MASTER OF SCIENCE IN GLOBAL CYBERSECURITY AND AI

PROGRAMME STRUCTURE

Hours of total learning: 2.250
Total Contact Hours: 920
Self Study Hours: 610
Assessment Hours: 720
Program Credits: 90 ECTS
EQF/MQF level 7
Duration: 18 months - 72 weeks
Mode of Delivery: Fully Online Learning
Language of Instruction: English
Mode of Attendance: Full Time

The program structure includes a range of study materials, assessments, and learning activities delivered through both synchronous and asynchronous formats.

The following units will delivered asynchronously:

- Pre-recorded lectures
- Assignment
- Project and research activities

To guarantee the direct interaction among students and professors and to monitor the student's progress and results, the following units are offered synchronously:

- Webinars (live class sessions)
- Forums
- Synchronous section (one to one meeting with tutors or professors)

In addition, the following involve synchronous supervised so as to maintain the integrity of the exam and assessment model:

- Mid-term assessment or test
- Final exam (open question)

The master's degree lasts 18 months and is divided into 3 semesters of 6 months each. Each semester includes:

1st semester: 4 courses
2nd semester: 4 courses
3rd semester: 1 course + final project

Module/Unit Title	Compulsory (C) or Elective (E)	ECTS (Figures must be whole integers and with a value of at least 1 ECTS)	MQF Level of each module	Mode of Teaching (Lectures, workshop, placement, asynchronous, forums, VLE, etc.)	Mode of Assessment (Examination, assignment, project, blog, etc.)
CYB 501 Cybersecurity Principles and Practices	C	8	7	Pre-recorded lectures, webinars, forums, synchronous sections	Mid-term assessment Final exam open question Assignments Project and research activities
CYB 502 Legal, Ethical and Global Cyber Governance	C	8	7	Pre-recorded lectures, webinars, forums, synchronous sections	Mid-term assessment Final exam open question Assignments Project and research activities
CYB 503 Network and Cloud Security	C	7	7	Pre-recorded lectures, webinars, forums, synchronous sections	Mid-term assessment Final exam open question Assignments Project and research activities
CYB 504 Cyber Threat Intelligence and Incident Response	C	8	7	Pre-recorded lectures, webinars, forums, synchronous sections	Mid-term assessment Final exam open question Assignments Project and research activities
CYB 505 AI Applications for Security & Intelligence	C	8	7	Pre-recorded lectures, webinars, forums, synchronous sections	Mid-term assessment Final exam open question Assignments Project and research activities
CYB 506 Machine Learning and secure AI systems	C	7	7	Pre-recorded lectures, webinars, forums, synchronous sections	Mid-term Assessment Final exam open question Assignments Project and research activities
CYB 507 Python for AI	C	7	7	Pre-recorded lectures, webinars, forums, synchronous sections	Mid-term assessment Final exam open question Assignments Project and research activities
CYB 508 Ethical Hacking and Penetration Testing	C	7	7	Pre-recorded lectures, webinars, forums, synchronous sections	Mid-term Assessment Final exam open question Assignments Project and research activities
CYB509 Project Work	C	30	7	Pre-recorded lectures, webinars, forums, synchronous sections	Project work presentation to the master committee

CYB501 Cybersecurity Principles and Practices: MQF/EQF Level 7 – 8 ECTS

This module provides a comprehensive introduction to the fundamental concepts, principles, and best practices in cybersecurity. Students will explore the core domains of information security, including confidentiality, integrity, and availability, as well as common threat vectors, attack types, and security controls. The course examines the architecture of secure systems, risk management frameworks, and organizational approaches to information assurance. Emphasis is placed on understanding how cybersecurity underpins the resilience and operational integrity of both public and private sector organisations.

CYB 502 Legal, Ethical and Global Cyber Governance: MQF/EQF Level 7 – 8 ECTS

This course offers a comprehensive exploration of the legal, ethical, and governance dimensions of cybersecurity in a globally connected digital landscape. It critically examines the intersections between law, policy, technology, and ethics, providing students with a solid foundation to analyse the international and national legal frameworks relevant to cybersecurity, data protection (including GDPR and cross-border privacy regimes), intellectual property and cybercrime.

The course also explores organizational governance models, compliance obligations, and breach notification requirements, preparing students to understand and implement best practices in risk management and apply ethical frameworks to real-world scenarios. By the end of the course, students will be able to assess the cyber risk landscape from the perspectives of legal liability, organizational governance, and ethical responsibility, skills that are essential for professionals shaping cyber policy and protecting digital infrastructures in both public and private sectors.

CYB503 Network and Cloud Security: MQF/EQF Level 7 – 7 ECTS

This module provides an in-depth examination of the principles, technologies, and best practices that underpin secure network and cloud environments. Students will explore foundational and advanced topics in cybersecurity, including network architecture, secure communications, cryptography, firewalls, intrusion detection and prevention systems (IDPS), VPNs, and endpoint protection. Through practical frameworks and case studies, students will gain the ability to evaluate cloud security postures and design security strategies that align with business continuity, regulatory compliance, and operational integrity. Key topics include: information systems strategy and planning, risk analysis and mitigation, audit readiness for cloud-based systems, and data protection frameworks. By the end of the module, students will be prepared to assess, design, and manage secure digital environments, whether operating on-premise, in hybrid deployments, or fully in the cloud, meeting the security demands of today's businesses and service providers.

