Course Name	CYBER SECURITY AND CYBER CRIME		Course Code	ITEC333		
Credit Hours	3		Contact Hours	Lec	Lab	Total
				2	2	4
Offered as	☐ University Requirement ☐ College Requirement ☒ Program Requirement ☐ Core ☒ Elective ☒ ITEC ☐ COMP ☐ CNET					
Level	6		Prerequisite	ITEC331		

Course Description:

This course explores cyber-security measures and the different forms of cybercrime and emergent forms of cyber-warfare. Students will learn challenges to cyber-security and examine the nature, prevalence, scope and the means by which criminals perform these crimes. They will be aware of how the concept of cyber power rises naturally from a holistic consideration of cybersecurity and, specifically, how it can be expressed through cyber criminality, cyberterrorism, cyber conflicts and cyberwarfare. The course also provides the impact of cybercrime on victims, business, and the state, and the responses of information security providers and police agencies. The course concludes with a critical assessment of the threats to rights posed by the emergent new digital age of surveillance.

Upon completion, the student will be able to:

- Understand the structure, mechanics and evolution of the Internet in the context of emerging crime threats and technological and other trends in cyberspace.
- Understand the threats that society should be prepared to face and the ways in which crimes and conflicts are carried out in cyberspace.
- Respond to cyberattacks and ensure cybersecurity strategies.
- Distinguish and classify the forms of cybercriminal activity and the methods used to undertake such crimes.
- Investigate assumptions about the behavior and role of offenders and victims in cyberspace, and use basic web-tools to explore behavior on-line.
- Develop the awareness and skills that will allow society to fight against cyber-based criminality and abuse
- Analyze and assess the impact of cybercrime on government, businesses, individuals and society.
- Evaluate the effectiveness of cyber-security its ethics, cyber-laws and other counter measures against cybercrime and cyber warfare.

Assessment Methods						
	☒ **Midterm Exam**	**15%**	☒ **Assignment 1**	**10%**	☒ **Assignment2**	**15%**
	☒ **Case Study Tasks +/ Case Study Presentation/ report**	**20%**	☒ **Final Exam**			**40%**

Text Book:

- Cyber Power CRIME, CONFLICT AND SECURITY IN CYBERSPACE, SOLANGE GHERNAOUTI-CRC PRESS

Reference Books:

- Citron, Danielle 2014, Hate Crimes in Cyberspace, Harvard University Press.
- Clough, John, 2010, Principles of Cybercrime, Cambridge University Press.
- Rosenzweig, Paul, 2012, Cyber Warfare: How Conflicts in Cyberspace are challenging America and Changing the World, Praeger, Santa Barbara.