Course Title	Introduction to Cybersecurity				
Course Code	CYS601				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 1st Semester				
Teacher's Name	TBA				
ECTS	7	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	This course introduces the fundamental concepts and terminology of cybersecurity as a whole, and functions as a short introduction to the large number of cybersecurity topics that are covered within this MSc course.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Describe the meaning and position of fundamental cybersecurity concepts and terminology • Explain the position of the different topics within cybersecurity and how they fit into a comprehensive cybersecurity model • Classify and describe different cybersecurity components and how they contribute to effective defence • Classify and describe different potential routes for cyber attacks.				
Prerequisites	None	Co-requisites	None		
Course Content	Introduction: Refresh on fundamental networking principles and devices and distributed systems, the context within which cybersecurity (or lack thereof) can be present. Network structure and ways of communication. History of cybersecurity: important attacks and consequences. Related history (e.g. the important role of cryptography and cryptanalysis in World War II, etc.) Current importance of cybersecurity, given the connectedness of most of our daily lives. Analysis of critical infrastructures and the position of critical information infrastructures within these – importance of the protection of such systems for the smooth operation of essential				

	services in all areas of life. The network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats. Asset protection (including data) as a valuable business operation and its contribution to business survivability. Main principles of cybersecurity – confidentiality, integrity, availability and combinations thereof, resulting in other important cybersecurity concepts and services – accountability, non-repudiation, authenticity, resilience, business continuity and disaster recovery, audit, cybercrime, data / system / network forensics, cyberdefence. Introduction to the phases of cybersecurity – Identify, Protect, Detect, Respond, Recover. Applicable cybersecurity and IT law Software licensing, Data privacy and security, Electronic signatures, Legal and regulatory risks, cyberattacks, digital forensics, liability issues, trust. Introduction to other courses in this MSc (to aid selection of the elective courses). Introduction to specific cybersecurity topics – database security, secure software development, malware analysis, etc. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.
Teaching Methodology	Face – to – face
Bibliography	*"Introduction to Computer Networks and Cybersecurity",* by Chwan-Hwa (John) Wu and J. David Irwin *"Cybersecurity Foundations: An Interdisciplinary Introduction Hardcover"*, by Lee Mark Zeichner IEEE Journals, Magazines and Websites $(ISC)^2$, ISACA, and other cybersecurity websites

Assessment	Examinations Assignment(s)	60% 40% 100%
Language	English	