CYB504 Cyber Threat Intelligence and Incident Response: MQF/EQF Level 7 – 8 ECTS

This module provides a comprehensive exploration of cyber threat intelligence (CTI) and incident response (IR) practices, equipping students with the analytical and operational skills required to detect, assess, and respond to modern cyber threats. Students will examine the lifecycle of threat intelligence, from data collection and analysis to dissemination and action and learn how to implement incident response plans aligned with organisational and regulatory frameworks. Special attention is given to the evolving nature of threat landscapes, the value of threat hunting, and the importance of insider threat identification. Case studies and simulation exercises will enhance students' ability to assess risks, coordinate response teams, and generate incident reports that support strategic decision-making. By the end of the module, students will be capable of proactively identifying cyber threats, mitigating potential damage, and supporting resilient cybersecurity operations through effective intelligence and response planning.

CYB505 AI Application for Security and Intelligence: MQF/EQF Level 7 – 8 ECTS

This course examines the role of artificial intelligence (AI) in advancing cybersecurity and intelligence operations. Students will explore foundational AI concepts and their strategic applications in threat detection, anomaly analysis, and decision support within security contexts. The course covers the design and deployment of intelligent agents capable of autonomously monitoring, analyzing, and responding to complex cyber threats. Topics include behavioral modeling, AI-driven surveillance systems, natural language processing for intelligence gathering, and the use of neural networks in malware and fraud detection.

The course also addresses the critical issue of AI security, focusing on the risks posed by adversarial attacks, model manipulation, and data poisoning. Students will learn how to assess vulnerabilities in AI systems and apply best practices to safeguard AI-powered tools used in cybersecurity.

CYB 506 Machine learning and secure AI systems: MQF/EQF Level 7 – 7 ECTS

This course introduces students to the foundations of machine learning and its secure deployment in modern digital environments. While covering essential supervised and unsupervised learning techniques, the course also examines how machine learning systems operate within the context of cybersecurity, data privacy, and adversarial resilience. Students will begin by exploring core concepts of machine learning, including model evaluation metrics, training paradigms, and algorithm selection. The course emphasizes hands-on practice through labs where students build, test, and validate machine learning models using real-world datasets.

CYB507 Python for AI: MQF/EQF Level 7 – 7 ECTS

This course develops students' proficiency in Python programming with a strong emphasis on data science and artificial intelligence applications. Throughout the course, students will gain hands-on experience in using Python to interact with data: loading datasets from various sources, manipulating and cleaning data, performing statistical analysis, and creating visualizations. Students will work with essential libraries such as pandas, NumPy, matplotlib, and seaborn, and will be introduced to basic machine learning techniques using scikit-learn. Emphasis is placed on practical data workflows, including data retrieval from APIs and web scraping, preparing data for AI models, and automating data-processing tasks. Upon completion, students will possess a solid understanding of Python syntax, the key mechanisms of object-oriented programming, and the ability to design, code, test, and debug Python programs specifically aimed at solving data science and AI problems.

CYB508 Ethical Hacking and Penetration Testing: MQF/EQF Level 7 – 7 ECTS

This course provides an in-depth exploration of ethical hacking and penetration testing as critical components of modern cybersecurity defense. Students will learn how to identify and exploit vulnerabilities in computer systems, networks, and applications in a controlled and ethical manner, simulating the techniques used by malicious hackers, but with the purpose of strengthening security posture. The course offers an overview of the legal, regulatory, and ethical frameworks that govern ethical hacking practices, including global standards and professional codes of conduct. Students will then gain hands-on experience with the methodologies and tools used in professional penetration testing, including reconnaissance, scanning, exploitation, post-exploitation, and reporting. Topics include vulnerability assessment, social engineering, wireless and web application testing, privilege escalation, and defensive countermeasures.

CYB 5509 Project Work: MQF/EQF Level 7 – 30 ECTS

The Master's Project Work is a substantial and in-depth component of the master programme, designed to allow students to apply, integrate, and expand upon the knowledge and skills acquired throughout their study. It provides an opportunity for students to engage in extended, focused research or development work on a topic of personal interest or strategic relevance to their professional goals. Given the academic weight of this 30 ECTS project, students are expected to produce a comprehensive, original piece of work that reflects advanced understanding, critical thinking, and practical insight into complex cybersecurity or AI challenges. Projects may be research-based, applied, or a hybrid of both, and can also take the form of case studies, technical developments, strategic frameworks, or simulation-based work. Students should begin identifying potential project topics during the second semester, with formal topic selection and proposal development taking place by the beginning of the third semester. Topics are often inspired by forum discussions, current industry trends, or real-world cybersecurity/AI incidents. Each student will be assigned a faculty member who will serve as their Project Advisor. The advisor plays a crucial role in guiding the student's research direction, recommending resources (technical tools, data sources), and providing feedback on progress and methodology.