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

Service **ALL**	**Minimum Qualification for Lecturers**
Language **English**	• Fully-qualified IT or Electronic Warfare officer • Outstanding knowledge of cyber security and IT technology and national/international experience in the field of IT. • Teaching experience in the field of cyber security and IT technology. • English: Common European Framework of Reference for Languages (CEFR) Level B2 or NATO STANAG Level 3.

Prerequisites for international participants:

- 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.

Goal of the Module

- Familiarise with the new type of threats and challenges of information society.
- Learn about cyber attacks: fundamentals of malwares, information-based attacks and their attacking methods.
- Present complex cyber security.
- Ensure knowledge on international/national cyber security strategies.
- Support basic personal and organisational cyber security skills.

Learning outcomes		
	Know-ledge	• Basic knowledge of the new type of cyber threats. • Basic knowledge of cyber attacks: malwares, information-based attacks and their attacking methods. • Understand the complex cyber security. • Understand the principles of international/national cyber security strategies. • Perceive of complex cyber security and its fields.
	Skills	• Identify the cyber threats. • Describe the cyber attacks: fundamentals of malwares, information-based attacks and their attacking methods. • Identify the task and tools to improve of personal and organisational cyber security.
	Compe-tences	• Ability to realise the cyber threats. • Ability to set up basic cyber security defences. • Consider the possibilities to develop cyber security capabilities.

Verification of learning outcomes

- **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.

Origin: Col KOVACS, PhD/NUPS ..... 24th of February, 2016
Revised: Col KOVACS, PhD/NUPS ..... 29th of April 2016
Revised by Col KOVACS & TMA after iMAF 2016 ..... 8th of September, 2016
Revised by Strategic Partners (3rd SP-Meeting) ..... 21st of September, 2016
Revised by the Implementation Group ..... 21st of December, 2016

The Strategic Partnership Project „Creating international semester regarding military education needs for future officers in Europe" has been financed by the European Commission in the frame of Erasmus+ Programme

Module Details		
Main Topic	**Recom-mended WH**	**Details**
E-learning (Threats and challenges of information society)	2	• Fundamentals of information society • Information Infrastructures • Human threats of information society • Technical threats information society
E-learning (Cyber Attacks)	3	• Cyber space and its components (civil and military) • Information-based attacks • Malwares
E-learning (Complex cyber security)	4	• Fields of cyber security • Human security • Administrative Security • Physical Security • Information Security
E-learning (National and international cyber security strategies)	2	• 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	• CSIRTs and CERTs • EU ENISA • International information security standards: ITIL, COBIT, ISO27001
Test	1	• 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	• National and international cyber security organisations and standards in practice
Cyber attacks	7 (incl. 4 SW)	• Attacking methods: DoS, DDoS, APT, Social Engineering, EW attacks (directed energy) • Identifying of malwares and other attacks
Case studies	2	• Analysing known cyber incidents, identifying attack vectors and the possible steps to prevent similar cases
Cyber Security tools	12 (incl. 6 SW)	• 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.

Origin: Col KOVACS, PhD/NUPS ..... 24th of February, 2016
Revised: Col KOVACS, PhD/NUPS ..... 29th of April 2016
Revised by Col KOVACS & TMA after iMAF 2016 ..... 8th of September, 2016
Revised by Strategic Partners (3rd SP-Meeting) ..... 21st of September, 2016
Revised by the Implementation Group ..... 21st of December, 2016

The Strategic Partnership Project „Creating international semester regarding military education needs for future officers in Europe" has been financed by the European Commission in the frame of Erasmus+ Programme

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

Origin: Col KOVACS, PhD/NUPS ..... 24th of February, 2016
Revised: Col KOVACS, PhD/NUPS ..... 29th of April 2016
Revised by Col KOVACS & TMA after iMAF 2016 ..... 8th of September, 2016
Revised by Strategic Partners (3rd SP-Meeting) ..... 21st of September, 2016
Revised by the Implementation Group ..... 21st of December, 2016

The Strategic Partnership Project „Creating international semester regarding military education needs for future officers in Europe" has been financed by the European Commission in the frame of Erasmus+ Programme