Course Title	Special Cybersecurity Topics				
Course Code	CYS670				
Course Type	Elective				
Level	Master (2nd cycle)				
Year / Semester	2nd Year / 3rd Semester				
Teacher's Name	TBA				
ECTS	10	Lectures / week	None	Laboratories / week	None
Course Purpose and Objectives	The objective of this course is to provide the student with a comprehensive view of the current state of cybersecurity – major incidents and statistics, recent developments in law, policies, national and European strategies, privacy considerations, new technologies, Safer Internet and the various related professional certifications that are available. Also to provide insight from the organizations and a market perspective of cybersecurity as a critical factor of business growth and economic development. Finally to present the emerging cybersecurity ecosystem and need to keep up to technological developments and threats.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Identify and define the current events in cybersecurity • Describe the various statistics available on cybersecurity and successful attacks around the world • Explain recent developments in national, European and international cybersecurity laws and policies • Define and describe recent developments in the European area and the impact that these may have on the way cybersecurity operations are conducted • Define and describe the different parts of national and European cybersecurity strategy and how they lead to a holistic approach to the response to cybersecurity threats • Identify and describe recent developments in the privacy area, and how it is related to and can be protected by proactive cybersecurity operations • Identify and describe emerging technologies in the cybersecurity field and their applications • Understand the principles of Safer Internet awareness and how cyber awareness becomes a critical factor of vulnerability for cybersecurity on individual or organizational level. • Define and describe the various professional certifications that are available in the area of cybersecurity and network and information security, and how they are applicable to different parts of a comprehensive cybersecurity architecture and related operations.				

Prerequisites	None	Co-requisites	CYS600
Course Content	Introduction: The pace of current developments in cybersecurity and the way that they can influence cybersecurity architecture and operations in organizations and governments. Statistics and major cyber-attacks / incidents in recent years. Law and Policy: Recent developments in law and policies at the national, European and international level. How these developments can impact the way that cybersecurity operations are conducted. Rising importance of privacy and associated policies. Implications of the expanding usage of cloud services. Strategy: National (including Cyprus) and European cybersecurity strategies, how they fit together, national and international cooperation, common and special threats, differences between national and organizational strategies, connections to the areas of cybercrime, cyberdefence and related external affairs. Critical Information Infrastructure Protection. Cybersecurity as a factor of growth and the Cybersecurity Ecosystem: The importance of cybersecurity for businesses and organizations in general and the interrelations with the other policies. How cybersecurity is a factor of growth and economic development of a business or a whole country. The Cyberecurity ecosystem is in constant evolution and a professional needs to make sure keeping up with it. As cybersecurity as a field has grown in scope and influence, it has effectively become an 'ecosystem' of multiple players, all of whom either participate in or influence the way the field develops and/or operates. It is crucial for those players to collaborate and work together to enhance the security posture of communities, nations and the globe, and security consultants have an important role to play in facilitating this goal, in order to achieve a collaborative security in cyberspace. Emerging technologies: Emerging technologies, both in the cybersecurity and in other technological domains, implications on current cybersecurity practices, penetration of technologies that are vulnerable to cyber attacks in all aspects of daily life, implications on vital societal functions. Safer Internet: national, European and international efforts in the Safer Internet area, importance of cyber awareness raising for both of these areas, importance and effects of a high level of cyber safety awareness on individual or organizational level, links and effects to other cybersecurity awareness raising initiatives, Better Internet for children as a key for an innovating society. Professional Certifications: Introduction to the different information security and cybersecurity professional certifications that are available, importance of their combination with academic qualifications, areas of specialization, additional cybersecurity areas covered. Business case study and lecture: Lecture by invited experts from the		

	cybersecurity industry. Discussion normally focuses on the latest developments in the cybersecurity area and their related implications.
Teaching Methodology	E-Learning
Bibliography	National, European and international cybersecurity strategy, policy and legal documents Other professional certification information sources
Assessment	Examinations 50% Assignments/On-going evaluation 50% 100%
Language	English