

CYBERSECURITY IN INLAND NAVIGATION

PIANC AWARENESS PAPER



RIS WEEK December 2018

Jean-Noël Schilling





Content

Introduction

Our Reliance on Information technology

PIANC Risk Awareness Paper

Next Steps

CCNR's role

Aiming at further Improving and harmonising inland navigation standards and regulations.

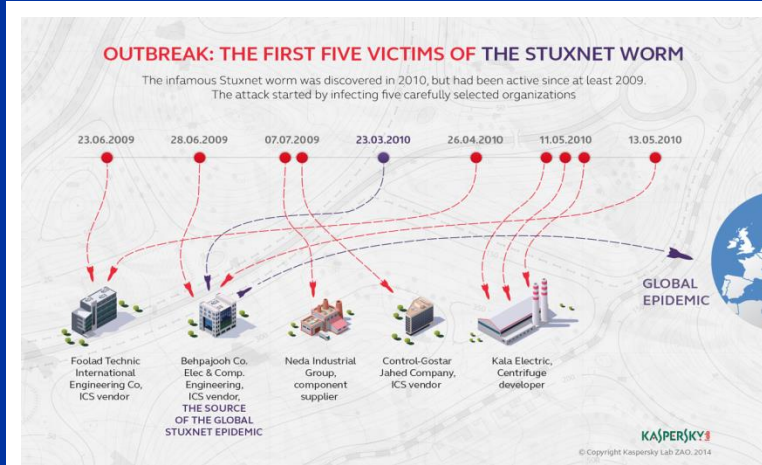
The safety of persons and goods in navigation activities is a longstanding concern which, however, requires ongoing adaptation of standards.



SAFETY

CYBERSECURITY

Cyber-threats are real



Protecting GPS From Spoofers Is Critical to the Future of Navigation

GPS is vulnerable to spoofing attacks. Here's how we can defend these important navigation signals

By Mark L. Psiaki and Todd E. Humphreys

Just hours before U.S. president Barack Obama delivered his final State of the Union speech in January, two U.S. Navy patrol boats wandered into Iranian waters. The Iranian military intercepted the vessels and captured 10 U.S. sailors, making for



SPIEGEL ONLINE

Hafen von Antwerpen Hacker halfen Drogenschugglern beim Containerklau

Europol hat gemeinsam mit der belgischen Polizei eine Bande von Drogenschugglern zerschlagen. Die Täter gingen äußerst raffiniert zu Werke: Sie versteckten ihre Fracht in fremden Containern - und engagierten Hacker, um diese Container im Hafen von Antwerpen wiederzufinden.



Hafen von Antwerpen: Container voller Drogen

Le Monde

Les 10 nuits en enfer de Maersk pour réinstaller 4000 serveurs et 45000 PC

Sécurité : Le transporteur a été frappé de plein fouet en 2017 par le ransomware NotPetya



