Course Description

Provides instruction in the techniques and practices used to identify incidents of digital crime and digital terrorism, methods of detection of incidents, methods of protection from digital crime and digital terrorism, and the future of digital crime and digital terrorism. Lecture 3 hours per week.

General Course Purpose

To provide instruction in the etiology of digital crime and digital terrorism: digital crime – types, nature, and extent; controlling digital crime – legislation, law enforcement, and investigation; and the future of digital crime and digital terrorism – prevention and trends. This course can be utilized as an elective in the Administrative of Justice AAS degree program.

Course Prerequisites/Co-requisites

Prerequisites: ADJ 100 and 107 or 201, basic computer literacy, experience using the Internet, or permission of the instructor.

Course Objectives

Upon completing the course, the student will be able to:

- Define and discuss digital crimes and digital terrorism.
- Discuss the criminology of digital crime.
- Define and discuss hacking and hackers.
- Identify white collar crimes, viruses, and malicious code, exploitation, stalking, and obscenity and molestation.
- Identify anarchy and hate on the World Wide Web.
- Define and discuss digital laws and legislation.
- Discuss the role and response of law enforcement.
- Discuss digital forensics.
- Complete risk analyses of future digital crime and digital terrorism.
- Discuss future digital crime and digital terrorism.

Major Topics to be Included

- Etiology of Digital Crime and Digital Terrorism
- Controlling Digital Crime: Legislation, Law Enforcement, and Investigation