STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

CYBR 368 – Cybercrime Law & Policy

Created by: Stephen Maher
Updated by: NA

SCHOOL OF SCIENCE, HEALTH & CRIMINAL JUSTICE
CENTER FOR CRIMINAL JUSTICE, INTELLIGENCE AND CYBERSECURITY
SPRING 2020

A. **TITLE**: Cybercrime Law & Policy

B. **COURSE NUMBER:** CYBR 368

C. **CREDIT HOURS:** 3 credit hours / week

D. **WRITING INTENSIVE COURSE**: No

E. **GER CATEGORY:** N/A

F. **SEMESTER(S) OFFERED:** Fall or Spring

G. **COURSE DESCRIPTION:**

This course provides students with an understanding of cybercrime law and policy, both in the US and internationally while touching upon the broader concepts of cyberspace and cybersecurity. The course provides a basic understanding of the US Constitution and an introduction to US law relating to cybercrimes, which target computers and networks, as well as those which use computers to commit more conventional crimes such as fraud and theft. The course also gives students an understanding of criminal law concepts such as intent, evidence, conspiracy, and privacy rights, and will review some important US Supreme Court cases related to cybercrime. Students also consider international law, cyber terrorism, national security and cyberwar.

H. **PRE-REQUISITES/CO-REQUISITES:**

a. Pre-requisite(s): 45 completed credits or permission of instructor
b. Co-requisite(s): None
c. Pre- or co-requisite(s): None

I. **STUDENT LEARNING OUTCOMES:**

Course Student Learning Outcome [SLO]	***Program Student Learning Outcome [PSLO]***	***ISLO & SUBSETS***
a. Classify the provisions of the US Constitution most relevant to cyber law.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	1[W] 2[IA] 4[ER]
b. Cite and understand the landmark Supreme Court decisions in the development of cyber law.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	1[W] 2[IA] 4[ER]
c. Explain key concepts of cybercrimes and their relevance to cyber law.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	1[W] 2[IA] 4[ER]

d. Explain the Fourth and Fifth Amendments to the US Constitution in the context of cyber law.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	1[W] 2[IA] 4[ER]
e. Identify and explain the factors that make attribution of cybercrimes difficult domestically and internationally, and whether it is possible or realistic to pursue cyber criminals into other jurisdictions.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	1[W] 2[IA] 4[ER]
f. Identify and explain how the cyber domain figures into global politics, nation state conflicts, espionage, and terrorist groups.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	1[W] 2[IA] 4[ER]
g. Identify and explain some of the future expectations regarding cybercrime including how the US can protect itself, how emerging democracies can protect themselves, and whether these goals can be accomplished through legislation, proactive law enforcement, treaties, military intervention, or all of the above.	5. Analyze and resolve Cybersecurity problems through the application of systematic approaches, and complete all work in compliance with relevant policies, practices, processes, and procedures	1[W] 2[IA] 4[ER]

KEY	**Institutional Student Learning Outcomes [ISLO 1 – 5]**
ISLO #	**ISLO & Subsets**
1	**Communication Skills** Oral [O], Written [W]
2	**Critical Thinking** *Critical Analysis [CA] , Inquiry & Analysis [IA] , Problem Solving [PS]*
3	**Foundational Skills** *Information Management [IM], Quantitative Lit,/Reasoning [QTR]*
4	**Social Responsibility** *Ethical Reasoning [ER], Global Learning [GL], Intercultural Knowledge [IK], Teamwork [T]*
5	**Industry, Professional, Discipline Specific Knowledge and Skills**

J. APPLIED LEARNING COMPONENT: **Yes_____** **No __X____**

K. TEXTS:
Brenner, Susan; Cybercrime: Criminal threats in Cyberspace; Santa Barbara, CA; Praeger, ISBN: 978-0313365461

L. REFERENCES: None

M. EQUIPMENT: None

N. GRADING METHOD: A-F

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:
- Discussions
- Essays
- Quizzes
- Final

P. DETAILED COURSE OUTLINE:
1. The US Legal System
2. The US Constitution as foundation
3. Cybercrimes as common law crimes against person and property
4. Need for specific criminal laws and legislation
5. US Supreme Court cases re cybercrime
6. Mechanisms and equipment of cybercrimes (hacking, malware, DDOS attacks)
7. Attribution
8. Evidence collection and preservation
9. Criminal Intent
10. Balance of Privacy and Security (4^{th} and 5^{th} Amendments)
11. Jurisdiction and international concerns
12. Global politics
13. Cyber War and Espionage
14. What's Next – future of cybercrime, protection and enforcement

Q. LABORATORY OUTLINE: N/A