MAERSK CASE STUDY



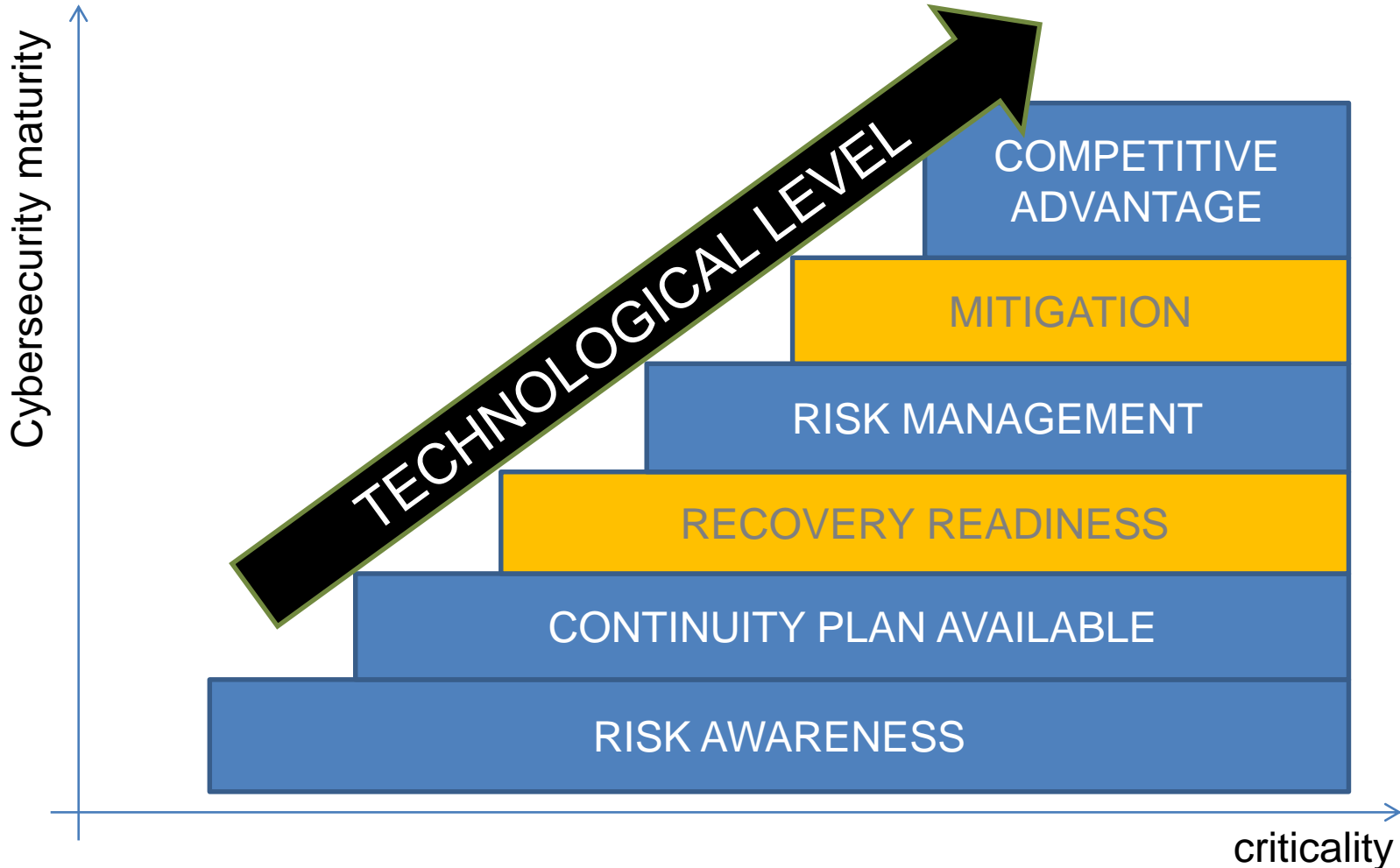
We are sorry but maerskline.com is temporarily down.

We confirm that some Maersk IT systems are down. We are working on this as quickly as possible. The safety of your business and our people is our top priority. We will provide you with more information as soon as we have it.

We apologize for any inconvenience this may cause. Thank you for your patience.
Maersk Line team



Reliance on Information Technology





FIRST STEP



RISK AWARENESS



PIANC
The World Association
Waterborne Transport Infrastr...

1

SYSTEMS
CURRENTLY IN USE

2

FUTURE
TECHNOLOGIES

3

RECOMMENDATIONS
FOR FOLLOW UP

Report No. 100
AWARENESS PAPER
**CYBERSECURITY IN INLAND
NAVIGATION**



RISK AWARENESS

- On-board systems
Controls
Navigations

SYSTEMS
CURRENTLY IN USE

- Infrastructure systems
Controls
Lock and bridge management
Traffic planning

- Servicing systems
Web portals
Distributed services

RISK
CASE
STUDIES



RISK AWARENESS

- Automated / autonomous Vessels
- Digital Multimodal Nodes
- E-documents

The diagram features a large light blue rectangular area on the left containing a bulleted list of technologies. To the right of this area, a blue ribbon banner with the text 'FUTURE TECHNOLOGIES' is positioned horizontally. Below this banner, a large orange arrow points from a square box containing the text 'FUTURE RISKS ?' towards the light blue area. The arrow and box are positioned such that they appear to be pointing towards the 'Automated / autonomous Vessels' and 'Digital Multimodal Nodes' items in the list.

FUTURE
TECHNOLOGIES

FUTURE
RISKS ?

