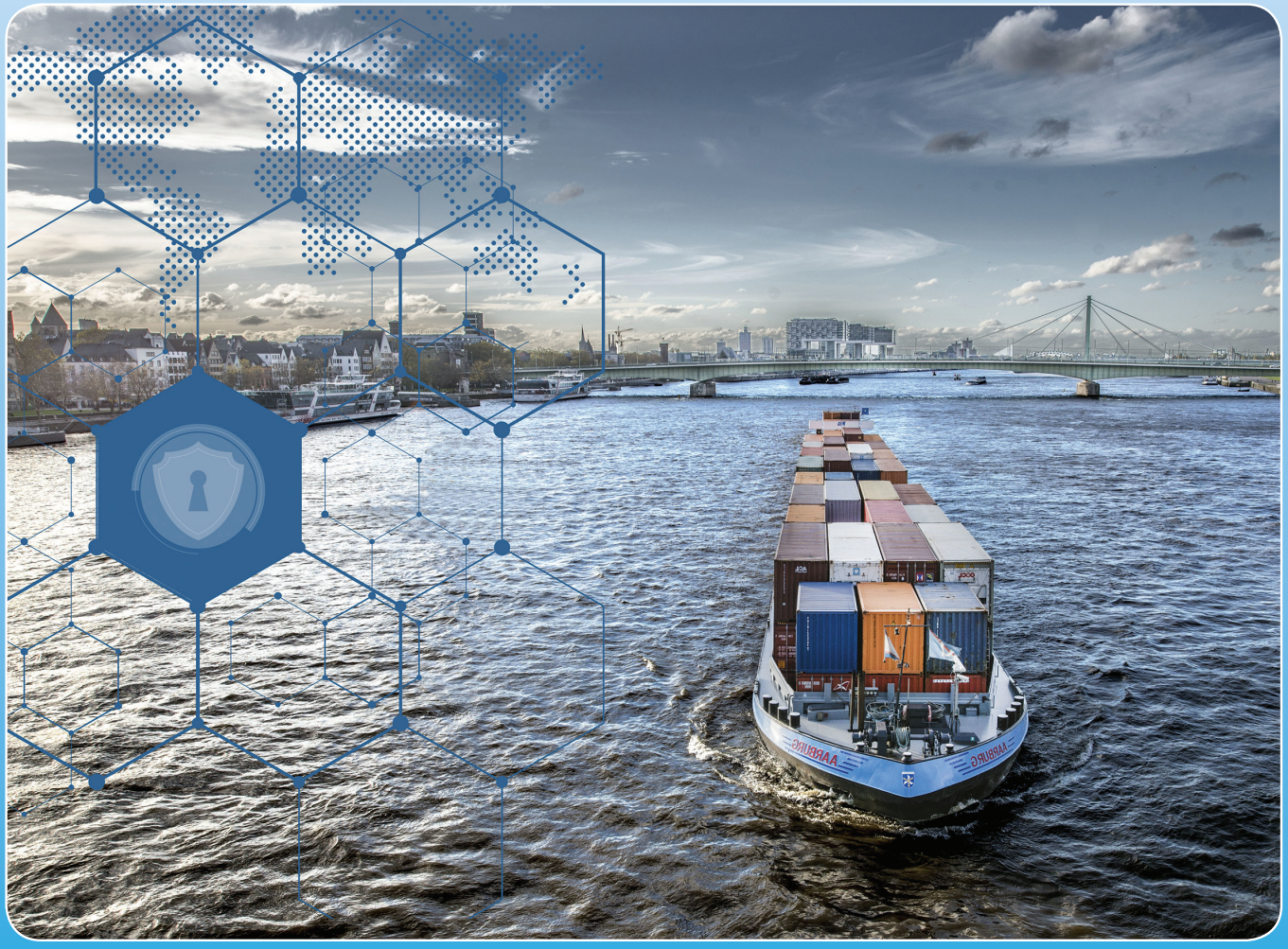
PIANC

InCom Task Group
n° 204 - 2019



AWARENESS PAPER ON CYBERSECURITY IN INLAND NAVIGATION

The World Association for Waterborne Transport Infrastructure

PIANC

The World Association for Waterborne Transport Infrastructure

PIANC TASK GROUP N° 204

INLAND NAVIGATION COMMISSION

AWARENESS PAPER ON CYBERSECURITY IN INLAND NAVIGATION

2019

PIANC has Technical Commissions concerned with inland waterways and ports (InCom), coastal and ocean waterways (including ports and harbours) (MarCom), environmental aspects (EnviCom) and sport and pleasure navigation (RecCom).

This report has been produced by an international Working Group convened by the Inland Navigation Commission (InCom). Members of the Working Group represent several countries and are acknowledged experts in their profession.

The objective of this report 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 the event that this report should be presented as an official standard.

PIANC Secrétariat Général
Boulevard du Roi Albert II 20, B 3
B-1000 Bruxelles
Belgique

http://www.pianc.org

VAT BE 408-287-945

ISBN 978-2-87223-259-8

SUMMARY

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.

TABLE OF CONTENTS

1 GENERAL ASPECTS 3
1.1 Purpose 3
1.2 Scope 3
1.2.1 Malicious Attack, Not Accidental Failure 3
1.2.2 Risk of Economic Loss or Environmental Damage (But Only Where Industry-Specific Networks Are Involved) 3
1.2.3 Sources and Methods of Attack 4
1.3 Structure 5
2 WIDER CONTEXT: CYBERPREPAREDNESS ACROSS INDUSTRY 6
2.1 In the Economy as a Whole, Organisations are not Considered Adequately Prepared to Deal with Cyberthreats 6
