CJ 5363 - Cybercrime Law and Policy
Online
Sul Ross State University

Instructor: Jade Pumphrey, PhD
Email: jade.pumphrey@sulross.edu

Course Description: This course provides a comprehensive examination of cybercrime, digital forensics, and related legal frameworks in our increasingly interconnected world. Students will explore the technical, legal, and social dimensions of cybercrime, analyzing various forms of computer-related crimes, investigative techniques, and policy implications. The course examines the challenges faced by law enforcement in the digital age, including jurisdictional issues, privacy concerns, and the evolving nature of cyber threats.

Key topics include computer hacking, malware, digital piracy, online fraud, cyber harassment, child exploitation, cyber terrorism, and illicit online markets. Students will study both theoretical frameworks for understanding cybercrime and practical aspects of digital forensics and cybercrime investigation. The course also explores the intersection of technology, law, and policy in addressing cybercrime challenges.

Through this course, students will develop a thorough understanding of cybercrime investigation techniques, digital evidence handling, and the legal considerations in cyber investigations. By examining these complex issues, students will be equipped to understand and address the challenges of cybercrime in modern society.

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

Understand Cybercrime Foundations

- Define various forms of cybercrime and their technical underpinnings
- Analyze the evolution of cybercrime and digital forensics
- Identify key legal frameworks governing cybercrime investigation
- Examine the role of law enforcement in addressing cyber threats

Master Technical and Investigative Concepts

- Understand basic computer and network security principles
- Analyze different types of cyber attacks and malware
- Evaluate digital forensics techniques and evidence handling

- Apply criminological theories to cybercrime

Explore Legal and Policy Frameworks

- Analyze privacy and security challenges in cybercrime investigation
- Evaluate jurisdictional issues in cyber investigations
- Understand legal requirements for digital evidence collection
- Assess policy responses to emerging cyber threats

Develop Practical Investigation Skills

- Understand digital forensics procedures and best practices
- Evaluate evidence acquisition and examination techniques
- Analyze legal challenges in digital investigations
- Apply appropriate investigation methods to different types of cybercrime

Required Materials

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2022). *Cybercrime and digital forensics: An introduction* (3rd ed.). Routledge. ISBN: 9780367360078

Supplemental Materials:

- Access to academic journals through the university library
- Statistical resources from government websites
- Case studies provided through Blackboard
- Additional readings posted in weekly modules

Module Assignments

Module 1: Introduction to Technology and Cybercrime Discussion Question: *Week 1: Digital Crime Foundations* **Assignment:** Cybercrime Analysis Paper

- Analyze current trends in cybercrime
- Evaluate technological factors enabling cyber offenses
- Assess implications for law enforcement

Module 2: Law Enforcement and Privacy Discussion Question: *Week 2: Balancing Security and Rights* **Assignment:** Privacy Impact Analysis

- Compare privacy protections across jurisdictions
- Analyze law enforcement challenges
- Propose balanced solutions

Module 3: Hacking and Technical Attacks Discussion Question: *Week 3: Understanding Cyber Threats* **Assignment:** Hacking Case Study Analysis

- Examine a significant hacking incident
- Analyze attack methods and impacts
- Evaluate prevention strategies

Module 4: Malware and Automated Attacks Discussion Question: *Week 4: Evolution of Cyber Threats* **Assignment:** Malware Analysis Report

- Analyze types of malware
- Evaluate automated attack patterns
- Propose detection and prevention strategies

Module 5: Digital Piracy and IP Theft Discussion Question: *Week 5: Protecting Digital Assets* **Assignment:** IP Protection Strategy Analysis

- Analyze digital piracy trends
- Evaluate IP protection methods
- Propose enforcement strategies

Module 6: Online Fraud and Financial Crime Discussion Question: *Week 6: Following Digital Money* **Assignment:** Cybersecurity Incident Simulation Report

- Analyze online fraud methods
- Evaluate investigation techniques
- Propose prevention strategies

Module 7: Digital Exploitation Crimes Part 1 Discussion Question: *Week 7: Addressing Digital Exploitation* **Assignment:** Policy Analysis Paper

