

# CJUS 5100.900 Cyber Crime & Victimization

**Instructor:** Jessica Craig, Ph.D.

**Term:** Summer I 2026

## **INSTRUCTOR'S CONTACT INFORMATION**

Office location: Chilton 273A

Phone: 940-565-3464

E-mail (preferred): [Jessica.Craig@unt.edu](mailto:Jessica.Craig@unt.edu)

Office hours: By appointment (virtual)

Connect with me through email and/or by attending office hours. During busy times, my inbox becomes rather full, so if you contact me and do not receive a response within two business days, please send a follow-up email. A gentle nudge is always appreciated. Finally, please know I can only discuss grades over email if it was sent through your Eagle Connect email account ([username@unt.edu](mailto:username@unt.edu)).

## **Course Description**

The purpose this course is provide students with a general understanding of cyber crime, cyber deviance, and cyber victimization. Students will develop a thorough understanding of the issues confronting the criminal justice system resulting from the expansion of the internet and internet of things (IoT). Theoretical explanations of cyber crime and deviance as well as cyber victimization will also be examined.

## **Course Structure**

This course will take place completely online through Canvas. The course is composed of weekly modules containing relevant chapter outlines and supplementary materials. Throughout our accelerated 5-week term, you will participate in two discussion boards, write two reaction essays, and complete one comprehensive final paper.

## **Course Objectives**

At the completion of this course, you should be able to:

- ✓ Discuss the evolving nature of cyber crime and cyber victimization.
- ✓ Differentiate between and discuss the issues associated with the types, nature, and extent of cyber crime and cyber victimization.
- ✓ Describe legislation associated with cyber crime as well as issues associated with the investigation and prosecution of cyber crime.
- ✓ Explain the unique role of each criminal justice agency in responding to cyber crime.
- ✓ Discuss future trends associated with cyber crime, deviance, and victimization.

## **Required Materials**

There are three required texts for the course listed below. Reading assignments and additional readings are outlined in the Course Calendar at the end of this document.

Bilton, N. (2018). *American kingpin: The epic hunt for the criminal mastermind behind the Silk Road*. Penguin. ISBN-13: 978-1591848141

Mitnick, K. (2011). *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. Little, Brown and Company. ISBN-13: 978-0316037709.

Taylor, R. W., Fritsch, E. J., Liederbach, J., Saylor, M. R., & Tafoya, W. L. (2024). *Cyber Crime and Cyber Terrorism* (5th ed.). New York, NY: Pearson. ISBN-13: 9780134846514

## Course Requirements

This course is made up of a series of assignments designed to assist you in achieving the course learning objectives. You can expect your grades and feedback to be released to you within 4 business days of submission. There is a total of **450 points** that can be earned in this class.

<i>Assignment</i>	<i>Points Possible</i>	<i>% of Final Grade</i>
<i>Discussion Boards (2 @ 50 pts each)</i>	<i>100 points</i>	<i>22%</i>
<i>Reaction Essays (2 @ 100 pts each)</i>	<i>200 points</i>	<i>44%</i>
<i>Final Paper</i>	<i>150 points</i>	<i>33%</i>
<i>Total Points Possible</i>	<i>450 points</i>	<i>100%</i>

Grading Scale: 405 - 450 = A

360 - 404 = B

315 - 359 = C

270-314 = D

269 or fewer points = F

### Discussion Posts (100 points total)

Since this is a fully online course, our discussion boards are the heart of our classroom community — the space where we explore concepts together, challenge each other's thinking, and build on one another's ideas. You will complete two discussion boards across the five-week term (Weeks 1 and 3), each worth 50 points for a total of 100 points toward your final grade.

- **Your Initial Post:** Write an original, well-supported response to the weekly prompt. Posts should be 400–500 words (excluding references) and must draw on the assigned readings and at least one additional peer-reviewed source. Back every argument with evidence — assertions without support will not earn full credit.
- **Engaging with Peers:** You must reply to at least one classmate in a substantive response of 150–200 words. Your reply should directly engage a specific argument your classmate made — either extending its logic or identifying a weakness in it. Simply agreeing, summarizing, or pivoting to an unrelated point will not earn full credit.
- **Post-First Rule:** You must submit your initial post before Canvas will allow you to view your peers' threads. Submitting a blank or placeholder post to unlock the board will result in a zero for the entire assignment.
- **Grading:** Posts are evaluated across four criteria: the quality of your ideas, arguments, and analysis; your engagement with and citation of course materials; your contribution to the learning community; and your writing quality and professional mechanics. A detailed rubric is available on Canvas — review it before posting.

