CptS 424: Cyber Law, Ethics, Rights, and Policies
Syllabus, Fall 2025
Last updated: January 16, 2026

Course Information

Credits: 3

Semester: Fall 2025

Meeting Times & Location: MWF 11:10—12:00, EME B0046

Learning Management System (LSM): Canvas will be used for the management of this course, including for posting of lecture materials, assignments, announcements, and messages. It will also be used for handling student submissions and instructor and Teaching Assistant feedback.

Instructor Information

Instructor 1: Sherri Conklin

Affiliation: Assistant Professor of Philosophy (School of PPPA)

Email: sherri DOT conklin AT wsu DOT edu

Instructor 2: Assefaw Gebremedhin

Affiliation: Associate Professor of Computer Science (School of EECS)

Email: assefaw DOT gebremedhin AT wsu DOT edu

Course Description

Professionals working in cyber operations must comply with laws, ethics, regulations, directives, and policies. This course explores such aspects from both technological and societal perspectives. The topics to be covered are grouped under six Modules:

- Module 1: Ethical Frameworks
- Module 2: Cyber Foundation
- Module 3: Cybersecurity and AI
- Module 4: Legal and Administrative Frameworks
- Module 5: Cyber Policies in a Global Context
- Module 6: Applied Issues in Cybersecurity

Rather than treating these Modules sequentially, however, lectures will be organized in cross-cutting fashion. Specific topics as well as coursework elements covered under each Module along with associated Readings are described later in the document.

Required Textbook:

None. Students are not expected to purchase any textbooks.

Lecture notes and other reading materials will be provided through the LMS.

Reference textbooks:

T. Schreider "Cybersecurity Law, Standards, and Regulations", 2nd Edition, 2020. Rothstein Publishing.

J. Kosseff, "Cybersecurity Law", 2nd Edition, 2020. Wiley Publishing.

M. Manjikian, "Cybersecurity Ethics: An Introduction", 2018. Routledge Publishing.

Student Learning Outcomes (SLO):

By the end of the course, students should be able to:

1) Given a cyber operations scenario, students should be able to:
   a) Provide an overview of the relevant technical cybersecurity issues.
   b) Provide an overview of any relevant legal frameworks, policies, or national priorities.
   c) Provide an overview of the relevant ethical frameworks and ethical concerns, including relevant stakeholders.

2) Provide a high-level explanation of national priorities relating to cybersecurity as well as the policies and ethical principles governing the permissible conduct of cyber operations and the use of tools, techniques, technology, and data.

3) Apply the notion of Grey Areas to describe situations where policy has not caught up with technology and ethical concerns emerging from its use.

4) Evaluate the relationship between ethical and legal concerns relating to cybersecurity.

5) Describe steps for carrying out ethical penetration testing, describe 'ethical hacking' principles and conditions, distinguish between ethical and unethical hacking, distinguish between nuisance hacking, activist hacking, criminal hacking, and acts of war.

SLO Assessment:

- SLO 1 is assessed by all graded items of the course.
- SLO 2 is assessed by Individual Reflection Assignment graded items of the course.
- SLO 3 is assessed by the Group Debate graded item of the course.
- SLO 4 is assessed by the Class Project graded item of the course.
- SLO 5 is assessed by the Class Activities, Group Debate, and Class Project graded items of the course.

Student Performance Evaluation and Grading

Student performance will be evaluated based on 1) Individual Reflection Assignments, 2) Group Debate Assignment, 3) Class Project, and 4) Class Activities. The Class Project has submissions at multiple stages. The weight for each element is provided below:

- Individual Reflection Assignments: 20%
- Group Debate: 20%
- Class Project Proposal: 10%
- Project/Group Presentation:10%
- Project Final Report: 30%
- Class Activities: 10%

All the coursework items and their due dates will be made available on the LMS.

Graded Coursework:

Individual Reflection Assignments will be varying in nature. There will be 2-3 such assignments. The assignments will be made available as the semester progresses. An assignment will typically be due a week after its release date. Due dates will be specified on the assignment prompt.

