NEW JOINT MASTER PROGRAMME

«SECURITY AND DEFENCE»

Open University of Cyprus

Hellenic Air Force Academy

Panagiotis Karampelas
Associate Professor
Hellenic Air Force Academy

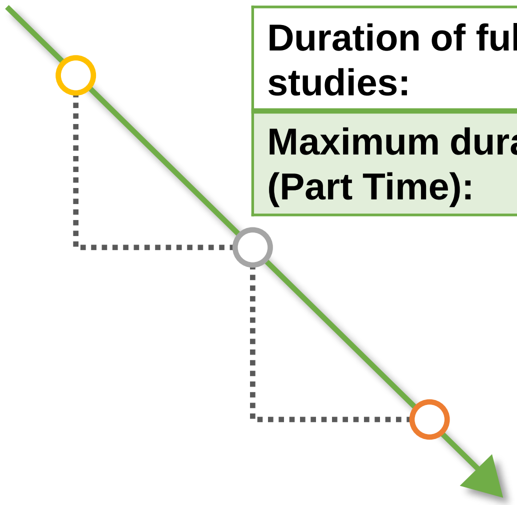
Who we are

MSc in Security and Defence

Institutions Offering the Program

- Open University of Cyprus, Nicosia, Cyprus – 3 permanent academic staff supporting the programme
- Hellenic Air Force Academy, Athens, Greece – 6 permanent academic staff + 1 adjunct staff supporting the programme

Duration of Studies

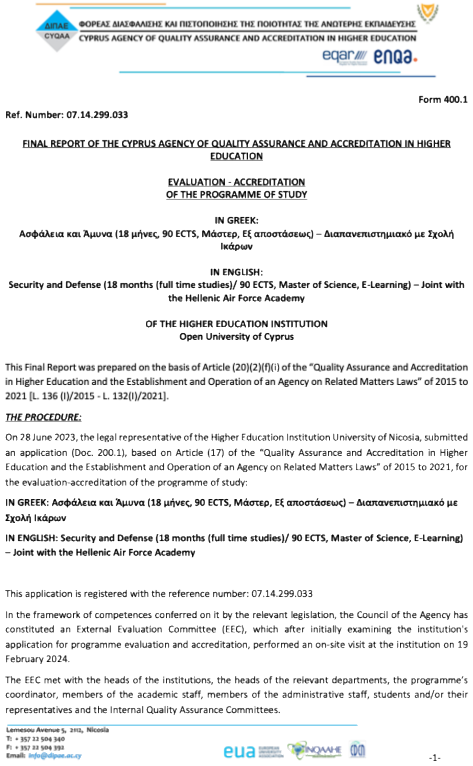


Duration of full-time studies:	**18 months**
Maximum duration (Part Time):	**Up to 6 years**

Number of credits necessary for the successful completion of the program:	**90 ECTS**

Program Accreditation

- The program has already been accreditated by the Cyprus Agency of Quality Assurance and Accreditation in Higher Education (April 2024)
- The program has also been assessed by the Hellenic Authority for Higher Education (July 2025) and the accreditation decision is pending to be received in September 2025



ΔΙΠΑΕ CYQAA
ΦΟΡΕΑΣ ΔΙΑΣΦΑΛΙΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΠΟΙΟΤΗΤΑΣ ΤΗΣ ΑΝΩΤΕΡΗΣ ΕΚΠΑΙΔΕΥΣΗΣ
CYPRUS AGENCY OF QUALITY ASSURANCE AND ACCREDITATION IN HIGHER EDUCATION
eqar enqa.

