San José State University
Department of Justice Studies
JS 161: Introduction to Cybercrime
Winter 2019

Course and Contact Information

Instructor:	Dr. Bryce Westlake
Office Location:	Health Building 211
Email:	Bryce.Westlake@sjsu.edu
Office Hours:	Online (TBD)

Course Format

Technology Intensive, Hybrid, and Online Courses (Required if applicable)

I will utilize the Canvas Learning Management System as a means for distributing course materials such as syllabus, handouts, lecture slides, assignment instructions, and communications about changes to the course. You are responsible for regularly checking with the messaging system through MySJSU to learn of updates.

Catalog Description

Introduces students to the growing legal, technical, and social issues surrounding crimes committed in cyberspace or assisted by computers. Discusses the nature of cybercrime from an international perspective and how the borderless nature of cybercrime impacts regulation and enforcement.

Course Description

This course explores how an interconnected world has modified how existing criminal activity is conducted and how new criminal opportunities have been created. Students will examine the history and complex nature of computer-related crime and how societies have attempted to respond. Students will discuss the different types of cybercriminals, including motives, rationale, and methods of attack. We will also evaluate various legal and regulatory issues in cyberspace, including surveillance, sting operations, current and proposed legislation, user-reporting initiatives, identity filtering/blocking technologies, vigilante movements, individual rights, and international law enforcement cooperation.

Course Goals

The Department of Justice Studies is committed to scholarly excellence. Therefore, the Department promotes academic, critical, and creative engagement with language (i.e., reading and writing) throughout its curriculum. A sustained and intensive exploration of language prepares students to think critically and to act meaningfully in interrelated areas of their lives–personal, professional, economic, social, political, ethical, and cultural. Graduates of the Department of Justice Studies leave San José State University prepared to enter a range of careers and for advanced study in a variety of fields; they are prepared to more effectively identify and ameliorate injustice in their personal, professional and civic lives. Indeed, the impact of literacy is evident not only within the span of a specific course, semester, or academic program but also over the span of a lifetime.

Course Learning Outcomes (CLO)

Upon successful completion of this course, students will be able to:

> (CLO 1) distinguish between the different types of cybercrimes, including who/what they target, how/where they are conducted, and why they persist.
> (CLO 2) describe the impacts of the Internet on the opportunities created for committing traditional crimes (e.g., bullying) and new crimes (e.g., phishing).
> (CLO 3) identify the challenges faced nationally and internationally at combating cybercrime and the steps taking by organizations to address these challenges.
> (CLO 4) take steps to increase their own security and privacy when online.
> (CLO 5) take what they have learned in class and apply it to current events.

Required Texts/Readings

Textbook (Supplied on Canvas)

Clough, J. (2015). *Principles of Cybercrime (2nd Edition)*. Cambridge University Press. ISBN13: 978-1-107698161.

Other Readings

Supplied electronically via Canvas (See Course Schedule Below)

Course Requirements and Assignments

Reflection Papers (20%): You will write four reflection papers, each at least two (full) pages in length. Each paper will focus on a specific topic and question, which I will provide to students via discussion. Students will be expected to provide their viewpoint and critically discuss the implications of the issue or event to our understanding of cybercrime and how it is addressed by societies. This assignment will specifically address CLO's 1, 2, 3, 4, and 5.

Paper #1 –Online Privacy (25%): The purpose of this assignment is to provide students with practical experience to explore the concept of personal privacy, or lack thereof, on the Internet. Students will write a short paper (6-8 pages) on their investigation of two topics. First, students will input their name into a search engine, with minimal other identifying information, and describe whether the data returned was about them, and how they felt about that information being readily accessible. They will describe the age (i.e., how old), personal nature (e.g., address, phone number, banking information), and online profile (e.g., your likes/dislikes, purchases, hobbies) it presented about them. Second, students will use any cyber methods they can devise to find information on the course instructor. Students will be required to record the steps they took (e.g., search terms) to acquire the information and what information they obtained, including where it was found. Students will then describe this process and reflect on the steps others may take to find out personal information about them. This assignment will specifically address CLO 4.

Paper #2 –Combating Cybercrime Internationally (25%): The purpose of this assignment is for students to explore the legal issues regarding how governments and social control agencies can police a virtual environment without physical boundaries and borders. Select a type of cybercrime discussed in the course and determine how partnerships/cooperation/resource-sharing could, realistically, be improved between them and the United States. Students will write a short paper (6-8 pages) on the laws, if any, that exist in each country and what each could learn from the other. Discussion should include how privacy and rights can be balanced with security. This assignment will specifically address CLO 3.

Final Examination (30%): Students will be administered a final examination worth 30% of their final grade. Exam is closed book and will cover material from lectures (including all media presented) and assigned readings**.** The final will be held during the final exam period. The exam will be comprised of multiple choice and short answer questions. The examinations will specifically address CLO's 1, 2, and 3.