### Reaction Essays (200 points total)

Throughout the term, you will complete two reaction essays worth 100 points each, for a total of 200 points toward your final grade. These essays provide an opportunity for you to critically evaluate and respond to our assigned readings.

- **Expectations:** At the graduate level, these essays should go beyond simple summaries. Your goal is to critically analyze the material, synthesize different viewpoints, and articulate your own evidence-based scholarly reaction to the topics.

- Logistics & Formatting: Specific prompts and detailed instructions can be found in the Writing a Reaction Essay guidance page on Canvas. Essays should be 4–6 pages of core text — title pages, reference lists, headers, and extra spacing do not count toward the minimum.
- AI Disclosure: Any use of Generative AI beyond spellcheck must be disclosed at the bottom of your essay per the course AI policy. Using AI to draft, brainstorm, or generate reasoning for any portion of your essay constitutes academic misconduct.

### **Final Paper (150 points)**

As the capstone to our course, you will write a comprehensive final paper that synthesizes the diverse concepts, theories, and positions we have explored over the past five weeks. The final paper is worth 150 points and counts as 33% of your final grade.

- Expectations: This assignment is your chance to demonstrate a thorough, integrated understanding of cyber crime and victimization. Rather than summarizing existing literature, you will apply course concepts analytically to a real-world cybercrime incident. Because of the accelerated 5-week schedule, I highly recommend taking detailed notes on your readings each week — the paper will be significantly easier to write if you have been building your analysis throughout the term.
- Logistics & Formatting: Your final paper should be 10–12 pages of core text — title pages, reference lists, headers, the AI Reflection Statement, and extra spacing do not count toward the minimum. Format with double spacing, 12-point font, and 1-inch margins, and submit through Canvas as a Microsoft Word document by June 18, 11:59 PM.
- Grading: A detailed prompt and grading rubric are available on Canvas so you know exactly how your work will be evaluated.
- AI Disclosure: This assignment requires a mandatory AI Reflection Statement (see the prompt for details). Your case selection, theoretical analysis, and policy proposals must be entirely your own intellectual work. Using AI to generate analysis or fabricate citations is academic misconduct and will result in a zero and a formal referral to the Office of Student Conduct.

### **COURSE NOTES AND RECOMMENDATIONS**

Please make sure to have your official UNT email forwarded to your preferred email address (if different) to receive important updates, changes, announcements, class cancellations (if applicable), and generally, so I can reach you if necessary. The announcement board in Canvas, and email, will be used for primary communication to the class as a whole. I advise you check the announcements section frequently. It is your responsibility to utilize a computer system that works and is compatible with Canvas.

Important: Minimum technology requirements for this course: a browser that is compatible with Canvas (visit [this link](#) to ensure your browser is suitable) and Microsoft Office Word (or a similar word-processing software). Microsoft Office 365 is available for free to all currently-enrolled students. For instructions to download the software, please see [this link](#). Students are expected to know how to access their UNT email, open attachments, and use Microsoft Word (or a similar word-processing software). Students facing IT issues should visit [UNT's IT website](#) or the [IT Helpdesk](#). Students are also expected to have basic digital literacy skills such as using UNT's library's website, searching online databases, and properly citing information sources. Here is a [UNT Library Guide for Criminal Justice students](#) that walks you through how to find research and official sources online.

## **CLASS POLICIES**

### **Academic Dishonesty/Integrity**

Students caught cheating or plagiarizing will receive a "0" for that particular assignment or exam. Additionally, the incident will be reported to the Dean of Students, who may impose further penalty. According to the UNT catalog, the term "cheating" includes, but is not limited to: a. use of any unauthorized assistance in taking quizzes, tests, or examinations; b. dependence upon the aid of sources beyond those authorized by the instructor in writing papers, preparing reports, solving problems, or carrying out other assignments; c. the acquisition, without permission, of tests or other academic material belonging to a faculty or staff member of the university; d. dual submission of a paper or project, or resubmission of a paper or project to a different class without express permission from the instructor(s); or e. any other act designed to give a student an unfair advantage. The term "plagiarism" includes, but is not limited to: a. the knowing or negligent use by paraphrase or direct quotation of the published or unpublished work of another person without full and clear acknowledgment; and b. the knowing or negligent unacknowledged use of materials prepared by another person or agency engaged in the selling of term papers or other academic materials.

