PPPE/PSCI 6315
Legal Aspects of Cyber Security and Cyber Security Ethics

Marcelo M. Leal

Fall 2025

E-mail: marcelo.leal@utdallas.edu
Office Hours: M 1:00 – 3:00 pm
Office: GR 3.526

Course website: UTD eLearning
Class Hours: W 7:00 – 9:45 pm
Classroom: GR 3.302

Teaching Assistant: Kayleigh Tompkins
E-mail: kayleigh.tompkins@utdallas.edu
Office Hours: Tu 1:00 – 3:00 pm
Office: GR 2.324

Course Description

Cyber security is a public good with ethical implications. The course explores how rapid change in technology interacts with the much slower pace of change in the law to better understand the role of government in regulating cyber security. We will explore the legal basis upon which governments may provide for cyber security as well as the ethical concerns raised by increasing government involvement in this area and privacy issues related to the collection of information. The course will also discuss the appropriate legal and compliance steps that need to be taken when responding to cyberattacks and reporting cyberattacks to law enforcement. Finally, the legal aspects of conducting cyber forensics as well as topics such as cyber espionage will also be discussed.

Learning Objectives

After participating in class, completing the assigned readings, and thinking about course materials, you should be able to achieve the following learning outcomes:

- *Define* key concepts related to cybersecurity law and ethics.
- *Identify* the legal basis for government action in cybersecurity.
- *Examine* cybersecurity legal obligations across various sectors.
- *Compare and contrast* distinct ethical perspectives and arguments.
- *Evaluate* the strengths and weaknesses of cybersecurity regulations.
- *Design* a policy to address cybersecurity legal and ethical challenges.

Course Materials

There is no textbook for this class, and all of the readings are free. You will need to read 2–3 readings (generally policy papers and book chapters) each week prior to our class meeting. All of these readings will be available through the UTD Library or through eLearning.

Office hours

Office hours are set times dedicated to all of you. This means that I will be in my office (GR 3.526) waiting for you to come by with whatever questions you have. This is the best and easiest way to find me and the best chance for discussing class material and concerns.

> **Note**
>
> If you cannot stop by my office hours due to a schedule conflict, you can request an appointment outside my office hours here.

Grading and Assessment

Your final grade will be based on the following assignments:

Assignment	Points
Attendance and Participation	20
Reading Response Quizzes	20
Sectoral Mapping	10
Cyber Crisis Simulation	20
Final Project	30
Total	*100*

Attendance and Participation

You are expected to attend each session prepared, having completed the weekly readings. Active participation in discussions, group work, and in-class exercises is required. Participation can take several forms, including answering instructor questions, asking clarifying questions on course material, and engaging productively with peers. Your attendance and participation grade is evaluated in two stages: 10 points for the first half of the semester and 10 points for the second half.

Reading Response Quizzes

Over the course of the semester, you will have the chance to complete eight short, four-question, multiple-choice quizzes based on the week's readings. Quizzes are paper-based, closed-book, and timed. You are required to complete at least five quizzes. If you take more than five, only your five highest scores will count toward your grade. Taking extra quizzes also gives you an opportunity to earn up to 1 extra credit per quiz if you score perfectly. These quizzes are designed to be straightforward if you have done the reading but challenging if you have not, so keeping up with the readings will pay off!

> **Note**
>
> Quizzes will be held in weeks 3, 4, 6, and 9–13. A note will be posted on eLearning inside each week to indicate if a quiz will take place that week.

Sectoral Mapping

In week 5, you will present a mapping of cybersecurity regulations and standards relevant to a critical infrastructure sector of your choice. This is a group project, and you will also submit a hard copy of your mapping. Groups will form and select their sector during Week 2 in class, giving you time to research and collaborate.

Cyber Crisis Simulation

In week 8, you will participate in a hands-on simulation where teams respond to realistic cyber incidents. Grades are based on active participation and a reflection paper linking the simulation to key course concepts, regulations, and standards.

Final Project

You will write a policy brief on a topic of your interest related to the course. You may work in groups of up to three. By Week 4 (Sep 17), you will submit a one-page summary of your proposed brief. During the term, you will develop a full draft, with a preliminary draft due on Week 10 (Oct 29). The final paper is due on the last day of class (Dec 3), when you will also present your findings to the class and receive feedback from your peers.

Grade Scale

For your final letter grade, I round the final numerical grade up to the next highest whole number if it is greater than or equal to 0.5 (e.g., 86.5 becomes 87). Individual assignment grades are not rounded. Final letter grades are determined as follows:

Letter	Range
A	100 – 94
A-	93 – 90
B+	89 – 87
B	86 – 84
B-	83 – 80
C+	79 – 77
C	76 – 70
F	< 70

Course Policies

Communication

If I need to contact, I will use your UTD email address. Please check your inbox regularly throughout the semester and follow proper e-mail etiquette. I typically respond to emails within one-two business days and expect you will do the same.

