INTERNATIONAL MARITIME ORGANIZATION

E

FACILITATION COMMITTEE
39th session
Agenda item 7

FAL 39/7
10 July 2014
Original: ENGLISH

ENSURING SECURITY IN AND FACILITATING INTERNATIONAL TRADE

Measures toward enhancing maritime cybersecurity

Submitted by Canada

SUMMARY

Executive summary:	This document proposes the development of *Guidelines on maritime cybersecurity in light of the dramatic increases in the use of cyber systems across the maritime sector and related risks*
Strategic direction:	6.1
High-level action:	6.1.1
Planned output:	No related provision
Action to be taken:	Paragraph 11
Related document:	FAL 38/7

Introduction

1 This document recommends the development of voluntary guidelines on cybersecurity practices to protect and enhance the resiliency of cyber systems supporting the operations of ports, vessels, marine facilities and other elements of the maritime transportation system. For the purposes of this proposal, *cybersecurity* is defined as measures taken to protect cybersystems, or any data contained therein, against unauthorized access or alteration.

Discussion

2 There are numerous examples of cybersecurity issues of relevance to the maritime community:

.1 researchers from the University of Texas in the United States demonstrated in July 2013 that it is possible to change a vessel's direction by interfering with its GPS signal to cause the onboard navigation systems to falsely interpret a vessel's position and heading;

.2 a hacker caused a floating oil-platform located off the coast of Africa to tilt to one side, thus forcing it to temporarily shut down;

.3 hackers infiltrated cyber systems in a port to locate specific containers loaded with illegal drugs and remove them from the port undetected;

.4 Somali pirates employed hackers to infiltrate a shipping company's cyber systems to identify vessels passing through the Gulf of Aden with valuable cargoes and minimal on-board security which led to the hijacking of at least one vessel;

.5 denial of service attacks (initiating a very high number of requests to a system to overwhelm it and cause it to cease operating) against ports have been reported;

.6 efforts to gain unauthorized access to wireless Internet networks in ports have been reported; and

.7 studies by the Brookings Institution and the European Union Agency for Network and Information Security both concluded that there is very little awareness of cybersecurity issues in the maritime transportation sector and few initiatives underway to enhance cybersecurity.

3 As the global maritime community moves further into a digital environment, ports, vessels and facilities are increasingly connected to, and dependent on, cyber systems. This includes almost every facet of their operations, such as financial and human resources management, security systems, navigation, communications and the operation of key systems and equipment.

4 As industries worldwide have turned towards greater reliance on cybersystems, organized crime, state-sponsored hackers, terrorists and other malicious actors have turned towards exploiting weaknesses in cybersecurity to gain intelligence, facilitate illegal activities and cause economic and physical damage.

5 The maritime sector is not immune to these potential vulnerabilities. Unauthorized access or alteration of cybersystems could result in compromised strategic, proprietary, or personal information, exploitation of cybersystems for nefarious purposes, or temporary loss of, or damage to, critical systems. Insufficiently robust cybersecurity practices could therefore potentially lead to a loss of life, increased criminality in the maritime sector or, given the importance of the maritime sector to international trade and supply chains, an operational disruption with significant adverse economic consequences.

6 As part of consultations to further the development of a domestic Maritime Cybersecurity Strategic Framework, stakeholders informed the representatives of the Government of Canada of their desire for maritime cybersecurity guidelines to serve as both a guide and benchmark for their own cybersecurity efforts. Given the technical nature of cybersecurity and its rapid emergence as an area of concern, it is likely that maritime sector stakeholders worldwide are also seeking guidance on this issue.

Analysis of implications

7 Cybersystems containing sensitive or private information and/or controlling critical equipment or processes are potentially vulnerable to unauthorized access or alteration that could lead to information breaches, system failures, security compromises or other negative

consequences. Cybersecurity guidelines developed specifically for the maritime sector could help protect ports, terminals, vessels and other stakeholders, as well as help mitigate the effects of successful intrusions and prevent disruptions to international trade, by providing guidance on areas of cybersecurity.

8 The need for guidance materials on cybersecurity has grown with the use and reliance on cyber systems among maritime stakeholders. As the maritime transportation system carries approximately 90% of international commerce, a successful cyber attack against a maritime stakeholder could have significant negative effects on the global economy and disrupt international trade.

9 Specifically, it is recommended that the Committee develop voluntary guidelines on cybersecurity as it conforms to IMO's objectives of enhancing the security of the maritime transportation system and protecting human life at sea.

10 Information on the potential contents of the proposed cybersecurity guidelines is provided in the annex.

Action Requested of the Committee

11 The Committee is invited to develop voluntary guidelines on maritime cybersecurity. The Committee may wish to consider creating an intersessional correspondence group to conduct this work with the following initial work programme:

.1 identify relevant existing standards and guidance materials;

.2 develop voluntary maritime cybersecurity guidelines, including best practices; and,

.3 report to FAL 40.

***

ANNEX

POTENTIAL CONTENTS OF THE CYBERSECURITY GUIDELINES

1 The proposed voluntary maritime cybersecurity guidelines could include:

.1 A description of types of cybersystems typically used by maritime sector stakeholders to support their operations;

.2 A description of potential cybersecurity vulnerabilities associated with the types of cybersystems typically used by maritime sector stakeholders;

.3 A description of mitigations that could be implemented by maritime sector stakeholders to address potential cybersecurity vulnerabilities.

2 The proposed voluntary maritime cybersecurity guidelines would:

.1 Be consistent to the greatest extent possible with similar cybersecurity guidelines previously promulgated by international organizations, such as the International Organization for Standardization;

.2 Identify implementable measures to enhance cyber security, but not include specific technical requirements or recommendations to use specific hardware, software, policies or processes.

3 Canada would provide to correspondence group members results of research conducted as part of the development of a Maritime Cybersecurity Strategic Framework, including information on cybersystems used in the maritime sector and associated potential vulnerabilities and mitigations, to serve as a basis for discussion.

4 Canada's Maritime Cyber Security Project has identified five categories to illustrate to maritime sector stakeholders the rationale and importance of identified vulnerabilities and mitigations, categories which could be adopted or adapted by the proposed correspondence group; they are:

.1 access control – ensuring sensitive data and hardware are accessed or altered only for legitimate ends;

.2 network design – taking a holistic and risk-based approach to implement security measures that balance between accessibility and security for different systems, data, and other network components;

.3 intrusion detection – putting in place measures to detect intrusions by malicious actors and limit ongoing harm;

.4 communication security – ensuring information communicated within or outside an organization is received by the person for whom it was intended without alteration; and,

.5 governance – establishing a management framework, including strategic planning, employee engagement and specific policies, to align resources and behaviours with an organization's cybersecurity needs.