### **AI Tools & Academic Integrity**

This course is about your ability to understand, apply, and critique criminological theories; that intellectual work must come from you, not from AI tools. Generative AI (e.g., ChatGPT, Claude, Gemini, Copilot, Grammarly) may be used only as a support tool for mechanics and limited research help, never as a substitute for your own analysis.

Allowed (support only – “green zone”): You may use AI to proofread for grammar and clarity after you have written your own work, to assist with APA formatting, and to help locate or preliminarily summarize sources that you then independently verify and read.

Use with caution (“yellow zone”): AI use for brainstorming case ideas or explaining theories as a study aid is generally discouraged because it can short-circuit your own critical thinking; if you choose to do this, you must still do the reading yourself and must not use AI-generated phrasing or reasoning in submitted work.

Prohibited (“red zone”): You may not use AI on quizzes, tests, or discussion posts, and you may not fabricate or “hallucinate” sources, data, or citations with AI. Submitting AI-generated reasoning or text as your own work is considered academic misconduct and may be referred to the Office of Student Conduct.

Transparency: Any AI use beyond basic spell-check must be clearly disclosed and cited in APA format, following assignment instructions (for example, in the required AI Reflection Statement for the final project). When in doubt about whether a use of AI is appropriate, you are responsible for asking me before using it.

### **Make-Up, Late Work & Authorized Absence Policy**

Make-up exams, assignments, and late work will only be accepted when an absence or missed deadline is authorized according to UNT policy. Authorized absences include religious holy days, official university functions (including university-sponsored activities), required military service, student pregnancy/parenting (Title IX), university closure, and other documented extenuating circumstances approved by the Dean of Students. If you anticipate an authorized absence, you must notify me as soon as possible—preferably before the due date—and provide written documentation.

Absences for school-sponsored activities require prior approval from the department chair and academic dean, along with authorized absence documentation from the Dean of Students. Requests for excused absences for religious holy days must be made in writing within the university’s prescribed time frame. Late work is generally not accepted unless linked to a documented authorized absence, in which case it will be treated under the same guidelines as make-up work. For unexpected emergencies, notify me as soon as possible. Students with excused absences will be granted a reasonable period—no fewer than 5 business days—to complete missed work unless otherwise specified.

If you have questions about what qualifies as an authorized absence or need assistance, please consult UNT’s Student Attendance and Authorized Absences policy or contact the Dean of Students. While I want all students to succeed, withdrawal may sometimes be the best option for those facing significant challenges. The last day to withdraw with a “W” is June 11, 2026.

### **Student Behavior and University Policy:**

I value the many perspectives students bring to our campus. Please work with me to create a classroom culture of open communication, mutual respect, and inclusion. All discussions should be respectful and civil. Although disagreements and debates are encouraged, personal attacks are unacceptable. Together, we can ensure a safe and welcoming classroom for all. If you ever feel like this is not the case, please stop by my office and let me know. We are all learning together.

To be successful at learning and understanding the material in this class, it is essential that you read and complete the assigned material and engage in thoughtful discussions. Your active participation, along with your willingness to engage in thoughtful discussions will be taken into account at all times during the semester. Certain topics in criminal justice policy are controversial, thus discussion may become heated where there will be disagreements. The classroom is a place to express ideas, opinions, and engage in thoughtful discussions. Students will respect the views and opinions of others at all times. While I do not foresee any problems, if problems do arise, I will address them with the individual student. Below are general guidelines for how to communicate well in a classroom—both in-person and online.

- Remember that college communication is still professional communication. Use correct spelling and grammar and always double-check your response before hitting send or reply. Do not use slang and limit the use of emoticons.
- Use standard, readable fonts, sizes, and colors and avoid writing in all caps.
- Use your instructor's title of "Dr." or "Professor," or if you don't know use "Mr." or "Ms." Do not use "Mrs." to address female instructors unless told otherwise by said instructor.
- Be mindful of tone in online communication as it lacks the nonverbal cues of face-to-face communication that provide clarity and context to conversations.
- Respect the personal identities of others based on gender, sexuality, race, ethnicity, class, and/or culture.
- Respect the privacy of yourself, your instructor, and your peers. Keep in mind what you reveal and do not reveal, particularly if this information involves personal health and/or classroom performance, such as grades.
- Give people the benefit of the doubt. Though there may be a computer between you, there are people on the other side of the screen.
- Do not make assumptions about others' technological skills. Technological skills vary across a variety of factors, including experience, age, culture, etc.
- Read these [Core Rules of Netiquette](#) for additional tips about online communication.