Form 400.1

Ref. Number: 07.14.299.033

FINAL REPORT OF THE CYPRUS AGENCY OF QUALITY ASSURANCE AND ACCREDITATION IN HIGHER EDUCATION

EVALUATION - ACCREDITATION
OF THE PROGRAMME OF STUDY

IN GREEK:
Ασφάλεια και Άμυνα (18 μήνες, 90 ECTS, Μάστερ, Εξ αποστάσεως) – Διαπανεπιστημιακό με Σχολή Ικάρων

IN ENGLISH:
Security and Defense (18 months (full time studies)/ 90 ECTS, Master of Science, E-Learning) – Joint with the Hellenic Air Force Academy

OF THE HIGHER EDUCATION INSTITUTION
Open University of Cyprus

This Final Report was prepared on the basis of Article (20)(2)(f)(i) of the "Quality Assurance and Accreditation in Higher Education and the Establishment and Operation of an Agency on Related Matters Laws" of 2015 to 2021 [L. 136 (I)/2015 - L. 132(I)/2021].

THE PROCEDURE:

On 28 June 2023, the legal representative of the Higher Education Institution University of Nicosia, submitted an application (Doc. 200.1), based on Article (17) of the "Quality Assurance and Accreditation in Higher Education and the Establishment and Operation of an Agency on Related Matters Laws" of 2015 to 2021, for the evaluation-accreditation of the programme of study:

IN GREEK: Ασφάλεια και Άμυνα (18 μήνες, 90 ECTS, Μάστερ, Εξ αποστάσεως) – Διαπανεπιστημιακό με Σχολή Ικάρων

IN ENGLISH: Security and Defense (18 months (full time studies)/ 90 ECTS, Master of Science, E-Learning) – Joint with the Hellenic Air Force Academy

This application is registered with the reference number: 07.14.299.033

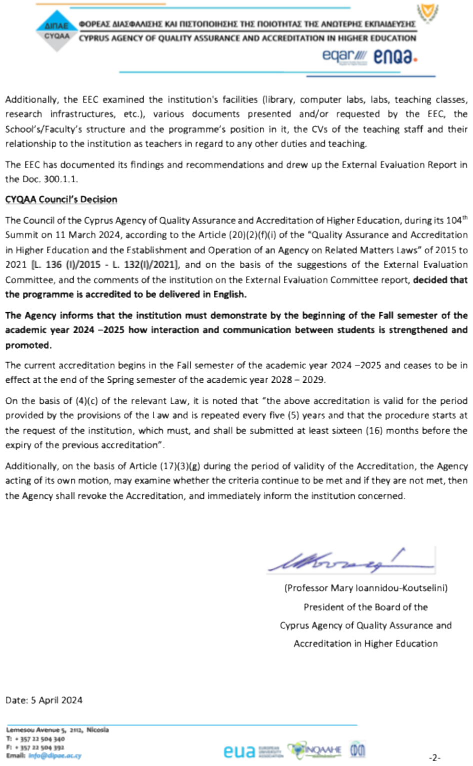
In the framework of competences conferred on it by the relevant legislation, the Council of the Agency has constituted an External Evaluation Committee (EEC), which after initially examining the institution's application for programme evaluation and accreditation, performed an on-site visit at the institution on 19 February 2024.

The EEC met with the heads of the institutions, the heads of the relevant departments, the programme's coordinator, members of the academic staff, members of the administrative staff, students and/or their representatives and the Internal Quality Assurance Committees.

Lemesou Avenue 5, 2112, Nicosia
T: + 357 22 504 340
F: + 357 22 504 392
Email: info@dipae.ac.cy

eua INQAAHE

-1-



ΔΙΠΑΕ CYQAA
ΦΟΡΕΑΣ ΔΙΑΣΦΑΛΙΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΗΣ ΠΟΙΟΤΗΤΑΣ ΤΗΣ ΑΝΩΤΕΡΗΣ ΕΚΠΑΙΔΕΥΣΗΣ
CYPRUS AGENCY OF QUALITY ASSURANCE AND ACCREDITATION IN HIGHER EDUCATION
eqar enqa.

Additionally, the EEC examined the institution's facilities (library, computer labs, labs, teaching classes, research infrastructures, etc.), various documents presented and/or requested by the EEC, the School's/Faculty's structure and the programme's position in it, the CVs of the teaching staff and their relationship to the institution as teachers in regard to any other duties and teaching.

The EEC has documented its findings and recommendations and drew up the External Evaluation Report in the Doc. 300.1.1.