- Analyze current legislation
- Evaluate enforcement challenges
- Propose policy improvements

Module 8: Digital Exploitation Crimes Part 2 Discussion Question: *Week 8: Protecting Vulnerable Populations* **Assignment:** Comparative Analysis of Legal Remedies Presentation

- Develop comprehensive protection strategies
- Address investigation challenges
- Propose prevention measures

Module 9: Cyberbullying and Harassment Discussion Question: *Week 9: Digital Age Harassment* **Assignment:** Intervention Strategy

- Analyze cyberbullying patterns
- Evaluate current interventions
- Propose improved solutions

Module 10: Extremism and Cyberterror Discussion Question: *Week 10: Online Radicalization* **Assignment:** Threat Assessment Report

- Analyze online extremism patterns
- Evaluate counter-measures
- Propose prevention strategies

Module 11: Cyberwarfare and Information Operations Discussion Question: *Week 11: State-Level Cyber Threats* **Assignment:** Information Warfare Analysis

- Analyze state-sponsored cyber operations
- Evaluate defense strategies
- Assess policy implications

Module 12: Underground Markets Discussion Question: *Week 12: Dark Web Operations* **Assignment:** Dark Market Analysis

- Analyze illicit market operations
- Evaluate investigation techniques
- Propose enforcement strategies

Module 13: Criminological Theories in Cybercrime Discussion Question: *Week 13: Understanding Cyber Offenders* **Assignment:** Theory Application Paper

- Apply criminological theories to cybercrime
- Analyze offender motivations
- Evaluate prevention implications

Module 14: Digital Forensics Evolution and Practice Discussion Question: *Week 14: Modern Digital Investigation* **Assignment:** Forensics Procedure Analysis

- Analyze forensic techniques
- Evaluate evidence handling
- Propose best practices

Module 15: Legal Challenges in Cyber Investigation Discussion Question: *Week 15: Digital Evidence Challenges* **Assignment:** Legal Framework Analysis

- Analyze legal requirements
- Evaluate jurisdictional challenges
- Propose policy solutions

Module 16: Future of Cybercrime and Policy Discussion Question: *Week 16: Tomorrow's Challenges* **Assignment:** Vision Paper

- Analyze emerging threats
- Evaluate future challenges
- Propose adaptive strategies

Class Schedule and Reading Assignments

Week	Dates	Module	Required Reading	Assignments
1	Jan 15 - Jan 19	Introduction to Technology and Cybercrime	Chapter 1: Technology and Cybercrime	Discussion: Digital Crime Foundations (Thu/Sun) Assignment: Cybercrime Analysis Paper (Sun)
2	Jan 20 - Jan 26	Law Enforcement and Privacy	Chapter 2: Law Enforcement, Privacy, and Security in Dealing with Cybercrime	Discussion: Security and Rights (Thu/Sun) Assignment: Privacy Impact Analysis (Sun)
3	Jan 27 - Feb 2	Computer Hackers and Hacking	Chapter 3: Computer Hackers and Hacking	Discussion: Cyber Threat Analysis (Thu/Sun) Assignment: Hacking Case Study (Sun)
4	Feb 3 - Feb 9	Malware and Automated Attacks	Chapter 4: Malware and Automated Computer Attacks	Discussion: Automated Threats (Thu/Sun) Assignment: Malware Analysis (Sun)
5	Feb 10 - Feb 16	Digital Piracy and IP Theft	Chapter 5: Digital Piracy and Intellectual Property Theft	Discussion: IP Rights (Thu/Sun) Assignment: Piracy Case Analysis (Sun)
6	Feb 17 - Feb 23	Online Fraud	Chapter 6: Online Fraud	Discussion: Digital Fraud (Thu/Sun) Assignment: Cybersecurity Incident Simulation Report (Sun)

