SESSION 1 : administration publique (salle 0.105)

11:30 **Collaboration européenne dans le domaine de la cybersécurité ferroviaire - Bonne pratique pour la navigation intérieure ?**

Christian Schlehuber, Expert cybersécurité,
DB Netz AG

**Service d'information fluviaux, e-navigation, ...
Un aperçu des TIC dans la navigation intérieure
vulnérables aux cybermenaces**

Dierik Vermeir, Vice-président du groupe
WG 125, AIPCN ; Président et CEO, ALSIC BVBA

**Le défi de la sécurité informatique : Effets sur le
fonctionnement des infrastructures critiques de la
navigation intérieure ?**

Reinhard Zimmermann, Directeur général,
in-innovative navigation GmbH

**Les mesures d'une autorité de navigation en matière
de cybersécurité - L'exemple de l'Allemagne**

Alan Jacobsen, Responsable de la sécurité
informatique pour l'ingénierie du trafic,
Direction générale des voies navigables et de
la navigation

13:10 *Pause déjeuner*

14:30 **Table ronde « Conclusions et recommandations
du point de vue de l'administration publique »**

- Daniel Arzani, Office fédéral de la sécurité
des technologies de l'information (BSI)
- Christian Schlehuber, DB Netz AG
- Geert Van Cappellen, AIPCN
- Bernd Birkhuber, BMVIT

15:30 *Plénière (salle 0.105)*

Rapports de synthèse des sessions 1 et 2

16:00 **Que faire à ce stade ?**

Nils Braunroth

16:30 *Fin de l'atelier*

SESSION 2 : secteur privé (salle 0.121)

Social Engineering - Accent porté sur l'être humain

Urs Maurer, Expert suisse de la CCNR ;
Collaborateur scientifique, Office fédéral des
transports

**Cybermenaces et cybersécurité en navigation
intérieure - L'expérience d'un opérateur de terminal
et d'utilisateur des voies navigables**

Heinrich Kerstgens, Directeur général, Contargo

**Mesures pratiques relatives à la cybersécurité des
entreprises de navigation intérieure**

Bernd Dettmers, Directeur,
net.e Network Experts

**Cybersécurité des navires - Les exigences
techniques sont-elles suffisantes et sur quelles
bases peuvent-elles être améliorées ?**

Laurent Banitz, Chef de la mission Sécurité
des navires et cybersécurité,
Direction générale des infrastructures, des
transports et de la mer

**Les cyber-risques du point de vue d'une société de
classification**

Svante Einarsson, Consultant principal en
cybersécurité, DNV GL

Pause déjeuner

**Table ronde « Conclusions et recommandations
du point de vue du secteur privé »**

- Sven Daniels, HPC Hambourg
- Athanasios Drougkas, ENISA
- Heinrich Kerstgens, Contargo
- Peter Spomer, Lloyds Register