Grading Information (Required)

A (plus)	97% to 100%	A	93% to <97%	A (minus)	90% to <93%
B (plus)	85% to <90%	B	80% to <85%	B (minus)	75% to <80%
C (plus)	70% to <75%	C	65% to <70%	C (minus)	60% to <65%
F	Below 60%				

University Policies

Per University Policy S16-9, university-wide policy information relevant to all courses, such as academic integrity, accommodations, etc. will be available on Office of Graduate and Undergraduate Programs' Syllabus Information web page at http://www.sjsu.edu/gup/syllabusinfo/"

JS 161: Introduction to Cybercrime
Winter 2019 Course Schedule

This course schedule is subject to change with fair notice, at the instructor's discretion. All reading assignments listed should be completed prior to class on that date. Additional readings may be assigned.

Course Schedule

Lecture	Date	Topics	Readings
1	01/02/19	**Introduction** -Course overview -Assignments -Canvas	*Principles of Cybercrime (Clough)* Chapter 1 (Cybercrime) *Articles* The Current State of Cybercrime Scholarship (Holt & Bossler) The Internet as a Conduit for Criminal Activity (Wall)
2	01/02/19	**What is Cybercrime** -Computer and Internet basics -Cybercrime research -Routine Activity Theory	*Principles of Cybercrime (Clough)* Chapter 2 (Computer as Target) *Articles* How does the Internet work (Strickland) How Firewalls Work (Tyson) What is an 'IP Address' (Gil)
3	01/03/19	**Malware** -Viruses, worms, trojan horses, rootkits, keyloggers, & ransomware	*Principles of Cybercrime (Clough)* Chapter 4 (Modification or Impairment of Data) *Articles* Mobile Malware Evolution 2016 (Kaspersky Lab) Internet Security Report 2017 (ISTR) *Reflection Paper #1 Due: What is Cybercrime*
4	01/04/19	**Personal Security** -Privacy -Surveillance -Personal safety -The Secret War	*Articles* The Secret War (Popular Mechanics) The Online Threat (Hersh) *Social Engineering Checklist (See Canvas)*
5	01/07/19	**Your Online ID** -Social networks & search engines -Identity theft and fraud	*Principles of Cybercrime (Clough)* Chapter 7 (Fraud) *Articles* What is Social Engineering (Webroot) **Assignment Due: Paper #1: Tell Me a Story**
6	01/08/19	**Hacking** -Hacker culture -Legal issues -Hacking as a service	*Articles* Hackers Manifesto (The Mentor) How Big and Powerful is Anonymous (Vandita)
7	01/09/19	**Copyright Infringement** -What is it? -Who owns the data on the Internet? -Piracy (peer-2-peer)	*Principles of Cybercrime (Clough)* Chapter 8 (Criminal Copyright Infringement) *Articles* An Oral History of Napster (Fortune) *Reflection Paper #2 Due: Role of ISP & Companies…*

Lecture	Date	Topics	Readings
8	01/10/19	**Organized Crime** -Carding, -Money laundering -Drugs & weapons	*Articles* Koobface: Inside a Crimeware Network (Villeneuve) The Great Cyberheist (Verini) A Hacker's Race to Build the Amazon.com of Stolen Credit Cards (WeirderWeb) Carders.cc Hacked (Reusablesec)
9	01/11/19	**Deep Web** -TOR -Digital currency (Bitcoin) -The Dark Web	*Articles* Exploring the Deep Web (Trend Micro) Everything You..Know About Deep Web (Security AP) Tor Project: Overview (TOR) What are BitCoins (Lifewire) How BitCoin Works (Forbes) *Reflection Paper #3: Deep Web*
10	01/14/19	**Cybercrime & the Law** -International challenges -Jurisdiction and joint operations	*Principles of Cybercrime (Clough)* Chapter 14 (Jurisdiction) Chapter 6 (Interception of Data)
11	01/15/19	**Email Spam** -Phishing & Pharming -Legal issues -Legislation efforts	*Principles of Cybercrime (Clough)* Chapter 9 ('Spam') **Paper #2: Combating Cybercrime Internationally**
12	01/16/19	**Personal Cyber-Crimes** -Stalking & bullying -Revenge pornography	*Principles of Cybercrime (Clough)* Chapter 12 (Harassment) Chapter 13 (Voyeurism)
13	01/17/19	**Sex Crimes** -Trafficking -Child sexual exploitation -Sexting	*Principles of Cybercrime (Clough)* Chapter 10 (Child Pornography) Chapter 11 (Grooming) *Reflection #4: Amanda Todd*
14	01/18/19	**Violent Extremism** -Terrorism in digital age -Methods of distribution -White Supremacists	*Articles* How Modern Terrorism Uses the Internet (Weimann) Terrorism and the Internet (Conway) Exploring Stormfront (Bowman-Grieve)
15	01/18/19 & 01/19/19	**FINAL EXAMINATION**	**NO READINGS**