#### *Communicating via Email*

- Check the syllabus before asking a question about the course and let the instructor know you checked the syllabus before asking. Instructors put a lot of time into making syllabi as comprehensive as possible for students.
- Use a descriptive subject line to get the instructor's attention. Instructors receive a lot of emails and a descriptive subject line helps them identify student inquiries more efficiently.
- Be concise and to the point.
- For a sample email, read this article, ["How to Email Your Professor."](#)

#### *Discussion Board Communication*

- Treat your posts like the professional communication that they are. Use correct spelling and grammar and always double-check a response before hitting send or reply. Do not use slang and limit the use of emoticons.
- Read all the messages in a thread before replying so you do not repeat something one of your peers may have already said.
- Avoid replies such as "I agree" and instead explain why you agree or do not agree.
- Show your work by sharing resources and utilizing citations.
- When disagreeing, do not make personal attacks or use language that discriminates based on gender, sexuality, race, ethnicity, class, and/or culture.

#### **Office of Disability Accommodation**

The University of North Texas makes reasonable academic accommodation for students with disabilities. Students seeking reasonable accommodation must first register with the Office of Disability Access (ODA) to verify their eligibility. If a disability is verified, the ODA will provide you with a reasonable accommodation letter to be delivered to faculty to begin a private discussion regarding your specific needs in a course. You may request reasonable accommodations at any time, however, ODA notices of reasonable accommodation should be provided as early as possible in the semester to avoid any delay in implementation. Note that students must obtain a new letter of reasonable accommodation for every semester and must meet with each faculty member prior to implementation in each class. Students are strongly encouraged to deliver letters of reasonable accommodation during faculty office hours or by appointment. Faculty members

have the authority to ask students to discuss such letters during their designated office hours to protect the privacy of the student. For additional information, refer to the [Office of Disability Access website](#). You may also contact ODA by phone at (940) 565-4323.

### **Student Evaluation of Instruction**

Student feedback is important and an essential part of participation in this course. The student evaluation of instruction is a requirement for all organized classes at UNT. This short survey will be made available at the end of the semester to provide you with an opportunity to evaluate how this course is taught.

### **Syllabus Changes**

I reserve the right and have the discretion to change this syllabus. While every effort will be made to follow this syllabus as closely as possible, it is sometimes the case that the syllabus must be modified. In the case that the syllabus needs to be adjusted, I will announce such adjustments to the class. I will make every effort to ensure that any changes to the syllabus benefit the class as a whole. It is the student's responsibility to check announcements/email so that any and all syllabus changes are documented. Failure to obtain syllabus changes because of failure to check and read announcements does not constitute a defense against missed assignments, test dates, and other applicable changes.

### **Miscellaneous:**

The material posted online is my personal intellectual property or that of the University of North Texas. You may not utilize the material for other than class purposes. Class recordings are reserved for use only by students in this class for educational purposes. The recordings should not be shared outside the class in any form. Failing to follow this restriction is a violation of the UNT Code of Student Conduct and could lead to disciplinary action.

### **Emergency Notification & Procedures**

UNT uses a system called [Eagle Alert](#) to quickly notify you with critical information in the event of an emergency (i.e., severe weather, campus closing, and health and public safety emergencies like chemical spills, fires, or violence). The system sends voice messages (and text messages upon permission) to the phones of all active faculty staff, and students. Please make certain to update your phone numbers at [my.unt.edu](#). Some helpful emergency preparedness actions include: 1) know the evacuation routes and severe weather shelter areas in the buildings where your classes are held, 2) determine how you will contact family and friends if phones are temporarily unavailable, and 3) identify where you will go if you need to evacuate the Denton area suddenly. In the event of a university closure, please refer to Canvas for contingency plans for covering course materials.

### **Retention of Student Records**

Student records pertaining to this course are maintained in a secure location by the instructor of record. All records such as exams, answer sheets (with keys), and written papers submitted during the duration of the course are kept for at least one calendar year after course completion. Course work completed via the Canvas online system, including grading information and comments, is also stored in a safe electronic environment for one year. You have a right to view your individual record; however, information about your records will not be divulged to other individuals without the proper written consent. You are encouraged to review the Public Information Policy and the Family Educational Rights and Privacy Act (FERPA) laws and the university's policy in accordance with those mandates at this [link](#). Information regarding data privacy for Canvas can be found [at this link](#).