CYQAA Council's Decision

The Council of the Cyprus Agency of Quality Assurance and Accreditation of Higher Education, during its 104th Summit on 11 March 2024, according to the Article (20)(2)(f)(i) of the "Quality Assurance and Accreditation in Higher Education and the Establishment and Operation of an Agency on Related Matters Laws" of 2015 to 2021 [L. 136 (I)/2015 - L. 132(I)/2021], and on the basis of the suggestions of the External Evaluation Committee, and the comments of the institution on the External Evaluation Committee report, **decided that the programme is accredited to be delivered in English.**

The Agency informs that the institution must demonstrate by the beginning of the Fall semester of the academic year 2024 –2025 how interaction and communication between students is strengthened and promoted.

The current accreditation begins in the Fall semester of the academic year 2024 –2025 and ceases to be in effect at the end of the Spring semester of the academic year 2028 – 2029.

On the basis of (4)(c) of the relevant Law, it is noted that "the above accreditation is valid for the period provided by the provisions of the Law and is repeated every five (5) years and that the procedure starts at the request of the institution, which must, and shall be submitted at least sixteen (16) months before the expiry of the previous accreditation".

Additionally, on the basis of Article (17)(3)(g) during the period of validity of the Accreditation, the Agency acting of its own motion, may examine whether the criteria continue to be met and if they are not met, then the Agency shall revoke the Accreditation, and immediately inform the institution concerned.

(Professor Mary Ioannidou-Koutselini)
President of the Board of the
Cyprus Agency of Quality Assurance and
Accreditation in Higher Education

Date: 5 April 2024

Lemesou Avenue 5, 2112, Nicosia
T: + 357 22 504 340
F: + 357 22 504 392
Email: info@dipae.ac.cy

eua INQAAHE

-2-

Motivation, Scope, Audience

Motivation

- Increase in security incidents which can be complex in nature
- Globally volatile environment in Security and Defence fields
- Regional wars among neighbouring countries – resulting in global recession

Scope

- Increase participants knowledge of current technological and asymmetric threats
- Develop the participants ability to manage challenges and crises

Audience / Prospective Students Profile

- Security forces and agencies, government employees involved in security and defence policy
- Civilians working or aspiring to work in fields related to security and defence

Admission Criteria, Employability Prospect

Admission Criteria

- Undergraduate degree from an accredited Higher Education Institution in Computer Science, Engineering or similar background
- Proven proficiency in English Language (prior degree in English, relevant certificates, i.e. IELTS 5.5)
- Adequate computer skills so they can meet the educations requirements of the programme
- Access to the Internet

Graduates Employability Prospect

- Increased demand for professionals specializing in cyber defence and security and related security areas
- Current estimate is that there are approximately 3.5 million such vacancies worldwide (https: // cybersecurityventures.com/jobs/).
- Graduates can be employed horizontally in multiple industries / domains

MSc PROGRAM STRUCTURE

Modules		*Semester*	*Required / Elective*	*Pre-requisite Modules*	*Co-requisite Modules*	*Workload*	
						Hours	*ECTS*
SEC101	Principles of Cyber Warfare	1st	R			250-300	10
SEC102	CyberSecurity	1st	R			250-300	10
SEC111	Telecommunication Systems for Security and Defence	1st	E			250-300	10
SEC112	Information Security Management	1st	E			250-300	10
SEC201	Open-Source Intelligence (OSINT)	2nd	R			250-300	10
SEC202	Research Methods	2nd	R			250-300	10
SEC211	Asymmetric Threats and Countermeasures	2nd	E			250-300	10
SEC212	Technoethics/Ethics for Emerging Military Technologies and Defence	2nd	E			250-300	10
SEC213	Space Applications for Security and Defence	2nd	E			250-300	10
SEC699	Preparatory Module	2nd / 3rd	R			250-300	0
SEC701A	MSc Thesis A	3rd	R	SEC202, SEC699 Minimum 40 ECTS required to enrol to the module		250-300	10
SEC701B	MSc Thesis B	3rd	R	SEC701A, SEC202, SEC699	SEC701A	500-600	20
					Total		**90**