Group Debate is an activity modeled after "Moot court" in law schools. Several topics suitable for debate, including those involving Grey Area in policy considerations, will be provided. Students will be asked to form groups arguing for or against a particular case. A week after the debate topics is assigned,

each group will be required to submit a short (max 2 pages) Group Debate Reflection document. The actual debate will happen a week after that.

Class Project is a significant component of the course, accounting in total for 50% of the final grade. Students, working in teams of two or three, will complete a project on a topic they choose from a list of project ideas the instructors will provide or propose their own project idea instead.

Whether selected from a list of project ideas instructors provide or propose their own ideas, each team will submit a Class Project Proposal as the first step of the project. The proposal should contain a description of the project, milestones, and a rough timeline of a security-themed project. The document will be at most 2 pages.

A Class Project will culminate in a written Final Report, which is due in Finals Week. The report will be assessed both for quality of content and clarity of presentation.

The Final Report is preceded by a **Project Presentation** in class. A Project Presentation could primarily focus on summarizing research conducted related to the project or on findings of the project itself. Students will be evaluated for their presentation and communication skills in addition to their technical competence. Project Presentations are scheduled to take place in Weeks 14 and 15.

Class Activities will vary from week to week. These activities include but are not limited to small group discussion tables, guided writing sessions, social engineering activities, and thought experiments in either groups or individually. Engagement in class activities will be recorded via Participation Question administered on Canvas (via the Discussion feature of Canvas).

Grade scale:

A: 93—100	A-: 90—92.99	
B+: 87—89.99	B: 83—86.99	B-: 80—82.99
C+: 77—79.99	C: 70—76.99	C-: 67—69.99
D: 60—66.99	F: less than 60	

Detailed Topics, Course Outline, and Readings:

Module 1: Ethical & Legal Frameworks

Topics:

- Overview of Cybersecurity Basics – Terminology, Major Problems, Kinds of Attacks, Hacking
- Five Cybersecurity Pillars
- Moral Foundations Theory (moralfoundations.org)
- Five Principles for AI in Society (Floridi & Cowls 2022)
- Normative Ethical Theories: Deontology and Consequentialism (esp. Kohno, Acar, & Loh 2023)
- Cybersecurity Law (esp. Chap 1 from Reference Textbook Schreider 2020)
- ACM Code of Ethics
    - https://www.acm.org/code-of-ethics
- NIST Cybersecurity Frameworks
    - https://www.nist.gov/cyberframework
- How to conduct a Stakeholder Analysis

IEEE Well-Being Metrics

Other Useful Ethics Concepts:

- Dirty Hands
    - https://ethics.org.au/ethics-explainer-dirty-hands/
- Moral Hazards

    - https://ethics.org.au/ethics-explainer-moral-hazards/
- The Original Position
    - https://ethics.org.au/thought-experiment-the-original-position/

Readings:

- Kohno, Tadayoshi, Yasemin Acar, and Wulf Loh. "Ethical frameworks and computer security trolley problems: Foundations for conversations." In *32nd USENIX Security Symposium (USENIX Security 23)*, pp. 5145-5162. 2023.Chapter 3 of Manjikian (2018) "Cybersecurity Ethics" (Selected Sections)
- Floridi, L., & Cowls, J. (2022). A unified framework of five principles for AI in society. *Machine learning and the city: Applications in architecture and urban design*, 535-545.
-

Optional Ethics Readings - Frameworks:

- Sri Ramulu, Harshini, Helen Schmitt, Bogdan Rerich, Rachel Gonzalez Rodriguez, Tadayoshi Kohno, and Yasemin Acar. "Ethics in Computer Security Research: A Data-Driven Assessment of the Past, the Present, and the Possible Future." In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3162-3176. 2025.
- Reidsma, Dennis, Jeroen van der Ham, and Andrea Continella. "Operationalizing cybersecurity research ethics review: from principles and guidelines to practice." In *2nd International Workshop on Ethics in Computer Security, EthiCS 2023*. Internet Society, 2023.
- Kenneally, Erin, and David Dittrich. "The menlo report: Ethical principles guiding information and communication technology research." *Available at SSRN 2445102* (2012).

