INTERNATIONAL MARITIME ORGANIZATION

E

SUB-COMMITTEE ON HUMAN ELEMENT, TRAINING AND WATCHKEEPING
12th session
Agenda item 6

HTW 12/6/35
10 November 2025
Original: ENGLISH
Pre-session public release: ☒

COMPREHENSIVE REVIEW OF THE 1978 STCW CONVENTION AND CODE

Proposed draft amendments to the STCW Code to address gap no.412

Submitted by ICS

SUMMARY

Executive summary:	This document provides draft amendments to the STCW Code, in order to address gap no.412.
Strategic direction, if applicable:	6
Output:	6.17
Action to be taken:	Paragraph 9
Related documents:	HTW 11/11 and HTW 12/6

Background

1 The Sub-Committee, at its eleventh session, agreed to the list of gaps identified in the STCW Convention and Code, as set out in annex 1 to document HTW 11/WP.4. The Sub-Committee also agreed to the commencement of phase 2 of the comprehensive review (HTW 11/11, paragraphs 6.34 and 6.35).

2 This document provides draft amendments to the STCW Code, in order to address gap no.412, in relation to cybersecurity.

Discussion

3 Awareness of the threat presented by cyber-attack to shipping has increased, as have the mechanisms to reduce it. The IMO requirement[1] to include cyber risk management in the Safety Management System (SMS) from 1 January 2021 has brought cyber risk management in the statutory realm. Further to cyber risk management, there is a need to specify the minimum standards of competency in this area along with the development of associated KUPs within the 1978 STCW Convention.

[1] Refer to resolution MSC.428(98) on " *Maritime cyber risk management in Safety Management Systems*".

4 While the Master has the overall responsibility, the crew member designated as the ship cyber security officer (ship CySO) is responsible for cyber risk management on the ship and ensuring the specifics of compliance with applicable cyber security guidelines and the SMS under the requirements of the ISM Code. While cyber security should be managed under the requirements of the ISM Code, in practice, companies may assign a suitable management-level qualified officer, such as the chief officer, chief engineer or the existing Ship Security Officer (SSO) the responsibility for managing onboard cyber security. Such responsibility should be seen as separate but complementary to their existing duties and responsibilities as outlined in the Ship Security Plan (SSP) and the ISPS Code. The crew member designated as the ship CySO, within the SMS, should also be provided with guidance on escalation paths to shore and coordination with the SSO/PFSO, where appropriate.

Amendments to chapters II and III of the STCW Code

5 ICS has evaluated the options for the most effective placement of cybersecurity training within the relevant chapters to ensure comprehensive coverage and have developed draft amendments to the STCW Code to provide for generic training related to cybersecurity that addresses the responsibilities of shipboard personnel.

6 The features of the proposed draft amendments are:

.1 introduction of an new competency and associated KUPs in the table for the management-level officers i.e. under the function "Controlling the operation of the ship and care for persons on board at the management level", within tables A-II/2 and A-III/2; and

.2 modification of an existing competency and Introduction of additional KUPs for an operational-level officer, i.e. under the function "Electrical, electronic and control engineering at the operational level", within table A-III/6.

Information to support the proposed amendments

7 Taking into account the information for the submission of proposals for phase 2 of the comprehensive review of the STCW Convention and Code, as set out in document HTW 12/6 (Secretariat), information to support the proposed amendments is set out below:

Gap no.*412	
Related documents, if any:	ISWG-STCW 1/2/19
Action requested:	Introduction of new competency and KUPs within tables A-II/2 and A-III/2. In table A-III/6, the competency is modified and KUPs are added.
Available evidence, data, research, etc., if any, to support the proposed amendments:	1 MSC-FAL.1/Circ.3/Rev.3 on *Guidelines on maritime cyber risk management* 2 Resolution MSC.428(98) on *Maritime cyber risk management in safety management system* 3 The Guidelines on Cyber Security Onboard Ships (5th Edition) 4 Cyber Security Workbook for On Board Ship Use 7th Ed.

* Gap nos. are listed in the annex to document HTW 12/6.

Voluntary assessment on the possible cumulative impact (if the proposal aims at adding new training requirements, provide information on the cumulative impact on seafarer's training/certification and possible measures to address the impact):	Information on the cumulative impact: Impact on delivery and training hours for certification for regulations II/2 and III/2 due to new competency and KUPs introduced and on regulation III/6 due to KUPs. Impact expected on Administration to approve new training programmes.
	Possible measures to address the cumulative impact: Optional pathways (recognition of prior learning, blended/CBT delivery, and simulator substitution) may be considered by Parties, as appropriate. Development of implementation guidance for Administrations and companies to leverage existing training records, company drills, and approved CBT to meet the new outcomes efficiently may be considered.

Proposal

8 It is proposed to amend tables A-II/2, A-III/2 and A-III/6, as set out in the annex.

Action request of the Sub-Committee

9 The Sub-Committee is invited to consider the information and proposals in paragraphs 3 to 8, and the annex, and take action, as appropriate.