### **Sexual Assault Prevention**

UNT is committed to providing a safe learning environment free of all forms of sexual misconduct. Federal laws and UNT policies prohibit discrimination on the basis of sex as well as sexual misconduct. If you or someone you know is experiencing sexual harassment, relationship violence, stalking and/or sexual assault, there are campus resources available to provide support and assistance. The Survivor Advocates can be reached at [SurvivorAdvocate@unt.edu](mailto:SurvivorAdvocate@unt.edu) or by calling the Dean of Students Office at 940-565-2648. Visit [Title IX Student Information](#) (Links to an external site) for more resources.

### **F1 Visa Holder Regulation**

Federal regulations state that students may apply only 3 fully-online semester credit hours (SCH) to the hours required for full-time status for F1 Visa holders. Full-time status for F1 Visa students is 12 hours for undergraduates and 9 hours for graduate students. Instructors teaching online courses should insert information into the syllabus to make F1 Visa students aware of this limitation and provide them with information about options to complete an on-campus experiential component in a course that is otherwise fully-online.

If a F-1 Visa holder intends to take more than 3 SCH of online courses in a term, they will need to document the on-campus experiential component of all courses that exceed the 3-hour limit. This on-campus experiential component can be satisfied in a number of ways including a face-to-face test, lab work, a required on-site lecture, mandatory library orientation, etc. Instructors should develop an option to assist students who request an on-campus experiential component to meet the federal regulation. Instructors should have students requesting this assistance to complete the On-campus Component Reporting Form for Online Courses which requires both the student and the instructor's signature. The instructor should make a copy for the student's departmental file and send a copy to the UNT International Student and Scholar Services (routing address on the form).

## ACADEMIC CALENDAR

*Reading Access Note: All journal articles and reports listed below are available through the Course Library Guide, which students can access directly through Canvas.*

<b>Week / Dates</b>	<b>Topic &amp; Focus</b>	<b>Required Readings</b>	<b>Assignments &amp; Due Dates</b>
<b>Week 1</b> May 18–23	Foundations of Cyber Crime & Measurement	- Taylor et al., Chapter 1 - <i>Large-scale measurement of cybercrime against individuals</i> - <i>An Environmental Scan of Cybercrime Measurement: Recommendations for the NCVS</i> (excerpts)	Discussion 1 - Initial post due May 21, 11:59 PM - Reply due May 24, 11:59 PM
<b>Week 2</b> May 24–30	Offending, Hackers, and Decision-Making	- Taylor et al., Chapter 3 - Mitnick, <i>Ghost in the Wires</i> - <i>Pathways to criminal hacking</i>	Reaction Essay 1 (on <i>Ghost in the Wires</i> ) due May 31, 11:59 PM
<b>Week 3</b> May 31– June 6	Cyber Victimization and Online Harms	- Taylor et al., Chapter 8 - <i>Sex, age, and cyber-victimization</i> - <i>Understanding cyber victimization</i>	Discussion 2 - Initial post due June 4, 11:59 PM - Reply due June 7, 11:59 PM
<b>Week 4</b> June 7– 13	Dark Web Markets, AI, and Cybercrime Ecosystems	- Bilton, <i>American Kingpin</i> - <i>The ‘Yelp-ification’ of the Dark Web</i> - <i>AI and Serious Online Crime</i> (excerpts)	Reaction Essay 2 (on <i>American Kingpin</i> ) due June 14, 11:59 PM
<b>Week 5</b> June 14–18	Law, Policy, and Policing	- Taylor et al., Chapter 10 - <i>Hacking cybersecurity law</i> (excerpts) - <i>Understanding cybercrime in ‘real world’ policing and law enforcement</i>	Final Paper due June 18, 11:59 PM

## Detailed Required and Optional Readings

**Note for Students:** Full citations and specific instructions for each reading listed in the course calendar (including which excerpts or sections to read) appear below. All articles and reports are available through the **CJUS Course Library Guide** linked in Canvas.

