INTERNATIONAL MARITIME ORGANIZATION

E

MARITIME SAFETY COMMITTEE
104th session
Agenda item 7

MSC 104/INF.9
28 July 2021
ENGLISH ONLY

Pre-session public release: ☐

MEASURES TO ENHANCE MARITIME SECURITY

Update on French initiatives on cybersecurity

Submitted by France

SUMMARY

Executive summary:	This information document provides a brief overview on recent French initiatives aimed at addressing cybersecurity issues in the maritime sector.
Strategic direction, if applicable:	5
Output:	Not applicable
Action to be taken:	Paragraph 14
Related documents:	Resolution MSC.428(98) and circular MSC-FAL.1/Circ.3/Rev.1

Introduction

1 Recalling the early steps taken in addressing cybersecurity issues in the maritime sector in France, this document sets out the initiatives taken since 2018 to build global governance mechanisms. A particular emphasis is placed on the creation of coordination entities schemes and also on the efforts taken to address the challenges incurred by Resolution MSC.428(98) on French flag maritime companies.

Early steps in addressing maritime cybersecurity challenges in France

2 In 2015 and 2016, the French Directorate for maritime affairs and the National cybersecurity agency (ANSSI) had joined their efforts to conduct a one-year survey on the French flag vessels. Involving more than sixty commercial ships and twenty key operators, this study mainly aimed at identifying the mitigation measures implemented on board, together with the most common vulnerabilities of their information systems.

3 Stemming from the outcomes of that survey, three sets of guidelines, aligned with MSC-FAL.1/Circ.3, were then published and subsequently brought to the attention of the Committee at its 98th session, under document MSC 98/INF.4.

4 Various works and initiatives closely followed, amongst which the following should be emphasized:

.1 The introduction of cybersecurity provisions in relevant French regulatory documents on ship security, e.g. an obligation for operators to address cybersecurity through the ship security assessment, including a mapping of critical information systems;

.2 A series of cybersecurity audits on commercial vessels;

.3 The holding of annual cybersecurity course sessions at the French merchant marine school (ENSM);

.4 The publication by the Directorate for maritime affairs in 2019 of guidelines on the reporting and handling of security incidents, for use by French flag operators.

Towards a global coordination of cybersecurity in the maritime sector

5 Recognizing the need for enhanced cooperation and harmonization in this matter, the French government moved further in November 2018 with a series of strategic decisions, aimed at setting a clear direction for a national maritime cybersecurity strategy.

6 The Maritime cybersecurity committee[1] (hereafter referred to as "the Committee") created a year after was a key step in this regard. Chaired by Prime Minister Services, supported by three vice-chairs representing at the highest level the National cybersecurity agency, the major maritime operators and the naval industry, the Committee serves as a forum for public and private partners.

7 The Committee brings together representatives of public administrations involved in the maritime domain - or more generally in the protection of key infrastructures and sectors - and industry representatives, including but not limited to major ship and port operators but also the shipbuilding industry, classification societies or the insurance sector. The involvement of the National cybersecurity agency (ANSSI) was also considered key for the success of the Committee.

8 An important task assigned to the Committee was the development of a national maritime cybersecurity strategy. This document, which provides a framework for all future developments, sets out the main cybersecurity challenges to be addressed by the maritime sector and includes an action plan with a series of work streams on several key domains, such as but not limited to:

- Governance and oversight;
- Network and information systems protection;
- Cyber defense, including incident management;
- Cyber resilience, including crisis management.

[1] Conseil de cybersécurité du monde maritime

9 Another year of joined efforts across Government administrations, regional authorities and key partners of the private sector, was needed for the setting-up of a non-profit organisation *France cyber maritime* having been mandated to build the future maritime cybersecurity coordination centre.

10 High in the agenda of this new entity, the setting up of the future M-CERT[2] is much awaited by all partners involved, as a significant step towards the handling of cybersecurity incidents, as well as a means to foster smooth and efficient communication on threat and risks. The M-CERT should become operational mid-year 2022 at the latest.

An important issue: implementing IMO Resolution MSC.428(98)

11 A crucial issue that needs to be thoroughly addressed by the maritime sector is how shipping companies will implement the provisions of resolution MSC.428(98), which encourages them to address cybersecurity through their Safety Management Systems (SMS). It is to be underlined that this specific point was jointly brought up by the United States and the shipping industry at the last MSC session in 2019 and has led to a first series of guidelines issues by the industry (most often referred to as the "BIMCO guidelines")

12 With this aim in mind, the French Directorate for maritime affairs issued in July 2020 a series of guidelines to be used, on one hand by the maritime companies, to provide guidance on how to establish cybersecurity policies and procedures meeting the objectives of the resolution. And on the other hand for use by national inspectors as guidance on how to address cybersecurity in the conduct of ISM verifications.

Next steps

13 With a view to strengthen the actions taken by the Committee in addressing the issues set out in this document, the establishment of dedicated work streams on maritime cybersecurity may be contemplated.

Action requested of the Committee

14 The Committee is invited to note the information provided in this document and take action, as deemed appropriate.

---

[2] Computer emergency response Team (M stands for Maritime)