

San José State University
Department of Justice Studies
JS 161: Introduction to Cybercrime
Spring 2017

COURSE AND CONTACT INFORMATION

Instructor: Jackson Sargent
Office Hours: By Appointment
Office Location: Virtual
Email: david.sargent@sjsu.edu
Class Day & Time: N/A
Classroom: Virtual
Prerequisites: JS 100W (or equivalent)

COURSE FORMAT

Online: 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 MyJSU 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.

LEARNING OUTCOMES

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

- ✓ Distinguish between the different types of cybercrimes, including who/what they target, how/where they are conducted, and why they persist.
- ✓ Describe the impacts of the Internet on the opportunities created for committing traditional crimes (e.g., bullying) and new crimes (e.g., phishing).
- ✓ Identify the challenges faced nationally and internationally at combating cybercrime and the steps taking by organizations to address these challenges.
- ✓ Take steps to increase their own security and privacy when online.
- ✓ Take what they have learned in class and apply it to current events.

REQUIRED TEXTS / READINGS

Textbooks

Yar, M. (2013). *Cybercrime and Society* (2nd Edition). Sage Publications. ISBN13: 978-1-4462-0194-7.

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

Online Discussion (25%): Active participation in discussions is a necessary and integral part of the course. Each week there will be an online discussion, through Canvas, on specific readings and key issues or current events related to that week's overall topic. Students will be expected to discuss the implications of the issue or event to our understanding of cybercrime and how it is addressed by societies.

Topic Paper – 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. Students will select a type of cybercrime discussed in the course and determine how partnerships/cooperation/resource-sharing could, realistically, be improved between United States and another nation of their choosing. Students will write a short paper (8 pages) on the laws, if any, that exist in each country and what each could learn from the other. The discussion should include how privacy and rights can be balanced with security. **The Topic Paper is due on Sunday April 30th.**

Midterm and Final Examinations (50%): Students will be administered a Midterm and a Final Examination, each worth 25% of their final grade. Each timed exam will occur online and will cover material from lectures (including all media presented) and assigned readings. Each exam will be non-cumulative and comprised of multiple choice, true/false, and short-answer questions.

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. *At the discretion of the course instructor, late assignments/papers may be subject to a deduction of 10% for every calendar day that they are late, including weekend days.*

Grade Scale

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

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/>.

COURSE SCHEDULE

Course topics are subject to change at the discretion of the instructor.

Week	Date	Topics	Readings
1	01/26/17	Introduction -Computer and Internet Basics -What is Cybercrime? -Cybercrime in Research	<i>Cybercrime and Society (Yar)</i> Chapter 1 (Cybercrime and the Internet) <i>Articles</i> How does the Internet work (Strickland) How Firewalls Work (Tyson) What is an 'IP Address' (Gil) The Current State of Cybercrime Scholarship (Holt & Bossler) The Internet as a Conduit for Criminal Activity (Wall)
2	01/30/17	Computer Crimes -Viruses, Worms, Malware, Rootkits, Keyloggers, Ransomware -International Espionage	<i>Principles of Cybercrime (Clough)</i> Chapter 4 (Modification or Impairment of Data) <i>Articles</i> Hackers Manifesto (The Mentor) Koobface: Inside a Crimeware Network (Villeneuve)
3	02/06/17	Hacking -Hacker Culture -Legal Issues -Hacking as a Service (DDos & Botnets)	<i>Cybercrime and Society (Yar)</i> Chapter 2 (Hackers, Crackers, and Viral Coders) <i>Principles of Cybercrime (Clough)</i> Chapter 1 (Cybercrime) & Chapter 2 (Computer as Target)

Week	Date	Topics	Readings
4	02/13/17	Copyright Infringement -Who Owns the Data on the Internet? -Piracy	<i>Cybercrime and Society (Yar)</i> Chapter 4 (Virtual Pirates) <i>Principles of Cybercrime (Clough)</i> Chapter 8 (Criminal Copyright Infringement)
5	02/20/17	Personal Security -Privacy -Surveillance -Personal Safety -The Secret War	<i>Cybercrime and Society (Yar)</i> Chapter 10 (Cybercrimes and Cyberliberties) <i>Articles</i> The Secret War (Popular Mechanics) The Online Threat (Hersh)
6	02/27/17	Your Online ID -Social Networks & Search Engines -ID Theft & Fraud	<i>Cybercrime and Society (Yar)</i> Chapter 5 (Cyber-Frauds, Scams, and Cons) <i>Principles of Cybercrime (Clough)</i> Chapter 7 (Fraud)
7	03/06/17	Email Spam -Phishing & Pharming -Legal Issues -Legislation Efforts	<i>Principles of Cybercrime (Clough)</i> Chapter 9 ('Spam')
8	03/13/17	MIDTERM EXAM	NO READINGS
9	03/20/17	Deep Web -TOR -Digital Currency -The Dark Web	<i>Articles</i> Tor Project: Overview (TOR) The Tor System (Philby) Why Tor Users Should Watch Out (Meyer) How Bitcoin Works (Forbes) Exploring the Deep Web (Trend Micro) What is the Dark Web (Egan)
--	03/27/17	SPRING RECESS	NO READINGS
10	04/03/17	Organized Crime -Carding, -Money Laundering -Drugs & Weapons	<i>Articles</i> The Great Cyberheist (Verini) A Hacker's Race to Build the Amazon.com of Stolen Credit Cards (WeirderWeb) Carders.cc Hacked (Reusablesec)
11	04/10/17	Personal Cyber-Crimes -Stalking -Bullying	<i>Cybercrime and Society (Yar)</i> Chapter 8 (The Victimization of Individuals Online) <i>Principles of Cybercrime (Clough)</i> Chapter 12 (Harassment) & Chapter 13 (Voyeurism)

Week	Date	Topics	Readings
12	04/17/17	Terrorism & Extremism -White Supremacists -Methods of Distribution	<i>Cybercrime and Society (Yar)</i> Chapter 3 (Political Hacking) <i>Articles</i> Terrorism and the Internet (Conway) Exploring Stormfront (Bowman-Grieve) How Modern Terrorism Uses the Internet (Weimann) Terror on the Internet (Tsfati & Weimann)
13	04/24/17	Sex Crimes -Trafficking -Child Sexual Exploitation -Sexting -Revenge Pornography	<i>Cybercrime and Society (Yar)</i> Chapter 7 (Child Pornography and Child Sex Abuse Imagery) <i>Principles of Cybercrime (Clough)</i> Chapter 10 (Child Pornography) & Chapter 11 (Grooming) Topic Paper Due: Combating Cybercrime Internationally
14	05/01/17	Cybercrime and the Law -Patriot Act -International Challenges -Jurisdiction -Joint Operations	<i>Cybercrime and Society (Yar)</i> Chapter 9 (Policing the Internet) <i>Principles of Cybercrime (Clough)</i> Chapter 14 (Jurisdiction) & Chapter 6 (Interception of Data)
15	05/08/17	REVIEW	NO READINGS
16	05/15/17	FINAL EXAM	NO READINGS