MAIN LEARNING OUTCOMES

Subject Knowledge and Understanding

- ❑ Understand the basic principles of security and the contemporary security challenges, risks and threats
- ❑ Recognize the offensive and defensive techniques used in a cyber war
- ❑ Demonstrate knowledge of modern weapons, especially smart ones
- ❑ Recognize terms and concepts pertaining to different types of telecommunication systems, along with their embedded components and implementations
- ❑ Demonstrate an understanding of the importance of cybersecurity governance and risk management
- ❑ Show knowledge of laws, regulations, and policies as they relate to cybersecurity and data protection
- ❑ Be aware of the tools and techniques that exist and can be applied in open-source intelligence gathering
- ❑ Demonstrate an understanding of the theoretical concepts of Space in Security and Defence

MAIN LEARNING OUTCOMES

Skills

- Define applications of security and defence in current operations
- Perform security risk analysis and assessments and develop contingency plans
- Analyse basic tactics used in cyber-attacks
- Analyse requirements associated with the design, implementation, and deployment of various types of telecommunication systems, especially for security and defence applications
- Identify the most appropriate sources of information in the Internet for a specific subject under investigation
- Specify Electronic Warfare concepts and techniques
- Comprehend low observable principles and anti-stealth approaches.
- Evaluate the potential impact of new space technologies on security and defence

MAIN LEARNING OUTCOMES

Abilities

- ❑ Ability to understand technology, management, and leadership issues related to cybersecurity governance
- ❑ Assess the security policy of your organisation
- ❑ Assess the vulnerabilities of ICT infrastructures using Risk Assessment tools
- ❑ Apply common security policies to protect critical infrastructures and high-value assets.
- ❑ Propose techniques and solutions against threats and security problems in telecommunication systems
- ❑ Apply common techniques in collecting data from social media & online communities
- ❑ Perform a basic assessment of a weapon system in terms of target detection, passive stealth capability and electronic warfare
- ❑ Assess the feasibility and potential impact of space-based solutions for security and defence

TEACHING METHODS and TEACHING MATERIAL

□ Courses are taught in English, including meetings, assignments, exams etc

□ At least one-hour scheduled live video conference on a weekly basis, in which the instructor presents and explains the main topics

□ Course forums, emails, etc are used for asynchronous interaction

□ Use of synchronous video conference tools for synchronous interaction

□ All Educational activities, course assignments and submissions are online.

