Common Module

Technologies in Cybersecurity

Module Description

Implementation Group	
Doc.:	ESDC/2020/261
Date:	18 Dec 2020
Origin:	MUT

Country	Institution	Common Module	ECTS
Poland	**Military University of Technology**	**Technologies in Cybersecurity**	**2.0**

Service **ALL**	**Minimum Qualification for Lecturers** **Officers or civilian Lecturers:** • English: Common European Framework of Reference for Languages (CEFR) Level B2 or min. NATO STANAG 6001 Level 3. • Thorough knowledge of particular technologies in cybersecurity. • Adequate knowledge of new trends in research and study on new technologies in cybersecurity.
Language **English**	
SQF MILOF	**Competence area** - Military technician **Learning area** - C4ISR systems & cyber defence **Organisation level** – Single Arm/Branch / Single Service

Prerequisites for international participants:

- English: Common European Framework of Reference for Languages (CEFR) Level B1 or NATO STANAG Level 2.
- At least 1 year of national (military) higher education.
- Students with computer science background.

Goal of the Module

- 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.
- Theoretical aspects of cybersecurity technologies, possibilities of IT within the cyber protection systems and future development and trends in cybersecurity.

Learning Outcomes		
	Knowledge	• Identify main facts of cyber-attacks: malwares, information-based attacks and their attacking methods. • Describe aim, role and basics of C4ISR cyber security and crucial technologies to be used within the cybersecurity systems.
	Skills	• Deal with C4ISR cyber security management procedures. • Develop creative solutions within a personal and organisational cyber security.
	Responsibility and Autonomy	• Take responsibility to manage cyber security in unforeseen and changing situations of the operating environment. • Make decisions in coherence with cyber security policies.

Created by Col Dr. Gontarczyk, Col Dr. Chmielewski ..... 10th June 2020
Revised by Col Assoc. Prof. Gell, PhD (Chairman IG) ..... 24th June 2020
Revised by LtCol Spinello (Chairman LoD 8) ..... 5th July 2020
Issued with the status of "Common" by the Implementation Group ..... 3rd September 2020
Revised according to SQF MILOF by CAPT (N) N. Dimitrov and Assoc. Prof. N. Karadimas / Chairpersons LoD 2/8 ..... 23rd May 2024

Evaluation of learning outcomes

- Observation: Throughout the Module students will meet with the cybersecurity technologies applications and they will discuss the given topics in the plenary and present teamwork results. During these work students will be evaluated to verify their competences.
- Project: A group project will focus on the basic description of a selected cyber threat. Students will have to select the specific set and describe the general characterisation of it, as well as possibilities of application some measures to detect, contain, and counteract against given threat. Students will point out main problems related to selected threat. Students can use basic methods of scientific work for realise the task.
- Test: Written exam at the end of the module.

Module Details
(the content is as an example and depend on the course director decision)

Main Topic	Recom-mended WH	Details
Theory of Cyberwar and Infowar	2	• Forms of action in cyberspace. TTP (Tactics, Techniques, and Procedures) applied in cyberspace: psychological operations. • Strategies for conducting activities in cyberspace. • Directing activities in cyberspace: planning, monitoring, controlling activities.
Cyberattacks and Digital Threats	2	• Primary ICT attacks. • Attack and penetration testing tools. • Selected, representative attack techniques. • Malware. Classification, principles of construction and operation. • Use, recognition; and principles of malware analysis.
Cybersecurity Aspects of mobile Technologies	2	• Introduction to mobile technologies - field concepts; hardware solutions, applications and application areas. • Wireless communication standards used in mobile solutions. • Mobile systems. • Types of mobile cyber threats.
Artificial Intelligence Applications	2	• Methods of inference – rule based reasoners. • Machine learning methods. • Introduction to artificial intelligence languages.
Technical Cyber Forensic	2	• The need for computer forensics in various fields (business, law enforcement, military, and government). • Processes in computer forensics. • Digital proof of information. • Computer forensic tools and their capabilities.
Penetration Testing	2	• Software testing. • Methods of testing. • Penetration testing techniques.
Software Reverse Engineering	2	• IT systems architecture, with particular emphasis on structures and processes. • Process modelling and analysis. • Methods of discovering processes.

