PRESS RELEASE

January 11, 2019

NEW PIANC PUBLICATION AVAILABLE

PIANC
The World Association for Waterborne Transport Infrastructure

PIANC

InCom Task Group n° 204 - 2019

AWARENESS PAPER ON CYBERSECURITY IN INLAND NAVIGATION

The World Association for Waterborne Transport Infrastructure

Title:	**'Awareness Paper on Cybersecurity in Inland Navigation'**
Authors:	PIANC InCom Task Group 204
Price:	35 pages - € 40.00
Available at:	https://www.pianc.org/publications/inland-navigation-commission/tg204

Since the end of the last century, the number and the complexity of navigational and information equipment on inland navigation vessels and for inland navigation infrastructure have increased dramatically. ICT is transforming shipping, bringing enhanced monitoring, communication and connection capabilities and thereby facilitating the development of new generations of intelligent transport systems, including automated inland navigation vessels.

According to the Terms of Reference established by the Inland Navigation Commission of PIANC (InCom) for Task Group 204 (TG 204) on 18 September 2017, this awareness paper provides an overview and stimulates feedback on the cyberrisks for inland navigation including its infrastructure, and on mitigating measures, taking into account work in neighbouring fields, such as maritime transport and ports management. The pursued objective is to raise awareness for cybersecurity in inland navigation among practitioners in the management of inland waterways, ports, as well as shipping companies. This paper also contains some recommendations for follow-up of these activities under the umbrella of PIANC.

This paper responds to the Terms of Reference (ToR) established by the Inland Navigation Commission of PIANC (InCom) for Task Group 204 (TG 204) on 18 September 2017. Accordingly, it is intended to provide an overview and stimulate feedback on the cyberrisks which apply to inland navigation, and mitigating measures, taking into account work in neighbouring fields such as maritime transport and ports management. The authors hope that the paper and the responses it elicits will raise awareness for cybersecurity in inland navigation among practitioners in the management of inland waterways, ports as well as shipping companies and that it will allow for an informed decision about a possible follow-up, in particular setting up a PIANC Working Group on cybersecurity.

Many guides are available on how to carry out good, general cyberrisk management. The US National Institute of Standards and Technology (NIST) Framework for Infrastructure Cybersecurity[1] provides a method to analyse the features of any system with a view to improving cybersecurity and perhaps most widely cited.

This paper, however, seeks to focus on risks specific to the inland water transport sector defined widely (as per the ToR) as the complex system, including vessels, waterways, ports, shipping companies and cargo, linked by ICT services (such as RIS).

The paper is not intended to give a comprehensive inventory of technologies, threats and mitigation measures – rather an appreciation of the salient issues being discussed in the industry. For any individual operator a proper cyberrisk assessment would be needed. This is discussed at the end of the paper.

NOTE: The objective of this guidance is to provide information and recommendations on good practice. Conformity is not obligatory and engineering judgement should be used in its application, especially in special circumstances. This report should be seen as an expert guidance and state of the art on this particular subject. PIANC disclaims all responsibility in case this report should be presented as an official standard.