

ATELIER CONSACRÉ À LA CYBERSÉCURITÉ EN NAVIGATION INTÉRIEURE

Ref: CC/CP (19)05



Bonn, le 5 septembre 2019 – Le 5 septembre 2019 s'est tenu dans la ville rhénane de Bonn le premier atelier international consacré à la cybersécurité en navigation intérieure, sous l'égide de la [Commission centrale pour la navigation du Rhin](#) (CCNR) et en partenariat avec le [Ministère fédéral allemand du transport et de l'infrastructure numérique](#) (BMVI) et l'[AIPCN](#). Onze présentations de haute qualité et deux tables rondes passionnantes ont permis de souligner à l'intention de plus d'une centaine de participants issus d'institutions et organisations publiques et privées la nécessité pour tous les acteurs du transport fluvial de relever les défis complexes en matière de cybersécurité, afin de réussir la transition numérique de la navigation intérieure. L'atelier a également permis à la CCNR de recueillir de nombreux enseignements, conseils et propositions concrètes pour ses travaux futurs sur la cybersécurité en navigation intérieure.

Dans leur [déclaration](#) adoptée à Mannheim le 17 octobre 2018, les Ministres des États membres de la CCNR appellent à promouvoir le développement de la numérisation, de l'automatisation et d'autres technologies modernes afin de contribuer ainsi à la compétitivité, à la sécurité et au développement durable de la navigation intérieure. Dans ce contexte, l'atelier consacré à la cybersécurité en navigation intérieure visait plus particulièrement à renforcer le niveau d'information des différents acteurs de la navigation intérieure en matière de cybersécurité, tout en favorisant les échanges et la coopération entre les différents acteurs du secteur. Il était en effet fondamental d'engager une réflexion coordonnée et de trouver un consensus sur la manière d'atténuer les risques susceptibles d'affecter la fiabilité de l'environnement numérique de la navigation intérieure.

M. Achim Wehrmann, président de la CCNR et Directeur du Sous-département Navigation au sein du ministère fédéral allemand des transports et de l'infrastructure numérique, a souhaité la bienvenue aux participants dans les locaux du BMVI. Dans son allocution, il a souligné que la navigation intérieure doit être bien positionnée en termes de cybersécurité pour bénéficier des avantages de la numérisation.

Il a également invité les participants à soumettre à la CCNR de nombreuses suggestions sur le thème de la cybersécurité en navigation intérieure. M. Geert Van Cappellen, secrétaire général de l'AIPCN, s'est déclaré convaincu, dans son allocution de bienvenue, que la navigation intérieure sera en mesure de gérer les risques informatiques si elle coopère au niveau international. L'événement a permis de réunir pour la première fois des acteurs majeurs dans le domaine de la cybersécurité – dont la [Commission européenne](#) (DG CONNECT) et l'[Agence européenne chargée de la sécurité des réseaux et de l'information](#) (ENISA) ainsi que des représentants du secteur maritime et ferroviaire –, des experts en matière de navigation intérieure d'administrations publiques, de sociétés de classification et d'entreprises privées de onze pays européens.

Fort de présentations générales sur les différents aspects de la cybersécurité, de sessions dédiées au secteur public et privé et de véritables échanges sous forme de table-rondes, l'atelier a confirmé l'importance de la cybersécurité en navigation intérieure. Les intervenants et participants ont mené une réflexion approfondie sur les mesures envisageables. Au-delà d'un besoin fort en termes de sensibilisation, de formation et d'information des différents acteurs et usagers de la voie fluviale aux thèmes de la cybersécurité et des cyberattaques, le thème de la coopération a été plus particulièrement mis en avant. Mettre en place des solutions communes et standardisées, fruit d'échanges entre les différentes parties prenantes à l'échelle internationale, au niveau du secteur public et privé, au niveau des constructeurs et des exploitants, etc. est en effet essentiel. À cet effet, la navigation intérieure pourra notamment s'appuyer sur l'expérience et les bonnes pratiques du secteur maritime et ferroviaire. Les acquis de l'ENISA, dans le soutien à la mise en œuvre de la « [Directive NIS](#) » (Directive européenne concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information), seront également précieux pour le développement d'un concept de cybersécurité en navigation intérieure.

À PROPOS DE LA CCNR

La Commission centrale pour la navigation du Rhin (CCNR) est une organisation internationale exerçant un rôle réglementaire essentiel pour l'organisation de la navigation sur le Rhin. Elle intervient dans les domaines technique, juridique, économique, social et environnemental. Dans l'ensemble de ses domaines d'action, l'efficacité du transport rhénan, la sécurité, les considérations sociales ainsi que le respect de l'environnement dirigent ses travaux. Au-delà du Rhin, de nombreuses activités de la CCNR concernent aujourd'hui les voies navigables européennes au sens large. Elle travaille étroitement avec la Commission européenne, ainsi qu'avec les autres commissions fluviales et institutions internationales.

De nombreux participants ont exprimé le souhait que la CCNR, avec le soutien de ses partenaires, assume un rôle moteur et central dans le domaine de la cybersécurité en navigation intérieure, par exemple en tant que plateforme de coordination réunissant à la fois les acteurs majeurs de la navigation intérieure et des experts en cybersécurité. Les questions relatives à la cybersécurité devront faire l'objet d'une analyse approfondie dans le cadre du nouveau groupe de travail du [Comité européen pour l'élaboration de standards dans le domaine de la navigation intérieure](#) (CESNI) consacré aux technologies de l'information (CESNI/TI). En outre, l'ENISA s'est déclarée disposée à soutenir les travaux futurs liés à la cybersécurité en navigation intérieure.

Au terme de l'atelier, M. Nils Braunroth, président du CESNI/TI et de l'atelier a remercié l'ensemble des intervenants et participants pour leur engagement et pour les informations, conclusions et recommandations recueillies. La CCNR en tiendra compte et, dans un premier temps, mettra à disposition les présentations de l'atelier et des documents de référence sur le thème de la cybersécurité via le lien suivant : <http://cybersecurityworkshop-inlandnavigation.evenium-site.com>. Un compte rendu détaillé de l'atelier et d'autres communications sur la cybersécurité en navigation intérieure y seront également disponibles dans les semaines à venir.



CCNR

COMMISSION CENTRALE
POUR LA NAVIGATION DU RHIN

Palais du Rhin
2, place de la République - CS10023
F - 67082 Strasbourg Cedex

Tél. +33 (0)3 88 52 20 10
Fax +33 (0)3 88 32 10 72

ccnr@ccr-zkr.org
www.ccr-zkr.org