University of Nicosia, Cyprus

Course Code	**Course Title**	**ECTS Credits**
CRIM-470	Cybercrime	6
Department	**Semester**	**Prerequisites**
Social Sciences	Fall/Spring	None
Type of Course	**Field**	**Language of Instruction**
Elective	Social Sciences	English
Level of Course	**Year of Study**	**Lecturer(s)**
1st Cycle	4th	Dr Ioanna Dionysiou
Mode of Delivery	**Work Placement**	**Co-requisites**
face-to-face	N/A	None

Objectives of the Course:

The main objectives of the course are to:

- provide students with an introduction to the criminological and sociological study of crime on the internet ("cybercrime"), including its commission, motivations, patterns of occurrence, detection, policing, and prevention
- explore different types of internet-related crime and study relevant computing and network technologies, especially where used either in the commission or detection or prevention of cybercrime
- examine the challenges to the prevention of cybercrime
- familiarize students with international, European, and national cybercrime legislation and the role of national organizations in the policing of cyber crime

Learning Outcomes:

After completion of the course students are expected to be able to:

1. identify and describe different forms of cyber crimes
2. demonstrate familiarity with basic relevant computing and network technologies, especially where used either in the commission, detection or prevention of cybercrime
3. analyze policing, legal, electronic, and other measures designed to combat cybercrime and identify their main strengths and weaknesses
4. critically assess recent sociological and socio-legal theories of cyberspace and apply these theories to the specific field of cybercrime
5. explain and demonstrate their knowledge of constitutional laws that apply to those being accused of cyber crimes

Course Contents:

1. Overview of Cybercrime
    a. Definitions

b. Evolution of cybercrime
c. Sociological and criminological aspects of cybercrime
d. Challenges of cybercrime

2. Cybercrime Types
    a. Cybercrimes where the computer is the target: hacking, cracking, fraud, virus dissemination, extortion, unauthorized access to electronic data
    b. Cybercrimes involving improper communications: sending obscene, abusive, or harassing communications; online stalking, harassment, and threats; spam
    c. Cybercrimes involving minors: sexual exploitation of children, sending offensive material to minors, transmitting information about a minor
    d. Intellectual property crimes: copyright infringement, trademark infringement, trade secret infringement
    e. Financial frauds and economic espionage
    f. Social networks and cybercrime: social engineering, vulnerabilities, exploits, identity thefts
3. Combating Cybercrime
    a. Investigating Cybercrime: digital evidence and computer forensics
    b. Interception, search and seizure, and surveillance
    c. Policing in the cyber world
    d. Guidelines for combating cybercrime: international, European, and national legislation
    e. Practical impediments to international investigation
4. Current Trends
    a. Information Warfare and National Security

Learning Activities and Teaching Methods:

Lectures, case studies, guest lectures

Assessment Methods:

Written assignments, project, midterm exam, final exam

Required Textbooks/Reading:

Authors	**Title**	**Publisher**	**Year**	**ISBN**
R. Moore	Cybercrime - Investigating High-Technology Computer Crime, 2nd edition	Elsevier	2011	9781437755824
J. Clough	Principles of Cybercrime	Cambridge University Press	2010	9780521899253