

Country	Institution	Common Module	ECTS
HU	National University of Public Service	Cyber Security	2.0

Service	Minimum Qualification for Lecturers
ALL	<ul style="list-style-type: none"> Fully qualified IT or Electronic Warfare officer Outstanding knowledge of cyber security and IT technology and national/international experience in the field of IT.
Language	<ul style="list-style-type: none"> Teaching experience in the field of cyber security and IT technology.
English	<ul style="list-style-type: none"> English: Common European Framework of Reference for Languages (CEFR) Level B2 or NATO STANAG Level 3.
SQF MILOF	<ul style="list-style-type: none"> Competence area - Military technician Learning area - C4ISR systems & cyber defence Organisation level – Single Arm/Branch / Single Service

Prerequisites for international participants:	Goals of the Module
<ul style="list-style-type: none"> English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG Level 2. Basic knowledge of IT (ECDL) or similar knowledge". Basic knowledge of social media. Basic knowledge of military rules and regulations. 	<ul style="list-style-type: none"> Explain the characteristics of cyber security specifics to the branch/service, Learn about cyber-attacks: fundamentals of malwares, information-based attacks and their attacking methods.

Learning outcomes	Know-ledge	<ul style="list-style-type: none"> Describe aim, role and basics of C4ISR cyber security. Identify main facts of cyber-attacks: malwares, information-based attacks and their attacking methods.
	Skills	<ul style="list-style-type: none"> Deal with C4ISR cyber security management procedures. Develop creative solutions within a personal and organisational cyber security.
	R&A	<ul style="list-style-type: none"> Take responsibility to manage cyber security in unforeseen and changing situations of the operating environment. Make decisions in coherence with cyber security policies.

Verification of learning outcomes
<ul style="list-style-type: none"> Observation: Throughout the Module students are to discuss given topics within syndicates and in the plenary. During these work students are evaluated to verify their performance. Evaluation: Group presentations of given topics. Test: Written exam (multiple choice) at the end of the Module.

Module Details (the content is as an example and depends on the course director decision)		
Main Topic	Recom- mended WH	Details
E-learning (Threats and challenges of information society)	2	<ul style="list-style-type: none"> Fundamentals of information society Information Infrastructures Human threats of information society Technical threats information society
E-learning (Cyber Attacks)	3	<ul style="list-style-type: none"> Cyber space and its components (civil and military) Information-based attacks Malwares
E-learning (Complex cyber security)	4	<ul style="list-style-type: none"> Fields of cyber security Human security Administrative Security Physical Security Information Security
E-learning (National and international cyber security strategies)	2	<ul style="list-style-type: none"> Fundamentals of Cyber Strategies Cyber Policies and Strategies of EU Cyber Strategies of NATO National Cyber Strategies
E-learning (Cyber Security Organisations and standards)	2	<ul style="list-style-type: none"> CSIRTs and CERTs EU ENISA International information security standards: ITIL, COBIT, ISO27001
Test	1	<ul style="list-style-type: none"> If the e-learning does not include tests anyway, the determination of the entry level according to the e-learning outcomes is to be conducted. If this hour is not used it counts to the self-studies hours.
Cyber Security Organisations and standards	2 SW	<ul style="list-style-type: none"> National and international cyber security organisations and standards in practice
Cyber attacks	7 (incl. 4 SW)	<ul style="list-style-type: none"> Attacking methods: DoS, DDoS, APT, Social Engineering, EW attacks (directed energy) Identifying of malwares and other attacks
Case studies	2	<ul style="list-style-type: none"> Analysing known cyber incidents, identifying attack vectors and the possible steps to prevent similar cases
Cyber Security tools	12 (incl. 6 SW)	<ul style="list-style-type: none"> Basics of personal cyber security tools on individual workstations Personal firewalls, anti malwares, secure use of workstation Ensuring cyber security on networks Firewalls, network tools Cyber security and social medias
Total	37	
Additional hours to increase the learning outcomes		
	13	Self-studies & pre-readings. E-learning may also be counted to the self-studies.

Total WH	50	The amount of hours for the use of the developed e-learning is up to the module director. He/she may replace the e-learning hours/topics with residential phases. The detailed amount of hours for the respective main topic is up to the course director according to national law or home institution's rules.
----------	----	---

List of Abbreviations:

APT	Advanced Persistent Threat
B1, B2	Common Reference Levels
CEFR	Common European Framework of Reference for Languages
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information and Related Technologies
CSIRT	Computer Security Incidence Response Team
DDoS	Distributed Denial of Service
DoS	Denial of Service
ECDL	European Computer Driving Licence
ENISA	European Network and Information Security Agency
EU	European Union
EW	Electronic Warfare
HU	Hungary
IG	Implementation group
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LU	Lecture Unit
NATO	North Atlantic Treaty Organisation
SP	The Strategic Partnership
STANAG	Standardization Agreement
SW	Syndicate Work
WH	Working Hour