7	Feb 24 - Mar 2	Digital Exploitation Part 1	Chapters 7 & 8: Pornography, Image-Based Sexual Abuse, and CSEM Offenses	Discussion: Exploitation Issues (Thu/Sun) Assignment: Policy Analysis (Sun)
8	Mar 3 - Mar 9	Cyberbullying and Harassment	Chapter 9: Cyberbullying, Online Harassment, and Cyberstalking	Discussion: Online Harassment (Thu/Sun) Assignment: Comparative Analysis of Legal Remedies Presentation (Sun)
9	Mar 10 - Mar 16	Online Extremism	Chapter 10: Online Extremism and Cyberterror	Discussion: Digital Extremism (Thu/Sun) Assignment: Threat Analysis (Sun)
-	**Mar 17 - - Mar 23**	**SPRING BREAK - NO CLASSES**	-	-
10	Mar 24 - Mar 30	Cyberwarfare and Info Operations	Chapter 11: Cyberwarfare and Information Operations	Discussion: Information Warfare (Thu/Sun) Assignment: Cyber Ops Analysis (Sun)
11	Mar 31 - Apr 6	Illicit Markets	Chapter 12: Illicit Market Operations Online	Discussion: Dark Markets (Thu/Sun) Assignment: Market Analysis (Sun)
12	Apr 7 - Apr 13	Criminological Theories	Chapter 13: Cybercrime and Criminological Theories	Discussion: Theory Application (Thu/Sun) Assignment: Theory Paper (Sun)
13	Apr 14 - Apr 20	Digital Forensics Evolution	Chapter 14: Evolution of Digital Forensics	Discussion: Forensic Evolution (Thu/Sun) Assignment: Forensics Report (Sun)

14	Apr 21 - Apr 27	Evidence Acquisition and Analysis	Chapter 15: Acquisition and Examination of Forensic Evidence	Discussion: Evidence Handling (Thu/Sun) Assignment: Evidence Analysis (Sun)
15	Apr 28 - May 4	Legal Challenges	Chapter 16: Legal Challenges in Digital Forensic Investigations	Discussion: Legal Framework (Thu/Sun) Assignment: Legal Brief (Sun)
16	May 5 - May 7	Future of Cybercrime and Policy	Chapter 17: The Future of Cybercrime, Terror, and Policy	Discussion: Future Trends (Wed) Final Assignment: Vision Paper (Wed)

Assessment Structure

Component	Points	Percentage	Details
Weekly Discussions	1600	25%	16 discussions @ 100 points each
Module Assignments	1500	60%	15 assignments @ 100 points each
Final Policy Analysis	200	15%	Policy analysis paper
Total	3300	100%	

Grade Distribution

Grade	Percentage	Points
A	90-100%	2970–3300
B	80-89%	2640–2969
C	70-79%	2310–2639

D	60-69%	1980–2309
F	Below 60%	Below 1980

Technology Requirements

Blackboard is an integral course management tool for this class. Regularly checking Blackboard is mandatory to stay updated on course developments. Throughout the course, several Blackboard features will be utilized, including email, course documents, the discussion board, grade center, external links, and SafeAssign.

This course requires significant online activity. To participate and progress, students must have:

1. **Basic Computer Skills**
    - Sending and retrieving emails
    - Opening and attaching files for course assignments
    - Locating websites and resources on the internet
2. **Internet Connectivity**
    - Regular access to the internet
    - Alternative locations for internet access (e.g., on-campus library, friend's house)

Any additional reading materials, resources, and other information will be posted in Blackboard under the heading "Materials." Students will be notified on how to access this information by the instructor via email and Blackboard announcements.

Assessment Rubric

- **Assignments**: Graded with a rubric created by the instructor. Students will have access to their grades via the Blackboard grade center, along with feedback on correct responses.
- **Discussion Forums**: Graded based on a rubric, outlining expectations and point allocation. Feedback will be given alongside the grade after the instructor has evaluated the discussion.

Any student needing special assistance for any class aspect should contact the instructor immediately.

Support for Students with Disabilities

Qualified students with disabilities needing accommodations to ensure full participation in programs, services, and activities at Sul Ross State University should contact the Disability Services Coordinator in Counseling and Prevention Services, Ferguson Hall 112, Box C-117, at (837-8203).

