Implementation Group	
Doc.:	
Date :	
Origin:	MUT

Country	Institution	Non-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**	

Prerequisites for international participants:	**Goal of the Module**
• 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.	• Discover and understand basic principles of functioning, structure and trouble spots of the cyber security. • Be aware of specification and classification of cybersecurity threats, including technologies used in. • Deepen knowledge of the practical application of particular technologies in cybersecurity and of the decision making process on selection of appropriate measures of treatment selected cyber threats. • Learn about theoretical aspects of cybersecurity technologies, how to use possibilities of IT within the cyber protection systems and forecast future development and trends in cybersecurity.

Learning outcomes		
	Know-ledge	• Knows the crucial technologies to be used within the cybersecurity systems. • Knows the basic direction of development of cybersecurity. • Knows the basics of the practical skills how to use particular technics in cyber threats detection. • Understands the clue of particular methods of defence against cyber penetration. • Demonstrates the necessary terminology allowing him/her to express opinion, arguments and feedbacks on cybersecurity technologies to be used within particular systems.
	Skills	• Is able to maintain, safety operate and manage selected cybersecurity systems used for the common systems. • Is able to consider the main problems related to the cybersecurity within the most frequent applications. • Is able to consider the consequences of development and evolution of cyber security threats and development of suitable cyber defence systems. • Is able to consider impacts of the cybersecurity on the other systems and processes within military.
	Compe-tences	• Is able to argue the necessity of the application of particular technologies in cybersecurity. • Is able to argue the suitability of usage of adequate tools for respective threats in cyber protection systems. • Is able to analyse the trends in development of the new technologies in cybersecurity and their potential future application.

Created by Col. Dr Gontarczyk, Col. Dr Chmielewski ..... 10th of June, 2020
Revised by Col Dr. Gell (Chairman IG) ..... 1th of ----, 2020

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 characterization 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 realize the task.
- **Test**: Written examination at the end of the module.

Module Details

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 cyberthreats
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, 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. • 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 the identification of possible variants of the opponent's action, expert methods of generating variants of the opponent's own troops' action, assessment and selection of the best variant of action, supporting march planning, setting the schedule of supplies, planning the distribution of points: supplies, medical, repair, functionality of computerized command support systems, computerized optimization 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.

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
Lt Col ..... Lieutenant Colonel
NATO ..... North Atlantic Treaty Organisation
PhD ..... Doctor / Doctor of Philosophy
PL ..... Poland
STANAG ..... Standardization Agreement
WH ..... Working Hour / Working Hours