Module 2: Cyber Priorities and Policy in a Global Context

Topics:

- Reading and Writing Cases Studies
    - https://www.scu.edu/ethics/focus-areas/technology-ethics/a-template-for-technology-ethics-case-studies/
- U. S. Priorities & Policy
    - **Case Study**: Election Integrity
    - "Cybersecurity in Elections-US Case Study" from Van der Staak, S., & Wolf, P. (2019). *Cybersecurity in elections: Models of interagency collaboration*. International Institute for Democracy and Electoral Assistance (International IDEA).
    - **Assignment:** Reflection Paper 1
- International Priorities & Policy
    - **Case Study**: NotPetya Cyber Attack
    - https://www.sipa.columbia.edu/sipa-education/picker-center-executive-education/case-collection/notpetya-cyber-attack
    - **Assignment:** Reflection Paper 2
- Title 18
- The Internet as a Human RightUN General Assembly on Cybercrimes
- EU Cybersecurity Policies

Readings:

- CISA Best Practices for Securing Election Systems:
    - https://www.cisa.gov/best-practices-securing-election-systems
- "The Ethics of Voting" in Brennan, J. (2012). The ethics of voting. Princeton University Press.

- https://www.scu.edu/government-ethics/resources/ethical-issues-in-voting-rights-during-the-2022-us-general-elections/
- https://www.brennancenter.org/our-work/research-reports/trump-administrations-campaign-undermine-next-election
- Statements on National Priorities: Whitehouse Statements
    - https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/
    - https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2/
    - https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-president-donald-j-trump-reprioritizes-cybersecurity-efforts-to-protect-america/
    - https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity
- UN Cybercrime Convention -
    - https://news.un.org/en/story/2024/12/1158521
    - https://news.un.org/en/story/2024/12/1158526
    - https://www.unodc.org/unodc/frontpage/2024/December/five-reasons-why-the-new-cybercrime-convention-matters.html
- EU Cybersecurity Policies:
    - https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
- Relevant Articles from Title 18
    - https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285#1-0
    - https://www.congress.gov/crs-product/LSB10801
    - http://congress.gov/bill/110th-congress/house-bill/6060
    - https://www.justice.gov/jm/jm-9-48000-computer-fraud
    - https://www.justice.gov/jm/9-51000
    - https://www.justice.gov/jm/jm-9-50000-chip-guidance
    - https://www.justice.gov/jm/jm-9-59000-economic-espionage
- Çifci H, Ergüner E. Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends, and comparisons. *Data & Policy*. 2025;7:e7. doi:10.1017/dap.2024.99
- Chapter 7 from Schreider (2020) "Cybersecurity Law, Standards, and Regulations"
- Chapter 10 from Kosseff (2020 "Cybersecurity Law"

Module 3: Special Problems with and Benefits of the Use of AI & Data

Topics:

- AI as an Adversary
- AI for Defense
- Securing AI Systems
- Privacy and Bias
    - https://www.ibm.com/think/insights/ai-privacy
    - https://www.scu.edu/ethics/healthcare-ethics-blog/opening-the-black-box-how-artificial-intelligence-increases-race-based-disparities-in-medicine/
- **Case Studies** for Debate Assigned
    - **Assignment:** Debate
    - **Assignment:** Reflection Paper 3

Readings:

- Chapter 4 from Manjikian (2018) "Cybersecurity Ethics"

- Nektaria Kaloudi and Jingyue Li. 2020. The AI-Based Cyber Threat Landscape: A Survey. ACM Comput. Surv. 53, 1, Article 20 (February 2020), 34 pages.
- AI Powered Cyber Attacks:
- Leonelli, S. (2016). Locating ethics in data science: responsibility and accountability in global and distributed knowledge production systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *374*(2083), 20160122.
- *Rabonato, R. T., & Berton, L. (2025). A systematic review of fairness in machine learning. AI and Ethics, 5(3), 1943-1954.*
- *Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. ACM computing surveys (CSUR), 54(6), 1-35.*
- *Bruschi, D., Diomede, N. A framework for assessing AI ethics with applications to cybersecurity. AI Ethics **3**, 65–72 (2023). https://doi.org/10.1007/s43681-022-00162-8*

Module 4: Applied Issues in Cybersecurity

Introduce Group Projects – Assignments are listed below.

