San José State University
Department of Justice Studies
JS 161: Introduction to Cybercrime
Winter 2022

Course and Contact Information

Instructor:	Dr. Bryce Westlake
Office Location:	Health Building 210B
Email:	Bryce.Westlake@sjsu.edu
Office Hours:	None
Prerequisites:	JS 100W (or equivalent)

Course Format

Technology Intensive, Hybrid, and Online Courses

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 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) use what they have learned to increase their own security and privacy when online.

(CLO 5) apply what they have learned to cybercrime-related current events.

Required Readings

Articles: supplied electronically via Canvas.

Course Requirements and Assignments

Reflection Papers (25%): You will write six 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 Canvas. 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 –Tell Me a Story (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, and/or 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 (25%): Students will be administered a final examination worth 25% 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

- Individual assignment rubrics will be provided closer to the due date, on Canvas.
- Late assignments/papers will lose 10% for every calendar day that they are late, including weekend days.

Determination of Grades

A (plus)	95% to 100%	A	90% to <95%	A (minus)	85% to <90%
B (plus)	80% to <85%	B	75% to <80%	B (minus)	70% to <75%
C (plus)	67% to <70%	C	63% to <67%	C (minus)	60% to <63%
F	Below 60%				

University Policies

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 2020 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 reviewing the lecture slides for that date. Additional readings may be assigned.

Lect	Date	Topics	Readings
1	01/03/21	**Introduction** -Course overview -Assignments -Canvas	*Articles* Historical Evolution of Cybercrime (Choi, Lee, & Louderback, 2019) The Internet as a Conduit for Criminal Activity (Wall, 2010)
2	01/04/21	**What is Cybercrime** -Computer and Internet basics -Cybercrime research -Routine Activity Theory	*Articles* The Current State of Cybercrime Scholarship (Holt & Bossler, 2014) Defining Cybercrime (Payne, 2019) *Reflection Paper #1 Due: What is Cybercrime*
3	01/05/21	**Malware** -Viruses, worms, trojan horses, rootkits, keyloggers, & ransomware	*Articles* 2020 Cybersecurity Outlook Report (VMware, 2020) The Evolution of Cybercrime and Cyberdefense (Trend Micro, 2018)
4	01/06/21	**Hacking** -Hacker culture -Legal issues -Hacking as a service	*Articles* What is Hacking (Guru99) The Kill Chain (Lockheed Martin, 2015) MITRE ATT&CK Framework (Petters, 2019) *Reflection Paper #2 Due: Impact of Malware Attacks*
5	01/07/21	**Privacy & Security** -Surveillance -Passwords -Personal safety	*Articles* Facebook Studies (Various Authors) What is Social Engineering (Webroot) Private Traits and Attributes (Kosinski, Stillwell, & Graepel, 2013) How Vulnerable are You - Social Engineering Checklist
6	01/10/21	**Identity Theft & Fraud** -Identity theft and fraud -Social media & crime	*Articles* Identity Theft: Nature, Extent, and Global Response (Golladay, 2019) Police Legitimacy in the Age of Social Media (Nhan & Noakes, 2019) **Paper #1 Due: Tell Me a Story**
7	01/11/21	**Deep Web** -TOR -Digital currency -The Dark Web	*Articles* Exploring the Deep Web (Trend Micro, 2015) Cryptocurrency: Enforcement Framework (US DoJ, 2020)

Lect	Date	Topics	Readings
8	01/12/21	**Copyright Infringement** -What is it? -Who owns the data on the Internet? -Piracy (peer-2-peer)	*Articles* An Oral History of Napster (Fortune, 2013) *Reflection Paper #3 Due: A Life with Digital Currency*
9	01/13/21	**Bullying & Stalking** -Online vs offline -Suicide -Law enforcement response	*Articles* Intimate Partner Violence and the Internet (Clevenger & Gilliam, 2019) Risk and Protective Factors for Cyberbullying Perpetration and Victimization (Wilson, Witherup, & Payne, 2019)
10	01/14/21	**Combating Cybercrime** - Jurisdiction - Police relations - Digital forensics	*Articles* Cybercrime Legislation in the United States (Bossler, 2019) Digital and Multimedia Evidence (SWGDE, 2012) Forensic Evidence and Cybercrime (Rodgers, 2019) Police and Extralegal Structures to Combat Cybercrime (Holt, 2019) *Reflection #4 Due: The Deadly Effects of Cyberbullying*
11	01/17/21	**Sex Crimes** -Human trafficking -Child sexual abuse -Sexting -Self-produced & revenge pornography	*Articles* The Past, Present, and Future of Online Child Sexual Exploitation (Westlake, 2019) Trafficking in Persons Report (Department of State, June 2019) **Paper #2 Due: Combating Cybercrime Internationally**
12	01/18/21	**Email Spam** -Legal issues -Legislation efforts -CAN-SPAM -Phishing & pharming	*Articles* Technology Use Abuse and Public Perception (Furnell, 2019) *Reflection #5 Due: The Internet is for Porn*
13	01/29/21	**Radicalization & Misinformation** -Terrorism -Fake news -Deep fakes	*Articles* Information Overload Helps Fake News Spread (Menczer & Hills, 2020) The Role of the Internet in Facilitating Violent Extremism and Terrorism (Scrivens, Gill, & Conway, 2019)
14	01/20/21	**FINAL EXAMINATION**	**NO READINGS** *Reflection #6 Due: The Risk of Deep Fakes*
15	01/21/21		**Final Exam**