Electronic devices

To maintain a focused learning environment, cell phones and other devices should only be used for approved class activities. Please silence and store your phone before class. Laptops and tablets may be used for note-taking only. Using a device for social media, messaging, or gaming during class will result in zero credit for attendance and participation for that day. Repeated misuse may lead to a temporary or permanent ban on electronic devices in class.

Grade disputes

If you have questions about your assignment grade, please wait at least 24 hours before contacting your TA so you have time to review the feedback carefully. To request a review, email your TA with your specific questions and a clear explanation of why you believe a change may be appropriate. Your TA will review your request and, if needed, meet with you to discuss it. If the issue is not resolved, you may ask the instructor to review it using the same process.

> **Note**
>
> After any review, your grade may go up, go down, or remain the same.

Late work

Late assignments will lose 10 percentage points per day and generally will not be accepted after five days, unless there is a family, personal, or medical emergency. This policy is meant to help you stay on track, not to punish you, and I am happy to be flexible when unexpected challenges arise. If you anticipate difficulty meeting a deadline, please reach out to your TA or me in advance, or let us know afterwards if something unforeseen comes up so we can work on a solution together.

Extra credit

Extra credit is not offered on an individual basis. Over the course of the semester, I may provide opportunities for all students to earn extra credit, to ensure fairness. Please do not request additional assignments for extra credit outside of these opportunities.

Excused absences

Excused absences are limited to observed religious holidays (per UTD policy), military service, official UTD events (e.g., athletics, debate, Moot Court), COVID-related exposure, or serious illness, as long as you notify your TA or me in advance. Documentation may be requested if needed. Absences for work, vacations, doctor's appointments, family events, or other personal matters are not considered excused, and you do not need to inform us about these.

> **Note**
>
> Missing a class or two will not hurt your grade, as long as you stay on top of deadlines and are present for in-class assignments.

Class recordings

The instructor may record class meetings, and these recordings will be made available to all registered students to support learning. Any other use of recordings requires the consent of any identifiable students, unless otherwise permitted by law. Students must follow University policies, protect passwords for accessing recordings, and may not record any part of the course unless approved by the AccessAbility Resource Center. Recordings may not be published, reproduced, shared with anyone outside the class, or uploaded to other online platforms, except to implement an approved accommodation. Failure to comply with these requirements is considered a violation of the Student Code of Conduct.

Academic honesty

Violation of UTD's Policy on Academic Honesty will result in an F in the course and may lead to further disciplinary action. All violations will be formally reported to the Dean of Students.

> **i** A Note on AI Use
>
> You may use AI tools like ChatGPT or Microsoft Copilot to help brainstorm, outline, or generate ideas. However, assignments that are fully generated by AI and submitted as your own work count as plagiarism and will receive a zero. If you use AI, make sure to adapt any suggestions to your own thinking, writing, and style so that the final submission reflects your own work.

UTD Policies and Resources

Accommodations for Students with Disabilities

The University of Texas at Dallas is committed to providing reasonable accommodations for all persons with disabilities. The syllabus is available in alternate formats upon request. If you are seeking classroom accommodations under the Americans with Disabilities Act (2008), you are required to register with the AccessAbility Resource Center (ARC), located in the Administration Building, Suite 2.224. They can be reached by email, calling 972-883-2098, or at their website. To receive academic accommodations for this class, please register and request services by completing the Request for Services form with the proper documentation and meeting with the Director of ARC at the beginning of the semester.

Academic Support Resources

Please visit the Academic Support Resources page to view the University's academic support resources for all students.

UT Dallas Syllabus Policies and Procedures

Please visit the Syllabus Policies page to view the University's policies and procedures segment of the course syllabus.

Schedule and Readings

All readings are available on eLearning. It is important to complete the assigned readings before class, as this will help you participate fully in discussions. Students are encouraged to engage critically and share their perspectives openly. Bringing notes to class can be helpful, so we can discuss the topics you find most interesting together.

Part I: Foundations

Week 1 (Aug 27) – Introduction

- Goldfoot, Josh A. 2023. *Cybersecurity as a Legal Problem*. Lawfare. https://s3.documentcloud.org/documents/24767726/cybersecurity-as-a-legal-problem-goldfoot.pdf

Week 2 (Sep 3) – Market Dynamics and Government Response

- Herr, Trey, Will Loomis, Emma Schroeder, Stewart Scott, Simon Handler, and Tianjiu Zuo. 2021. *Broken Trust: Lessons from Sunburst*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf
- Woods, Daniel W., and Tyler Moore. 2020. "Does Insurance Have a Future in Governing Cybersecurity?" *IEEE Security & Privacy* 18 (1): 21–27.