2.2 Shipping Industry Behind Others 6
2.3 Complexity of ICT Systems within the Shipping Industry is a Recurrent Theme – Preference for Risk-Management Approach 6
2.4 Difficulty in Identifying Patterns of Risk on a System-By-System Basis 7
2.5 A Fragmented Governance/Regulatory Picture 7
2.6 Growing Concerns Regarding Data Protection 8
3. SYSTEMS CURRENTLY IN USE, CYBERRISKS AND MITIGATION MEASURES 9
3.1 Systems Currently in Use 9
3.2 General Aspects of Risk and Mitigation 9
3.3 Vessel Control 10
3.3.1 Extensive Use of SCADA Systems 10
3.3.2 Mitigation for SCADA Systems 11
3.4 Navigation 11
3.4.1 Position, Speed, Heading and Other Data About Vessels 11
3.4.2 GNSS 12
3.4.3 Mitigation for GNSS 12
3.4.5 AIS 13
3.4.6 Mitigation for AIS 14
3.4.7 ECDIS 15
3.4.8 Mitigation for ECDIS 15
3.4.9 Radar 16
3.4.10 Mitigation for Radar 17
3.4.11 Electronic Ship Reporting in Inland Navigation (ERI) and Notices to Skippers for Inland Navigation (NtS) 17
3.4.12 Web/Database Servers 18
3.5 Infrastructure Control Systems 18
3.5.1 River Infrastructure Systems such as Lock and Bridge Management (LBM) 18
3.5.2 Traffic Planning 18
3.6 Information Reporting/Exchange 19
3.7 Network/Communication Systems 19
3.7.1 On-Board LAN or Other Networks 19
3.7.2 Bespoke Industry Web Portals 19
3.7.3 Distributed Devices 20
4. POSSIBLE FUTURE TECHNOLOGIES AND RISKS 21
4.1 Future Technologies 21
4.1.1 Automated/Autonomous Vessels: e.g. NOVIMAR Platoons 21
4.1.2 Digital Inland Waterway Area and Digital Multimodal Nodes 21
4.2 Future Risks 21
5. RECOMMENDATIONS FOR FOLLOW-UP 23
ANNEX I – Task Group Terms of reference 25
ANNEX II – TASK Group Members 29
ANNEX III – GLOSSARY 30