***

ANNEX[1]

PROPOSED DRAFT AMENDMENTS TO TABLES A-II/2, A-III/2 AND A-III/6 OF THE CODE

CHAPTER II
Standards regarding the master and deck department

Section A-II/2
Mandatory minimum requirements for certification of masters and chief mates on ships of 500 gross tonnage or more

1 The following new competence and corresponding columns 2 to 4 are proposed to be inserted in table A-II/2 (Specification of minimum standard of competence for masters and chief mates on ships of 500 gross tonnage or more):

"**Function: Controlling the operation of the ship and care for persons on board at the management level**

Column 1	Column 2	Column 3	Column 4
Competence	**Knowledge, understanding and proficiency**	**Methods for demonstrating competence**	**Criteria for evaluating competence**
…	…	…	…
Monitor and maintain the cybersecurity of the vessel's systems	Understanding of maritime cybersecurity and the relevance of cyber risk to ship operations. Awareness of current and emerging cyber threats and vulnerabilities affecting shipboard systems. Application of access control, password management, and software update procedures. Understanding of best practices for handling external devices and connections.	Assessment evidence obtained from one or more of the following: .1 approved training and experience including shore side, on board and computer based remote training approved training .2 approved in-service experience	Procedures and working practices designed to safeguard against cyber risks are observed at all times Threats are quickly identified and appropriate protective and detective measures commensurate with system criticality and vendor guidance are taken to minimise impact on the ship systems whilst implementing reversionary modes. Redundancy measures are demonstrated to be put in place to ensure continued safe operation of the ship

[1] Tracked changes are used based on the existing provisions, which are provided in document HTW 12/6/1, i.e. "strikeout" for deleted text and "grey shading" to highlight all modifications and new insertions, including deleted text.

Column 1	Column 2	Column 3	Column 4
Competence	**Knowledge, understanding and proficiency**	**Methods for demonstrating competence**	**Criteria for evaluating competence**
	Knowledge of methods for enhancing cybersecurity awareness and vigilance on board Organisation of drills at intervals and maintain evidence (plans, drill records, outcomes, lessons learned)		when systems are disabled. Once an incident is identified, the impact on the operation of the ship and its systems can be evaluated and reversionary modes activated. Familiarity with IMO and industry guidance on maritime cyber risk management[2]
…	…	…	…

"

[2] ICS-BIMCO Cyber Security Workbook for On board Ship Use.

CHAPTER III
Standards regarding engine department

Section A-III/2
Mandatory minimum requirements for certification of chief engineer officers and second engineer officers on ships powered by main propulsion machinery of 3,000 kW propulsion power or more

2 The following new competence and corresponding columns 2 to 4 are proposed to be inserted in table A-III/2 (Specification of minimum standard of competence for chief engineer officers and second engineer officers on ships powered by main propulsion machinery of 3,000 kW propulsion power or more):

"**Function: Controlling the operation of the ship and care for persons on board at the management level**

Column 1	Column 2	Column 3	Column 4
Competence	**Knowledge, understanding and proficiency**	**Methods for demonstrating competence**	**Criteria for evaluating competence**
…	…	…	…
Monitor and maintain the cybersecurity of the vessel's systems	Understanding of maritime cybersecurity and the relevance of cyber risk to ship operations. Awareness of current and emerging cyber threats and vulnerabilities affecting shipboard systems. Application of access control, password management, and software update procedures. Understanding of best practices for handling external devices and connections. Knowledge of methods for enhancing cybersecurity awareness and vigilance on board. Organisation of drills at intervals and maintain evidence (plans, drill records, outcomes, lessons learned)	Assessment evidence obtained from one or more of the following: .1 approved training and experience including shore side, on board and computer based remote training approved training .2 approved in-service experience	Procedures and working practices designed to safeguard against cyber risks are observed at all times Threats are quickly identified and appropriate protective and detective measures commensurate with system criticality and vendor guidance are taken to minimise impact on the ship systems whilst implementing reversionary modes. Redundancy measures are demonstrated to be put in place to ensure continued safe operation of the ship when systems are disabled. Once an incident is identified, the impact on the operation of the ship and its systems

Column 1	Column 2	Column 3	Column 4
Competence	**Knowledge, understanding and proficiency**	**Methods for demonstrating competence**	**Criteria for evaluating competence**
			can be evaluated and reversionary modes activated. Familiarity with IMO and industry guidance on maritime cyber risk management[1]
…	…	…	…

"

Section A-III/6
Mandatory minimum requirements for certification of electro-technical officers

3 Table A-III/6 (Specification of minimum standard of competence for electro-technical officers) is proposed to be amended, as follows:

"**Function: Electrical, electronic and control engineering at the operational level**

Column 1	Column 2	Column 3	Column 4
Competence	**Knowledge, understanding and proficiency**	**Methods for demonstrating competence**	**Criteria for evaluating competence**
…	…	…	…
Operate computers and computer networks on ships	Understanding of: .1 main features of data processing .2 construction and use of computer networks on ships .3 bridge-based, engine-room-based and commercial computer use .4 Understand the vulnerabilities of the computer-based systems on board which include Operational technology (OT) and Information Technologies (IT) in order to safeguard ships and ship-port interfacing systems.	…	Computer networks and computers are correctly checked and handled Threats to computer systems are quickly identified and appropriate protective and detective measures commensurate with system criticality and vendor guidance are taken to minimise impact on ship systems whilst implementing reversionary modes The type and scale of a cyber-attack are promptly identified and appropriate actions taken.

Column 1	Column 2	Column 3	Column 4
Competence	**Knowledge, understanding and proficiency**	**Methods for demonstrating competence**	**Criteria for evaluating competence**
	An ability to: .1 recognise a cyber incident on hardware or software and be able to take appropriate action to mitigate consequences .2 coordinate with shore/vendor/port counterparts as required .3 verify safe restoration and functional checks post-remediation Ensure that: .1 Computer systems onboard have the up-to-date anti-virus and anti-malware software installed.		Familiarity with IMO and industry guidance on maritime cyber risk management[3]
…	…	…	…

"

---

[3] ICS-BIMCO Cyber Security Workbook for On board Ship Use.