- Project Proposal
- Group Presentations
    - 1-2 graded group presentations on selected research articles per remaining days
- Final Group Project Report

Critical Infrastructure

- Cybersecurity and Infrastructure Agency (CISA)
    - https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
    - https://www.cisa.gov/resources-tools/resources/cybersecurity-best-practices-smart-cities
    -
- Ethical Infrastructure
    - https://ethics.org.au/ethics-explainer-ethical-infrastructure/
        - Cyber-Physical Power System Security
        - Securing WA State Energy Critical Infrastructure
        -

Military Cybersecurity

- Just War Theory
    - https://ethics.org.au/ethics-explainer-just-war/
- Clandestine Operations
    - https://www.congress.gov/crs-product/R45175
- Drone Warfare
    - https://ethics.org.au/eye-in-the-sky-and-drone-warfare/
- Hacktivism
    - https://ethics.org.au/ukraine-hacktivism/

Environmental Justice and Security

- https://ethics.org.au/were-in-this-together-the-ethics-of-cooperation-in-climate-action-and-rural-industry/

Healthcare Security

Web and Systems Security

- Deepfakes
    - https://ethics.org.au/thats-not-me-how-deepfakes-threaten-our-autonomy/
- Intellectual Property
    - https://ethics.org.au/ai-is-not-the-real-enemy-of-artists/

Policies

Conduct

Students are expected to maintain a professional and respectful classroom environment. This includes:

- Silencing personal electronics (non-disruptive devices may be used during class)
- Arriving on time and remaining throughout class.

Use of Generative AI Tools and Technologies

The use of generative AI tools and technologies, such as ChatGPT, to create content is permitted, but it must be fully disclosed as follows:

- If the tool is used to generate **text**, at the beginning of the submitted document, include a statement that says, "Generative AI was utilized to generate a draft of this text", and then indicate in what way you edited or changed the draft to produce the submitted text.
- If the tool is used to generate **code**, the generated code should first be saved in some way (e.g., in a separate file or committed to a repository) before being adapted with the following statement in the comments of the code: "Generative AI was utilized to generate this code" followed by a description of the functionality that the autogenerated code is fulfilling.
- Next, the code can be adapted and saved again (or committed)—the comments of the code should be updated to provide a summary of the adaptation.

If you find yourself in a situation that is not listed above and are worried about whether it might be considered cheating or if you are uncertain about the need to disclose the use of a particular tool, err on the side of caution and email the instructors (via Canvas). We will give you a definitive answer.

Correspondence

All class related correspondence with the instructors will be made via Canvas.

Attendance

Regular attendance is expected. While students may miss class for urgent reasons, excessive absences that are not cleared with the instructors will factor into the Class Activities portion of the semester grade.

Missing or Late Work

Submissions will be handled via Canvas. Students are expected to submit assignments by the specified due date and time. Assignments turned in up to 48 hours late will be accepted with a 10% grade penalty per 24 hours late. Except by prior arrangement, missing or work late by more than 48 hours will be counted as zero. Extensions for assigned work will be provided in special circumstances if the reason has been approved by the instructor prior to the due date.

Academic Integrity

Academic integrity is the cornerstone of higher education. You are responsible for reading WSU's Academic Integrity Policy, which is based on Washington State law. If you cheat in your work in this class you will:

- Fail the assignment or exam in which the cheating happened.
- Be reported to the Center for Community Standards.
- Have the right to appeal the instructors' decision.
- Not be able to drop the course or withdraw from the course until the appeals process is finished.

If you have any questions about what you can and cannot do in this course, ask the instructors. If you want to ask for a change in the instructors' decision about academic integrity, use the form at the Center for Community Standards website. You must submit this request within 21 calendar days of the decision.

Other Policies in the University Syllabus

Students are responsible for reading and understanding all university-wide policies and resources pertaining to all courses (for instance: accommodations, care resources, policies on discrimination or harassment), which can be found in the university syllabus website:

https://syllabus.wsu.edu/university-syllabus/.

Academic Dates and Deadlines

Students are encouraged to refer to the academic calendar often to be aware of critical deadlines throughout the semester. The academic calendar can be found at http://registrar.wsu.edu/academic-calendar.

Changes

This syllabus is subject to change. Updates will be posted on the course website.