San José State University
Department of Justice Studies
JS 161: Introduction to Cybercrime
Fall 2018

Course and Contact Information

Instructor:	Dr. Bryce Westlake
Office Location:	Health Building 210B
Email:	Bryce.Westlake@sjsu.edu
Office Hours:	Monday and Wednesday 2:00 pm to 4:00 pm
Class Days/Time:	Monday and Wednesday 4:30 pm to 5:45 pm
Classroom:	MacQuarrie Hall 523
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 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) takes 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 Readings

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

Other Readings: Supplied electronically via Canvas.

Library Liaison

Silke Higgins (silke.higgins@sjsu.edu), (408) 808.2118)
http://libguides.sjsu.edu/justicestudies

Course Requirements and Assignments

Class Discussion (15%): The purpose of this assignment is for students to be able to engage on key issues and current events related to the week's overall topic. 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 3, 4, and 5.

Paper #1 –Online Privacy (15%): 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 six to eight-page paper (excluding title page and references) 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's 2 and 4.

Paper #2 –Combating Cybercrime Internationally (20%): 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 six to eight-page paper (excluding title page and references) 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's 3 and 4.

Presentation #1 – Malware (10%): The purpose of this assignment is for students to become familiar with some of the most impactful malware attacks over the past decade. In small groups, students will give a maximum 15-minute presentation on an influential malware attack. Students will describe the type of malware, the attack, how it was detected, the resulting damage, and the long-term effects. A more detailed breakdown of the requirements for this assignment can be found on Canvas. This assignment will specifically address CLO's 1, 3, and 5.

Presentation #2 -Data Breach (10%): The purpose of this assignment is for students to become familiar with some of the most impactful data breaches over the past decade. In small groups, students will give a maximum 15-minute presentation describing the data breach, how it was detected, the resulting damage, and the technical and managerial implications of the incident. the resulting damage, and the long-term effects. A more detailed breakdown of the requirements for this assignment can be found on Canvas. This assignment will specifically address CLO's 1, 3, and 5. This assignment will specifically address CLO's 1, 3, and 5.

Final Examination (30%): Students will be administered a final examination worth 30% of their final grade. The 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

- In order to receive a grade for this course, all course requirements must be met, and every assignment must be completed. Failure to complete any one assignment may result in a failing grade for this course.
- 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)	97% - 100%	A	93% - <97%	A (minus)	90% - <93%
B (plus)	85% - <90%	B	80% - <85%	B (minus)	75% - <80%
C (plus)	71% - <75%	C	67% - <71%	C (minus)	63% - <67%
D (plus)	59% - <63%	D	54% - <59%	D (minus)	50% - <54%
F	Below 50%				

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
Fall 2018 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.

Week	Date	Weekly Overview (Subject to Change)
1	08/22/18	**Introduction:** Course overview (flipped class, discussion, assignments, lectures, Canvas, etc.) *Readings* The Current State of Cybercrime Scholarship (Holt & Bossler) The Internet as a Conduit for Criminal Activity (Wall) *In-Class Discussion:* Welcome & Introduction
2	08/27/18	**What is Cybercrime:** Computer & Internet basics; Cybercrime research; Routine Activity Theory *Readings* Principles of Cybercrime Chapter 1: Cybercrime (Clough) Principles of Cybercrime Chapter 2: Computer as Target (Clough) *Supportive Readings* How does the Internet Work (Strickland) How Firewalls Work (Tyson) What is an 'IP Address' (Gil) *In-Class Discussion:* What is Cybercrime?
3	08/29/18 & 09/05/18	**Email Spam:** Phishing & Pharming; Legal issues; Legislation efforts *Readings* Principles of Cybercrime Chapter 9: Spam (Clough) *In-Class Discussion:* Combating Spam Internationally & Stealing Your Information
4	09/10/18 & 09/12/18	**Malware:** Viruses vs Worms vs Trojan Horses; Rootkits, Keyloggers, & Ransomware *Readings* Principles of Cybercrime Chapter 4: Modification or Impairment of Data ((Clough) Mobile Malware Evolution 2016 (Kaspersky Lab) Internet Security Report 2017 (ISTR) *In-Class Discussion:* **Malware Group Presentation**
5	09/17/18 & 09/19/18	**Social Media, and Identity Theft/Fraud:** Social networks & Search engines; Identity theft & fraud *Readings* Principles of Cybercrime Chapter 7: Fraud (Clough) What is Social Engineering (Webroot) *In-Class Discussion:* Social Engineering Checklist & Web Search *Guest Lecturer:* Trey Crawley