Week 3 (Sep 10) – U.S. Approaches to Cybersecurity Regulation

- Bradford, Anu. 2023. "The American Market- Driven Regulatory Model." In *Digital Empires The Global Battle to Regulate Technology*. Oxford University Press.
- White House. 2023. *National Cybersecurity Strategy*. The White House. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
- Dempsey, Jim. 2025. "The Cybersecurity Patchwork Quilt Remains Incomplete." *Lawfare*, July 16 2025. https://www.lawfaremedia.org/article/the-cybersecurity-patchwork-quilt-remains-incomplete

Week 4 (Sep 17) – U.S. Law, Standards, and Regulations I

- National Institute of Standards and Technology (NIST). 2024. *NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
- Choi, Bryan H. 2024. *NIST's Software Un-Standards*. Lawfare. https://www.lawfaremedia.org/article/nist's-software-un-standards.

Week 5 (Sep 24) – U.S. Law, Standards, and Regulations II

- Kane, Bridget R., Stephen Webber, Katherine H. Tucker, Sam Wallace, Joan Chang, Devin McCarthy, Dennis Murphy, Daniel Egel, and Tom Wingfield. 2024. *Threats to Critical Infrastructure: A Survey*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2300/RRA2397-2/RAND_RRA2397-2.pdf

Week 6 (Oct 1) – Compliance and Enforcement in Practice

- Sivan-Sevilla, Ido. 2023. "To Save Society from Digital Tech, Enable Scrutiny of How Policies Are Implemented." *Issues in Science and Technology* 39 (4): 28–30.
- Wright, Isabella, and Maia Hamin. 2024. *"Reasonable" Cybersecurity in Forty-Seven Cases: The Federal Trade Commission's Enforcement Actions Against Unfair and Deceptive Cyber Practices*. Atlantic Council. https://dfrlab.org/wp-content/uploads/sites/3/2024/06/47-cases-ftc-cyber-csi.pdf.

Week 7 (Oct 8) – Ethics and Professional Responsibility

- Manjikian, M. 2023. "What is Ethics?" In *Cybersecurity Ethics: An Introduction*, 2nd ed. Routeldge.

- Association for Computing Machinery. 2018. "ACM Code of Ethics and Professional Conduct." *ACM*. https://www.acm.org/code-of-ethics.

Week 8 (Oct 15) – Cyber Crisis Simulation

- Simulation Preparation Materials

Part 2: Controversies

Week 9 (Oct 22) – Privacy vs Security

- Twetman, Henrik, and Gundars Bergmanis-Korats. 2020. *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf
- Roberts, Jen, Trey Herr, Nitansha Bansal, Nancy Messieh, Emily Taylor, Jean Le Roux, and Svitlana Gelava. 2024. *Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights*. Atlantic Council. https://dfrlab.org/wp-content/uploads/sites/3/2024/09/Mythical-Beasts.pdf

Week 10 (Oct 29) – Platform Liability and Online Content

- Gorwa, Robert. 2024. "From Coast to Coast: State-Level Platform Regulation in the United States." In *The Politics of Platform Regulation: How Governments Shape Online Content Moderation*, 114–143. New York: Oxford University Press.
- Langvardt, Kyle. 2020. *Platform Speech Governance and the First Amendment: A User-Centered Approach*. Lawfare. https://s3.documentcloud.org/documents/20420835/langvardt-dsc-final-2.pdf

Week 11 (Nov 5) – Software Liability and Risk Management

- Lostri, Eugenia, and Justin Sherman. 2024. *"Security by Design" in Practice: Assessing Concepts, Definitions, and Approaches*. Lawfare. https://s3.documentcloud.org/documents/25049674/sbd_lostrisherman_final.pdf
- Dempsey, Jim. 2024. *Standards for Software Liability: Focus on the Product for Liability, Focus on the Process for Safe Harbor.* Lawfare. https://s3.documentcloud.org/documents/24371794/krp-editsdempsey_sbd-paper_final_jan23.pdf

Week 12 (Nov 12) – Private Actors and Active Cyber Defense

- Manjikian, M. 2023. "The Ethical Hacker." In *Cybersecurity Ethics: An Introduction*, 2nd ed. Routeldge.
- Stevens, Salome. 2020. "A Framework for Ethical Cyber-Defence for Companies." In *The Ethics of Cybersecurity*, edited by Markus Christen, Bert Gordijn, and Michele Loi. Springer International Publishing.

Week 13 (Nov 19) – Artificial Intelligence and Emerging Technologies

- Manjikian, M. 2023. "Ethics of Artificial Intelligence." In *Cybersecurity Ethics: An Introduction*, 2nd ed. Routeldge.
- Crichton, Kyle, Jessica Ji, Kyle Miller, John Bansemer, Zachary Arnold, David Batz, Minwoo Choi, Marisa Decillis, Patricia Eke, Daniel M. Gerstein, Alex Leblang, Monty McGee, Greg Rattray, Luke Richards, and Alana Scott. 2024. *Securing Critical Infrastructure in the Age of AI*. Center for Security and Emerging Technology. https://cset.georgetown.edu/wp-content/uploads/CSET-Securing-Critical-Infrastructure-in-the-Age-of-AI.pdf

Week 14 (Nov 26) – Fall Break

Week 15 (Dec 3) – Student Presentations and Future Directions

- No reading