ADA Statement: Sul Ross State University is committed to equal access in compliance with the Americans with Disabilities Act of 1973. Students with qualifying disabilities who seek

accommodations must initiate a request for a meeting for accessibility services. Contact Rebecca Greathouse Wren, M.Ed., LPC-S, Counseling & Accessibility Services at 432-837-8203 or via email at rebecca.wren@sulross.edu. More information can be found here.

Distance Education Statement

Students enrolled in distance education courses have equal access to the university's academic support services, library resources, and instructional technology support. For more information about accessing these resources, visit the SRSU website. Online assignments should be submitted through Blackboard or SRSU email, which requires secure login information to verify students' identities and protect their information. Procedures for filing a student complaint are included in the student handbook. Students in web-based courses must adhere to all policies pertaining to academic honesty and appropriate student conduct, as described in the student handbook. Maintaining appropriate equipment and software is required according to the course's needs and requirements, as outlined on the SRSU website.

Attendance

Students are expected to regularly check Blackboard for assignments and pertinent information. The Department of Criminal Justice emphasizes that attendance is a direct predictor of student success. Therefore, CJ faculty will enforce a strict attendance policy. Students must log in for updates, assignments, discussion boards, etc. Failure to log in will result in being dropped from the course for failure to attend.

It is the student's responsibility to inform the instructor of any events that would prevent participation. Students may email the instructor. Attendance demonstrates maturity, responsibility, and a serious attitude toward education. Many times, students seek letters of recommendation from their instructors. Prospective employers or graduate programs are all interested in a student's class attendance record.

Academic Dishonesty/Plagiarism

In the learning environment, professional attitude begins in the classroom. Students and faculty will not tolerate or commit any form of academic dishonesty. This includes:

- Copying work from any source
- Assisting or allowing another to commit academic dishonesty
- Sharing answers during a test or in submitting an assignment
- Claiming another's work, data, or creative efforts as your own
- Resubmitting graded assignments for multiple classes
- Providing false information about your academic performance to the college

To avoid plagiarism, do not "copy and paste" into assignments without using proper quotation marks and citing the source in APA format.

Unauthorized Use of AI Tools

The unauthorized use of AI tools is considered academic dishonesty. Examples include:

- Using AI to generate essay content and submitting it as your own work without proper attribution.
- Allowing AI tools to complete assignments or quizzes on your behalf.
- Copying responses generated by AI and presenting them as original ideas or answers.
- Using AI to rephrase or paraphrase your own work or another's work.

Plagiarism Rules and Resources

- **Direct Quotes**: Should be used very sparingly. Always provide a citation and use quotation marks or indented quotes for direct quotes.
- **Paraphrasing/Indirect Quotations**: Provide a citation even if you change the sentence structure or words.
- **Using Others' Ideas**: Cite the source of ideas that are not your own, even if written in your words.
- **Collaborative Work**: Acknowledge all contributors when submitting collaborative work.

Consequences of Academic Dishonesty/Plagiarism

Violations of academic policy are documented and may result in:

- Reduction in grade on the assignment
- No credit on the assignment
- A failing grade for the course
- Suspension or dismissal from the college

Dropping the Course

Students who wish to drop the class should follow the procedures outlined by Sul Ross State University. Failure to do so may result in an "F" grade. Consult the Sul Ross State University Student Handbook and/or university catalog for details.

Library

The Bryan Wildenthal Memorial Library in Alpine offers FREE resources and services to the entire SRSU community. Access and borrow books, articles, and more by visiting the library's website at library.sulross.edu. Off-campus access requires logging in with your LoboID and password.

Librarians are a tremendous resource for your coursework and can be reached in person, by email at srsulibrary@sulross.edu, or by phone at 432-837-8123.

In some cases, you can borrow textbooks from the library. WorldCat allows you to be linked to libraries across America. If you find the book in the system, fill out a request form at the library.

Netiquette

Netiquette guidelines govern online behavior. All participants in the course are expected to contribute to the learning environment in a respectful manner when posting information. Additionally, academic discourse is expected. The link below provides helpful reminders and can be used as a guide to assist students when posting information online in this course.

Netiquette Guidelines