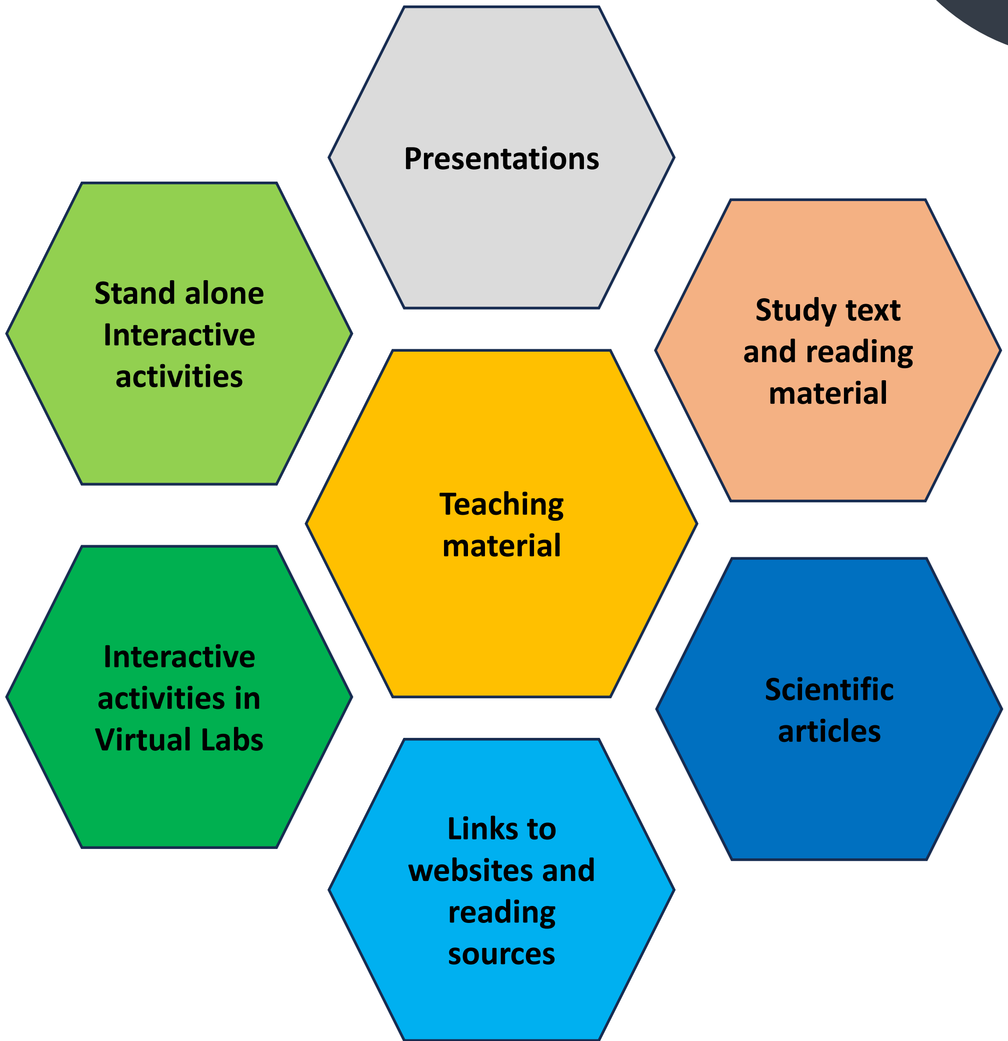
Teaching materials:

□ Online teaching materials that are available through e-class Distance Learning Platform, OUC library, etc.

□ The aim is to be open and accessible to all, so online teaching materials come in a variety of formats, which are designed to suit the variety of students.

□ Materials are mainly available in the formats shown in the diagram.

□ Interactive activities are supported with the use of specialised software either in a synchronous or asynchronous manner



