Implementation Group
Doc.: ESDC/2026/111
Date: 18/02/2026
Origin: ESDC Secretariat

Country	Institution	Common Module	ECTS
PL	**PNA**	**Naval Cyber Threats**	**2.0**

Service(s): **Navy**	**Minimum Qualification of Instructors:** • PhD degree in Cyber Security. • English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG Level 2.
Language: **English**	
SQF MILOF:	• **Competence area** – Military technician. • **Learning area** – C4ISR systems & cyber defence. • **Organisational level** – Single Arm/Branch.

Prerequisites for participants:	**Contents of the Module:**
• English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG Level 2. • Computer network basic knowledge.	• Cyber security risks and cyber threats. • System's defensive vulnerability against possible cyber-attack. • The complex cyber security basic principles of cyber security strategies in the maritime domain.

Learning outcomes	Know-ledge	• Formulate the basics of information security, security of communications, data Encryption, Systems evaluation techniques, Vulnerability and methodologies of attack, the complex cyber security. • Perform a review of the principles of cyber security strategies in the maritime domain.
	Skills	• Analyse threats for confidentiality, integrity and availability in IT and OT systems, risks for IT/OT networks and common applications. • Improve the personal and organisational cyber security, identifying the tasks and tools.
	Respon-sibility & Autonomy	• Independently interpret and evaluate cyber risk Assessments and VA&PT reports, identifying priority vulnerabilities, translating findings into actionable mitigation recommendations within the maritime domain context, and assuming responsibility for first-line response to cyber threats affecting ship/port IT–OT systems by applying approved procedures. • Demonstrate autonomous judgment in selecting appropriate protective measures and personal/organisational cyber-hygiene actions, documenting decisions and communicating risk-relevant information through the chain of command.

Verification of learning outcomes:

- Observation: the course consists of theoretical classes followed by practice on cyber security laboratory.
- Tests: the module learning outcomes verification concept is based on assessment of trainee's knowledge, skills, and competences revealed after personal tasking during the training process, supported by fictitious scenarios.
- Evaluation: the final evaluation of trainees is made based on observation of results and practical tests during the final stage of the presented module. Certificate of attendance and individual feedback is provided to participants.

Created by X ..... DD MM YYYY
Revised by CAPT (N) Nedko Dimitrov / Chairman LoD-02 ..... 01 09 2025
Revised by Col. Catalin Popa / Chairman LoD-11 ..... 03 02 2026
Revised by Col Assoc. Prof. Harald Gell, PhD / Chair IG 04 02 2026
Revised by Assoc. Prof. Nikolaos Karadimas, Chairman LoD-08 ..... 13 02 2026
Issued with the status of "Common" by the Implementation Group ..... DD MM YYYY

Module details:		
Main Topic	**Recom-mended WH** for the residential phase	**Details**
Cyber security - characteristics and risk management in the Maritime Domain.	6	• Cyber security characteristics. • IT and OT systems. • Development of protection plans and procedures - Roles, responsibilities, and tasks of maritime institutions.
The threats identification process.	4	• Types of cyber threats. • A cyber incident – definition and stages. • Let`s measure a cyber-threat.
Identification of vulnerabilities and risk management.	4	• Typical vulnerable systems. • Presenting a “Likelihood” as a projection of threat over vulnerability. • Assess the impact of critical vulnerabilities. • Risk assessment.
Dimensions of IT/OT convergence in cyber protection of the Maritime domain.	4	• Common tasks and design of IT/OT systems. • The integration of information technology systems with operational technology systems onboard ships. • IT/OT convergence in the Maritime Transportation System. • Development of protective measures.
Simulations and trainings.	5	• Simulation of penetration test against virtual hosts. • Simulation of penetration test against virtual networks.
Total WH (contact hours)	**23**	
Additional hours (WH) to increase and assess the learning outcomes (during residential phase):		
Self-studies	25	• The guidelines on cyber security onboard ships. • Protect EU - European Union Security Strategy (https://home-affairs.ec.europa.eu/policies/internal-security_en) • European Union Cyber Security Strategy. • EU Cyber Security Strategy for the Digital Decade (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0)
Test/evaluation / assessment	2	• Observations of results and practical tests during the final stage of the module.
Total WH	**50**	The detailed amount of hours for the respective main topic is up to the course director according to national law or the home institution’s rules.

Created by X ..... DD MM YYYY
Revised by CAPT (N) Nedko Dimitrov / Chairman LoD-02 ..... 01 09 2025
Revised by Col. Catalin Popa / Chairman LoD-11 ..... 03 02 2026
Revised by Col Assoc. Prof. Harald Gell, PhD / Chair IG 04 02 2026
Revised by Assoc. Prof. Nikolaos Karadimas, Chairman LoD-08 ..... 13 02 2026
Issued with the status of “Common” by the Implementation Group ..... DD MM YYYY

List of Abbreviations:

B1, B2, C1	CEFR Levels
BIP	Blended Intensive Programme
CEFR	Common European Framework of Reference for Languages
ECTS	European Credit Transfer and Accumulation System
ESDC	European Security and Defence College
IG	Implementation Group
IT/OT	Information Technology/Operational Technology
NATO	North Atlantic Treaty Organization
PL	Republic of Poland
PNA	Polish Naval Academy
STANAG	Standardisation Agreement
VA&PT reports	Vulnerability Assessment and Penetration Testing reports
WH	Working Hour (60 minutes)

Created by X DD MM YYYY
Revised by CAPT (N) Nedko Dimitrov / Chairman LoD-02 01 09 2025
Revised by Col. Catalin Popa / Chairman LoD-11 03 02 2026
Revised by Col Assoc. Prof. Harald Gell, PhD / Chair IG 04 02 2026
Revised by Assoc. Prof. Nikolaos Karadimas, Chairman LoD-08 13 02 2026
Issued with the status of “Common” by the Implementation Group DD MM YYYY