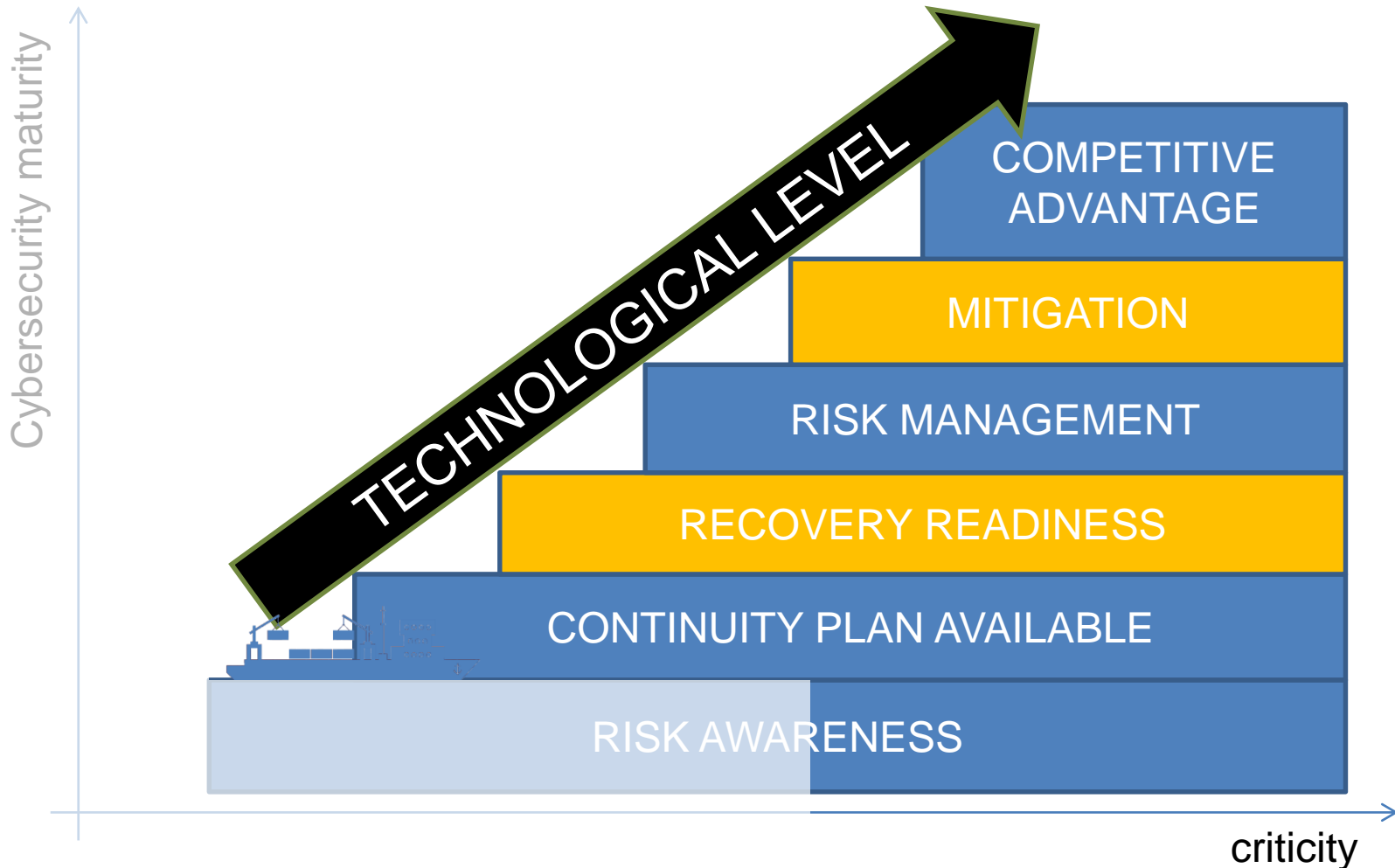


RISK AWARENESS

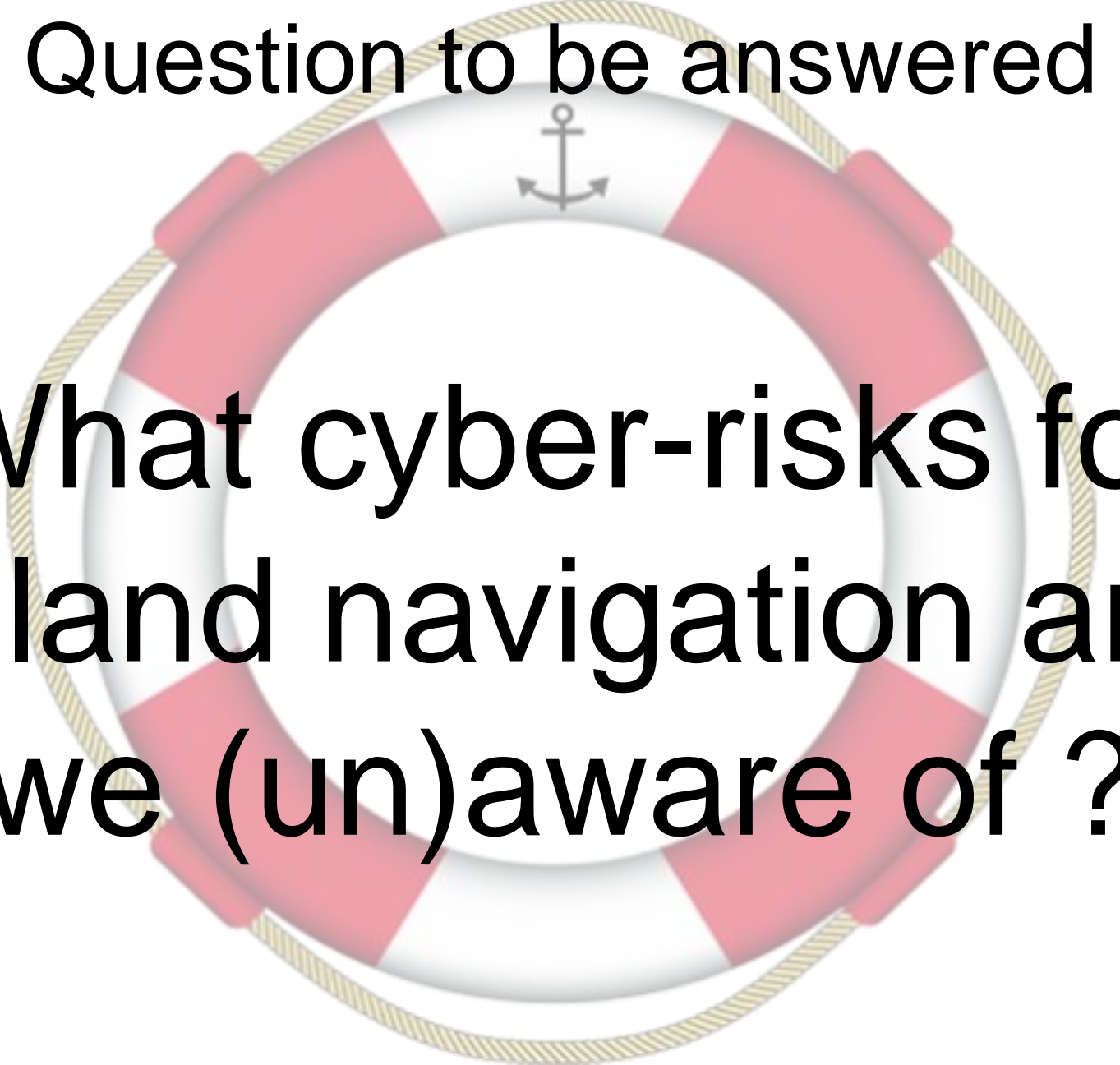
- Broaden the risk assessment
- Use all possible levers
- Promote Trainings and continuous learnings

RECOMMENDATIONS
FOR FOLLOW UP

Next steps



Question to be answered



What cyber-risks for inland navigation are we (un)aware of ?

CESNI 2019-21 work programme



Undertake technical and legal analysis and develop recommendations regarding cyber-risks and other safety risks for IT applications in inland navigation and provide proposals for concrete mitigation measures



2019 Workshop Cybersecurity

- Further Awareness supported by CS experts
- Draw a roadmap for cybersecurity
- Deliver and share good practices





We have created societies in the **physical world where we feel safe,**
We need to make sure that that **also happens in the digital World**

Jim Hagemann Snabe
CEO A.P. Møller-Mærsk
Tallinn Digital Summit keynote speech
September 2017



THANK YOU FOR YOUR ATTENTION

Jean-Noël Schilling

T +33 (0)3 88 52 45 20

jn.schilling@ccr-zkr.org