The University of Texas at Austin
School of Law

389T Cybersecurity Law & Policy

Fall 2022 (#29255)

Welcome to Cybersecurity Law & Policy! This is the foundational course for the interdisciplinary cybersecurity program sponsored by UT's Strauss Center for International Security and Law, a campus-wide center that operates an array of education and research programs. The goal of the overall program is to pioneer an interdisciplinary approach to graduate education relating to cybersecurity, drawing on relevant aspects of law, computer science, policy, engineering, and business administration. In short, we promote cross-training. This class in particular draws students from the Law School, LBJ School of Public Policy, and graduate Business, Computer Science, and Information programs.

Class Meetings

Monday 9:05 - 10:20 am (TNH 3.**142**)
Wednesday 9:05 - 10:20 am (TNH 2.**138**) [Please note that we meet in two different rooms!]
Final exam on Friday, December 9.

Class Overview

The goal of this course (which is, basically, a hybrid law and public affairs course) is to provide you with foundational knowledge concerning the nature and function of the various government and private actors associated with cybersecurity in the United States, the policy challenges they face, and the legal environment for it all.

This is *not* a technical course, and you do not need a technical background to understand any of it. Indeed, my working assumption will be that you know nothing in particular about the technologies involved.

Learning Outcomes

As you will see in more detail below, the first half of the course focuses on what we might call the "defensive perspective" on cybersecurity. That is, we will proceed from the assumption that the overarching public-policy goal is to minimize unauthorized access to (or computer-based disruption of) computers. Then, in the second half of the course, we will take the offensive perspective. On this view, there are situations in which the overarching public-policy goal might actually be to *enable* (rather than prevent) some particular entity to engage in unauthorized access to (or computer-based disruption of) computers.

In both contexts, our general learning objectives are to understand:

1. The players: Identify the roles and responsibilities of various public and private actors with respect to defense.
2. The architecture: Understand the laws, policies, and incentive structures regulating or impacting those actors.
3. The pros and cons: Grasp the pros and cons of the status quo in relation to these structures and institutions.
4. The path forward: Develop ideas for potential reform of these structures and institutions.

More-specific learning objectives are listed for every single class meeting in the text of the assigned reading for each day. We will also try to spend the first few minutes of each class discussing cybersecurity issues in the news that day.

Assigned Materials

Dean Bobby Chesney authored a customized eCasebook for this course, as part of a multi-year grant project supported by the Hewlett Foundation calling for the creation of pioneering interdisciplinary course materials to be made available for free to others. Happily, that means that the book for this course won't cost you anything. Our homepage on Canvas provides you with the link you need to download the book. As you will see, the book contains a sequence of 25 assignments, with the majority addressing aspects of the "defensive perspective" and the final six addressing the "offensive perspective." Please note: the assignments frequently call for you to click on a link to access an external reading, and they also typically contain specific questions for you to consider about those readings. Our class discussions will emphasize those questions.

Grading and Assessment Methods

The final exam will be on Friday, December 9. Your grade will be based on the final exam (please note that this is standard law school practice). It will be designed to focus on the questions and objectives emphasized in the readings, with a heavy emphasis on the things we treat as important during our class discussions.

The final exam is a timed exam administered by the Student Affairs Office. The exam will contain multiple choice, short answer, and essay questions. The exam will be open book. The exam will be administered using Extegrity's Exam4 software in open laptop mode. Cell phones, smart watches, tablets, and other electronic devices may not be used during the exam for any reason. You will have 3 hours to take the exam.

I reserve the right to make adjustments to your final grade based on your course participation, meaning both timely attendance (real-time, on-time attendance is required) and being prepared for class (in the sense that, if called upon, it is clear that you have done the readings).

We frequently will use Poll Everywhere. Your answers will have no bearing on your grade so long as you participate; it's a formative, no-stakes exercise intended to help you understand the materials, stir discussion, and so forth. *Please note*: we have secured a site license and hence this will not cost you anything. You will need to ensure you have opened a Poll Everywhere account with your UT email address, using the specific link that Poll Everywhere is going to send to you once our Canvas page is active. That is how I will know you are participating in the process. Don't worry about having this set up for the first day of class, we'll discuss and then start using Poll Everywhere during the second class.