Presentations

Stand alone Interactive activities

Study text and reading material

Teaching material

Interactive activities in Virtual Labs

Scientific articles

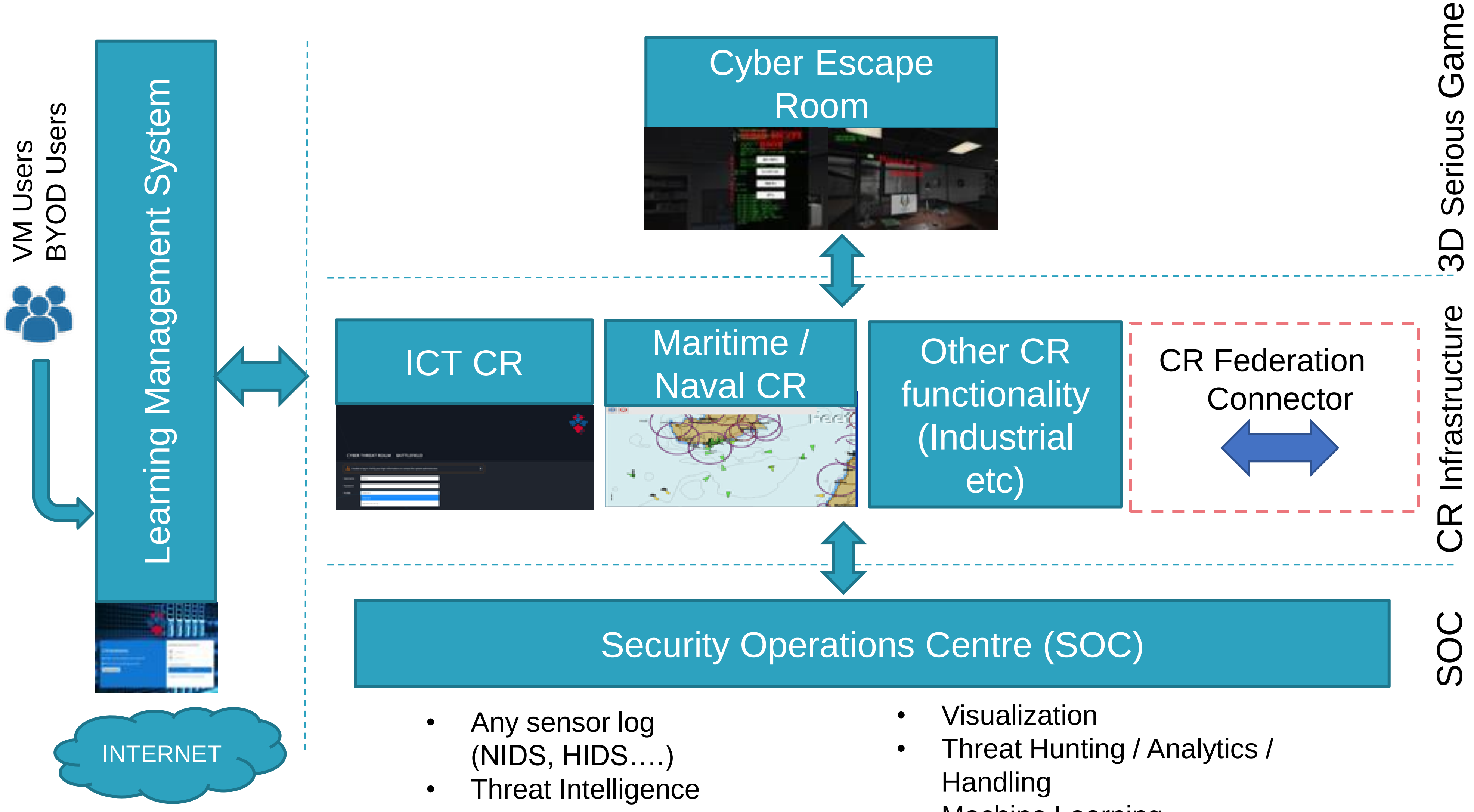
Links to websites and reading sources

Virtual Lab Platforms & Infrastructure

- Provision and access to **Cyber Threat Realm (CTR)** a **Cross Domain Cyber Range (CR)** developed and deployed in house by the Cybersecurity and Telecommunications Research Lab (CTRL). This is a Large-scale virtualization environment which includes ICT, Maritime, and Industrial components.
- Provision and access to a training **Security Operations Centre (SOC)** developed, deployed and operated in house by CTRL. An active operational version of the SOC is also used by national governmental organizations
- The Cyber Range and the SOC provide a realistic cybersecurity training environment which can support horizontal and vertical cyber training activities

Virtual Lab Platforms

Cyber Threat Realm (CTR)



VM Users

BYOD Users

Learning Management System

INTERNET

Cyber Escape Room

3D Serious Game

ICT CR

Maritime / Naval CR

Other CR functionality (Industrial etc)

CR Federation Connector

CR Infrastructure

Security Operations Centre (SOC)

SOC

- Any sensor log (NIDS, HIDS….)
- Threat Intelligence

- Visualization
- Threat Hunting / Analytics / Handling
- Machine Learning
- Scoring

🎓 Joint Master Program in Security & Defence

Applications Open: October 2025

Program Start: January 2026

Mode: 100% Online

Language of Instruction: English

⍰ Gain advanced expertise in security and defence with a flexible, globally accessible program designed for professionals and graduates

HAFA Program’s Website

https://hafa.haf.gr/en/studies/postgraduate-studies/mscinsecanddef/

OUC Program’s Website

https://www.ouc.ac.cy/index.php/en/studies/master/sec

OPEN
UNIVERSITY OF
CYPRUS

OPEN
UNIVERSITY OF
CYPRUS

THANK YOU

Questions?