### Weekly Required Readings

#### Week 1

- Taylor et al., Chapter 1
- Breen, J., Herley, C., & Redmiles, E. M. (2022). A large-scale measurement of cybercrime against individuals. *Proceedings of the CHI Conference on Human Factors in Computing Systems*.
- *An Environmental Scan of Cybercrime Measurement: Recommendations for the NCVS* (2023).
  - Executive Summary only

#### Week 2

- Taylor et al., Chapter 3
- Mitnick, *Ghost in the Wires*
- Martineau, M., Spiridon, E., & Aiken, M. (2024). Pathways to criminal hacking: Connecting lived experiences with theoretical explanations. *Forensic Sciences*, 4(4), 647–668.

#### Week 3

- Taylor et al., Chapter 8
- Lozano-Blasco, R., Quilez-Robres, A., & Latorre-Coscolluela, C. (2023). Sex, age and cyber-victimization: A meta-analysis. *Computers in Human Behavior*, 139, 107491.
- Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, 9(1), 35–49.

#### Week 4

- Bilton, *American Kingpin*
- Burton, J., Janjeva, A., Moseley, S., et al. (2025). *AI and Serious Online Crime*. Centre for Emerging Technology and Security (CETaS), Alan Turing Institute.
  - Executive Summary and Section 3 (Case Studies) only
- Brinck, J., Nodeland, B., & Belshaw, S. (2023). The “Yelp-ification” of the Dark Web. *Journal of Contemporary Criminal Justice*, 39(2), 185–200.

#### Week 5

- Taylor et al., Chapter 10
- Kosseff, J. (2020). Hacking cybersecurity law. *University of Illinois Law Review*, 811–858.
  - Introduction; Clear, Adaptive, Collaborative principles only
- Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in real-world policing and law enforcement. *The Police Journal*, 96(4), 573–592.

### Optional Enrichment Readings & Media

These readings and media are not required, but are recommended for students who want to go deeper.

- Holt, T. J. (2023). "Understanding the state of criminological scholarship on cybercrimes." Systematic review of how criminology has studied cybercrime (theories used, offense types, gaps). Great for term papers or students thinking about research topics.
- Bada, A., & Nurse, J. R. C. (2021). "Profiling the Cybercriminal: A Systematic Review of Research." Reviews 39 studies on profiling cyber-offenders (including hackers), profiling methods, and proposed frameworks; dense but excellent for students interested in offender profiling and law-enforcement perspectives
- National Academies of Sciences (2025). *Cybercrime Classification and Measurement* (selected chapters). Advanced reading on building a taxonomy of cyber-dependent and cyber-enabled crimes, and why no single data system can fully measure cybercrime
- Hutchings, A. "Hacking and fraud: Qualitative analysis of online offending and victimization." Interview-based study of hackers and online fraudsters; explores motives, target selection, and offenders' perceptions of victims—an empirical counterpart to *Ghost in the Wires*
- Reyns, B. W., Henson, B., & Fisher, B. S. (2016). "Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization." *Journal of Contemporary Criminal Justice*, 32(2), 148–168. Applies routine activity theory to cyberstalking, showing that traditional offline guardianship does not significantly reduce risk, while certain online "target hardening" behaviors and online guardianship are more relevant for preventing cyberstalking victimization
- Lacson, W., & Jones, B. (2016). "The 21st Century DarkNet Market: Lessons from the Fall of Silk Road." *International Journal of Cyber Criminology*, 10(1), 40–61. Analyzes discussions around the Silk Road takedown to show how dark-net markets adapt and reconfigure after law-enforcement interventions; useful for policy and displacement debates
- Casefile: "Case 76 – Silk Road" (Parts 1–3). Three-part true-crime podcast series that provides a detailed narrative of Ross Ulbricht and the Silk Road marketplace, including the role of libertarian ideology, Tor, Bitcoin, and law-enforcement investigation
- De Paoli, S., Hutchings, A., Johnstone, J., & Wolak, J. (2021). "A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists." Interview-based study with cybercrime specialists from multiple countries; ideal for students who want a deeper look at specialist-unit practice, digital evidence, training, and jurisdictional problems
- Ogu, E. C., Ogu, C., & Oluoha, O. U. (2020). "Global cybersecurity legislation? — factors, perspective and implications." Useful for students interested in why cyberlaw remains fragmented globally and how political and institutional differences shape cybersecurity legislation
- Weiss, M., & Biermann, F. (2023). "Cyberspace and the protection of critical national infrastructure." Comparative governance piece on how states protect critical infrastructure, useful if students want a policy-comparison angle rather than a U.S.-only lens