Week	Date	Weekly Overview (Subject to Change)
6	09/24/18 & 09/26/18	**Personal Security:** Privacy; Surveillance; Personal safety; The Secret War *Readings* The Secret War (Popular Mechanics) The Online Threat (Hersh) *In-Class Discussion:* Right to Privacy & Internet Surveillance *Guest Lecturer:* Dan Schott
7	10/01/18 & 10/03/18	**Copyright Infringement:** What is it?; Who owns the data on the Internet?; Peer-2-peer (piracy) *Readings* Principles of Cybercrime Chapter 8: Criminal Copyright Infringement (Clough) An Oral History of Napster (Fortune) *In-Class Discussion:* Role of ISPs and Tech Companies & Internet as an Open System **Paper #1 (Tell Me a Story) Due 10/03/18**
8	10/08/18 & 10/10/18	**Deep Web:** Dark vs Deep Web; How do you access it (TOR)?; Digital currency (e.g., Bitcoin) *Readings* Exploring the Deep Web (Trend Micro) Tor Project: Overview (TOR) What are BitCoins (Lifewire) How BitCoin Works (Forbes) *In-Class Discussion:* Silk Road, Red Rooms & Chloe Ayling *Guest Lecturer:* John Penn
9	10/15/18 & 10/17/18	**Organized Crime:** Carding; Money laundering; Drugs & weapons *Readings* 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) *In-Class Discussion:* **Data Breach Group Presentation**
10	10/22/18 & 10/24/18	**Sex Crimes:** Trafficking; Child sexual exploitation; Sexting; Revenge pornography *Readings* Principles of Cybercrime Chapter 10: Child Pornography (Clough) Principles of Cybercrime Chapter 11: Grooming (Clough) Fighting Human Trafficking (European Commission) *In-Class Discussion:* Sweetie & Vigilantism *Guest Lecturer:* Bryce Westlake
11	10/29/18 & 10/31/18	**Personal Cyber Crimes:** Stalking; Bullying *Readings* Principles of Cybercrime Chapter 12: Harassment (Clough) Principles of Cybercrime Chapter 13: Voyeurism (Clough) *In-Class Discussion:* Amanda Todd & Megan Meier

Week	Date	Weekly Overview (Subject to Change)
12	11/05/18 & 11/07/18	**Hacking:** Hacker culture; Legal issues; Hacking as a service *Readings* Hackers Manifesto (The Mentor) How Big and Powerful is Anonymous (Vandita) *In-Class Discussion:* *Guest Lecturer:* TBD
13	11/14/18 & 11/19/18	**Violent Extremism:** In the digital age; methods of distribution; researching online terrorism *Readings* How Modern Terrorism Uses the Internet (Weimann) Terrorism and the Internet (Conway) Exploring Stormfront (Bowman-Grieve) *In-Class Discussion:* Hacktivism vs Terrorism & Role of Companies in Combating Terrorism *Guest Lecturer:* Richard Frank or Ryan Scrivens
14	11/26/18 & 11/28/18	**Combating Cybercrime:** Patriot Act; Jurisdiction; International challenges; Joint operations *Readings* Principles of Cybercrime Chapter 14: Jurisdiction (Clough) Principles of Cybercrime Chapter 6: Interception (Clough) *In-Class Discussion:* International Combat *Guest Lecturer:* Brandon Epstein
15	12/03/18 & 12/05/18	**Cyber Forensics** *Readings* Digital Forensics as a Forensic Science Discipline (SWGDE) Collection of Digital and Multimedia Evidence Myths vs Facts (SWGDE) Best Practices for Computer Forensics (SWGDE) Digital and Multimedia Evidence (SWGDE) *In-Class Discussion:* *Guest Lecturer:* John Powell **Paper #2 (Combating Cybercrime Internationally) Due 12/05/18**
16	12/11/18	**Review** *Readings* None