Created by Col Dr. Gontarczyk, Col Dr. Chmielewski ..... 10th June 2020
Revised by Col Assoc. Prof. Gell, PhD (Chairman IG) ..... 24th June 2020
Revised by LtCol Spinello (Chairman LoD 8) ..... 5th July 2020
Issued with the status of "Common" by the Implementation Group ..... 3rd September 2020
Revised according to SQF MILOF by CAPT (N) N. Dimitrov and Assoc. Prof. N. Karadimas / Chairpersons LoD 2/8 ..... 23rd May 2024

		• Methodologies and IT tools supporting process exploration.
Introduction to Cryptology	2	• The historical background of cryptology. • Basic concepts of cryptography and cryptology. • Definition of a cryptosystem. • Basic base and shift ciphers. • Elements of cryptanalysis.
Methods and Tools for Decision Support	2	• Identification of decision-making processes. Theoretical limitations of automatic decision making. • Models of decision-making processes in a selected class of systems, formulation of decision-making tasks based on accepted models. • Activities of particular stages and phases of the command cycle of troops of different types, the execution of which can be supported by computer, supporting several steps and sub-activities of the process. functionality of computerised command support systems, computerised optimisation packages.
Computer Simulation Tools and Methods	2	• Introduction to simulation modelling. • Basic concepts, classification, and assumptions of computer simulation methods and computer number and random process generators. • Methods and techniques of discrete step, event, and process-oriented simulation. • Selected languages of discrete simulation programming.
Total	**20**	
Additional hours (WH) to increase the learning outcomes		
Self-Studies	30	• Separate hours for in-depth-studies on an as-required basis. • Those hours comprise work of students in laboratories and exercises to improve skills and consolidate knowledge.
Total WH	**50**	**Remarks:** • The module encourages the active participation of students. • 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.

Created by Col Dr. Gontarczyk, Col Dr. Chmielewski ..... 10th June 2020
Revised by Col Assoc. Prof. Gell, PhD (Chairman IG) ..... 24th June 2020
Revised by LtCol Spinello (Chairman LoD 8) ..... 5th July 2020
Issued with the status of "Common" by the Implementation Group ..... 3rd September 2020
Revised according to SQF MILOF by CAPT (N) N. Dimitrov and Assoc. Prof. N. Karadimas / Chairpersons LoD 2/8 ..... 23rd May 2024

List of Abbreviations:

B1, B2 ..... Common Reference Levels
CEFR ..... Common European Framework of Reference for Languages
Col ..... Colonel
Doc. ..... Document
e. g. ..... exempli gratia (for example)
ECTS ..... European Credit Transfer and Accumulation System
ESDC ..... European Security and Defence College
IG ..... Implementation Group
IT ..... Information Technology
GIS ..... Geographic Information System
LtCol ..... Lieutenant Colonel
NATO ..... North Atlantic Treaty Organization
PhD ..... Doctor / Doctor of Philosophy
PL ..... Poland
STANAG ..... Standardization Agreement
WH ..... Working Hour / Working Hours

Created by Col Dr. Gontarczyk, Col Dr. Chmielewski ..... 10th June 2020
Revised by Col Assoc. Prof. Gell, PhD (Chairman IG) ..... 24th June 2020
Revised by LtCol Spinello (Chairman LoD 8) ..... 5th July 2020
Issued with the status of “Common” by the Implementation Group ..... 3rd September 2020
Revised according to SQF MILOF by CAPT (N) N. Dimitrov and Assoc. Prof. N. Karadimas / Chairpersons LoD 2/8 ..... 23rd May 2024