Country	Institution	Module Description	ECTS
GR	**HAFA**	**Cyber Warfare**	**4.0**

Service **AF**	**Minimum Qualification for Lecturers** ○ English: Common European Framework of Reference for Languages (CEFR) Level B2 or NATO STANAG Level 3. ○ Thorough knowledge in cyber security threats and technologies ○ Thorough knowledge of security tools and systems ○ Adequate knowledge of forensic techniques ○ Adequate knowledge in military information systems
Language **English**	

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.

Goal of the Module

- To familiarize students with the basic aspects of the cyber war
- To help students understand the threats and the targets in the connected world
- To analyze the offensive and defensive cyberwarfare techniques
- To describe the cyber environment as a military domain
- To present the cyber capabilities by nation-states
- To discuss the legal, ethical and political aspects of cyber warfare
- To outline the future trends in cyber warfare

Learning outcomes		
	Know-ledge	• Understands the Cyber Threat Landscape • Identifies the High-Value Assets of the Military Organizations • Recognizes an Advanced Cyber Attack Attempt • Describes Issues Regarding Privacy, Anonymity and Security
	Skills	• Identifies and Explains the Various Types of Vulnerabilities in an Cyber Ecosystem • Analyses a Cyber Attack and Identify Effective Countermeasures • Uses Software Tools to Attack or/and Defend Computer Systems • Investigates Actively Security Incidents
	Responsibility & Autonomy	• Applies the Technologies Used to Actively Defend Systems and Networks • Identifies How Threat Actors Conduct Activities in Cyberspace • Identifies the Emerging Trends in Cyber Warfare • Understands the Ethical, Legal, Military and Political Aspects of Cyber Warfare

Draft: Panagiotis Karampelas ..... 06th Jan 2021
Revised by Name(s) Surname(s) XXXXXX
Approved by the Project Committee XXXXXX

Verification of Learning Outcomes	
Test	• A final exam will be given to the cadets for verifying their understanding of the course topics
Assignment	• A group assignment will be given to the cadets to test their understanding of individual threats and techniques used in cyber war
Case study	• A case study will be discussed in the context of the module regarding the risks a nation faces in the cyber war era

Module Details		
Main Topic	**Recom-mended WH**	**Details**
E-learning	8	• Basic Networking and Mobile Devices Concepts
Fundamental Concepts	4	• Information as a Military Asset • Critical Infrastructure • Nonstate Actors in Cyberwar
Setting the Environment	2	• Weaponizing Cyberspace: A History • Targets and Combatants • Worldwide Cyber Threats and Attacks • Security for Critical Infrastructure - SCADA Systems
Cyber Warfare Tools & Tactics	8	• Tools and Tactics Used as Cyber Weapons • Hacking • Network Penetration • Mobile Devices and Internet of Things Compromise • Bots and Spyware • Social Engineering and Psychological Weapons • Physical Security
Defensive Cyberspace Operations	6	• Cyber Defense • Network Systems Protection and Network Counter-Surveillance Operations • Mobile Device Protection • Systems Development with Integrated Security • Protecting Critical Infrastructures • Digital Forensincs
Offensive Cyberspace Operations	6	• Operational Cyberwar • Taxonomy of Cyber Attack Weapons • Cyber Attacks Strategies • Exploring Cyber Security Vulnerabilities of IoT • Attacking Critical Infrastructure • Cyber Threats in Civil and Military Aviation
Electronic Warfare	4	• Communication Electronic Warfare • Attack, Defence and Support
Cyber Terrorism	4	• Using the Internet as a Weapon of Destruction • Terrorism and the Internet • Online Radicalization, Extremism and Cyber Propaganda • Cyber Terrorism Attacks
Military Approach to Cyberwar	4	• Cyber as a Military Domain • The Role of Cyber in Military Doctrine • Direct Military Threats

Cyber Warfare Capabilities by Nation-States	4	• EU Cyber Capabilities and Cyber Defense Institutions • NATO Cyber Capabilities and Cyber Defense Institutions • United States Cyber Capabilities • Russia Cyber Capabilities • China Cyber Capabilities • Israel Cyber Capabilities • Iran Cyber Capabilities • North Korea Cyber Capabilities
Legal Status and Ethics of Cyber Warfare	4	• Targeting and Precautions in Attack • Personal Privacy • Legislations • Legitimate Military Targets • Protection of Civilian Networks, Hospitals and Other Medical Units
Emerging trends in Cyber Warfare	4	• Weaponized Artificial Intelligence • Deepfake in the Service of the Countries • State Supported Cyber Attacks • Attacks against the Cloud • Cyber Attack as a Service • Supply Chain Attacks • Hybrid Threats • Data Privacy Violations
Test	2	• Module examination
Self-Study Hours		
Topic	40	• The self-study hours are required for the preparation of the daily lectures since the students will be actively involved in presenting cyber warfare cases, tools and techniques • Extra hours are required for the preparation and contribution in the group assignment and/or case study of the course
Total WH	**100**	

List of Abbreviations:

CEFR ..... Common European Framework of Reference for Languages
ECTS ..... European Credit Transfer and Accumulation System
NATO ..... North Atlantic Treaty Organisation
STANAG ..... Standardization Agreement
WH ..... Working Hour
IoT ..... Internet of Things
EU ..... European Union

Acknowledgement

The course syllabus was developed in the context of the Strategic Partnership Project "International Air Force Semester" under the contract No. 2020-1-EL01-KA203-079068 co-funded by the Erasmus+ Programme of the European Union.

International Air Force Semester
2020-1-EL01-KA203-079068

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the Erasmus+ Programme of the European Union