Input paper: [[1]](#footnote-1) ENAV18-12.14.1

Input paper for the following Committee(s): check as appropriate Purpose of paper:

**X** ARM **X** ENG **□** PAP x Input

**X** ENAV **X** VTS **□** Information

Agenda item [[2]](#footnote-2) 12

Technical Domain / Task Number 2 …………………………………

Author(s) / Submitter(s) A Grant

Cyber-attacks

# Summary

In general, the level of connectivity between different computerised systems, both on the vessel and ashore, is on the increase. Such connectivity enables more efficient use of data and allows for new services to be offered, especially when considering e-Navigation services. However, such interconnectivity also increases the threat of cyber-attacks, if sufficient security if not applied.

Cyber-attacks are when a third party either gains unauthorised access to (predominately computerised) systems and either disrupts the intended service, changes underlying data or prevent access altogether. These attacks can cause a loss of data integrity and/or a loss of service. Signal jamming and spoofing can be considered cyber-threats.

Governments and other bodies are working to raise awareness of the threat of cyber-attacks so that people are more aware and therefore able to prevent them where possible. In addition, there are a number of reports publically available which consider the potential for cyber-attacks on maritime systems, some of which are listed in the reference section below.

The aim of this paper is to raise awareness of cyber-attacks and to encourage IALA members to consider the potential vulnerabilities to their own systems and to consider such concerns when undertaking IALA work.

# References

The Committee may find the following references useful. Copies of these documents are attached for reference.

1. USCG cyber strategy (<https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf>)
2. European Network and Information Security Agency (ENISA), “Analysis of cyber security aspects in the maritime sector”, November 2011. (<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1>)
3. Guidelines on Cyber Security Onboard Ships, produced by BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO. These guidelines are due to be submitted to MSC 96 later this year for approval/adoption by IMO and have been provided by CIRM. The aim of this document is to offer guidance to shipowners and operators on how to assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems on board their ships.
4. Guidance Notes on The Application of Cybersecurity Principles to Marine and Offshore Operations (Volume 1: Cybersecurity). This document has been published by the American Bureau of Shipping, and provides information on cyber-security. This document was also provided by CIRM.

# Action requested of the Committee

The Committee is requested to:

* Be aware of the threat of cyber-attacks and to consider potential vulnerabilities to their own systems and when undertaking IALA work.

1. Input document number, to be assigned by the Committee Secretary [↑](#footnote-ref-1)
2. Leave open if uncertain [↑](#footnote-ref-2)