Attendance Policy

Regular and punctual attendance is required in all courses pursuant to the Law School's Attendance Policy. As discussed above, your in-person attendance (as measured by Poll Everywhere) and class participation can be a basis for modifying your final grade.

Course Requirements and Assignments

I will try to record most class meetings and make the recordings available to you. Class recordings are there for study and to help students who have legitimate-and-approved reasons for absence, *not as a substitute for real-time attendance*. The University's position on unauthorized disclosure of these recordings is strict: these are FERPA-protected materials, and unauthorized sharing could lead to Student Misconduct/Honor Code proceedings. I will generally *not* record class meetings when we have a guest speaker, most of whom will be current or former government officials, so they may speak candidly.

Our book covers 26 assignments, and we will move them in order. Please note: Every assignment begins with a clear list of learning objectives, and also contains a variety of questions/discussion-prompts embedded amidst the readings. Your task is to read the material carefully each time, pondering those objectives, questions, and prompts so that you can engage in serious discussion of them during the class meetings.

August 22	**1. Holiday Bear and SolarWinds: A Case Study**
August 24	**2. Introduction to Key Terms and Concepts**
August 29	**3. The Crime Model: Key Institutions and the CFAA**
August 31	**4. CFAA Case Studies**
September 5	*Labor Day, No Class*
September 7	**5. Other Criminal Statutes**
September 12	**6. Civil Liability Under the CFAA**
September 14	**7. What if the attacker is a foreign government? (I)**

September 19	**8. What if the attacker is a foreign government? (II)**
September 21	**9. What if the attacker is a foreign government? (III)**
September 26	**10. What if the attacker is a foreign government? (IV)**
September 28	**11. The Role of Regulators (I)**
October 3	**12. The Role of Regulators (II)**
October 5	**13. Private Lawsuits (I)**
October 10	**14. Private Lawsuits (II); Insurance and Contract Terms**
October 12	**15. Facilitating Better Defense Through Info-Sharing (I)**
October 17	**16. Facilitating Better Defense Through Info-Sharing (II)**
October 19	**17. How the Government Protects Itself (I)**
October 24	**18. How the Government Protects Itself (II)**
October 26	**19. Improving Cybersecurity for Critical Infrastructure**
October 31	**20. Federal Coordination and Significant Cyber Incidents**
November 2	**21. Lawful-But-Unauthorized Access: Private Sector Hacking?**
November 7	**22. Government Hacking: Law Enforcement**
November 9	**23. The Insecurity Industry**
November 14	**24. Government Hacking: Espionage**
November 16	*No new assignment; we will catch up and review*

====Fall break November 21-26====

November 28	**25. Government Hacking: Armed Conflict**
November 30	**26. Government Hacking: Grey-Zone Competition**
December 5	**Last day of class; catch up and review**

Student Workload

This course complies with the Law School's Credit Hour Policy and will require at least 42.5 hours of total student work per credit during the semester.

Please expect to spend a few hours preparing for each class meeting.

Classroom Safety and COVID-19

The University provides guidance and information to help us preserve our in person learning environment.

Accessibility Statement

The Law School is committed to creating an accessible and inclusive learning environment consistent with university policy and federal and state laws. If you are a student with a disability, or you think you may have a disability, and may need academic accommodations, please contact the Division of Diversity and Community Engagement, Disability and Access (D&A) for information and assistance. If you are already registered with D&A, please deliver

your Accommodation Letter to the Student Affairs Office as early as possible in the semester to arrange your approved accommodations. If you have accommodations for exams, arrangements must be made with the SAO at least a week before the exam.

Because the Law School operates primarily on an anonymous grading system where possible, academic accommodations are coordinated through the Student Affairs Office. Faculty members are included in the process only when needed to implement classroom accommodations.