CYBERSECURITY LAW, POLICY & INSTITUTIONS
UNIVERSITY OF FLORIDA LEVIN COLLEGE OF LAW
COMPRESSED SPRING SEMESTER SYLLABUS – LAW 6930– 1 CREDIT

CONTACT INFORMATION:
Lyn Brown
Phone: (202) 719-4114
Email: lbrown@wiley.law
Web: https://www.wiley.law/people-LynBrown

MEETING TIME:

January 12th to January 15th (Mon, Tues, Wed, Thurs) 9:00 a.m. to 12:00 p.m.
January 16th (Fri) 9:00 a.m. to 11:00 a.m.

LOCATION: Insert Room

COURSE DESCRIPTION AND OBJECTIVES:

This course will provide an overview of core legal, regulatory, and policy issues associated with cybersecurity. The course will focus on recent case studies involving high-profile cyber-attacks, imposing criminal penalties or sanctions on malicious cyber threat actors, defending the private sector through information sharing, cyber incident regulatory reporting obligations, and offensive cyber operations by the government.

Students will gain an understanding of the government actors including, law enforcement, intelligence agencies, and the military as well as the increasing role of federal regulators in combatting malicious cyber intrusions. Students will also gain an understanding of national security impacts from the role of certain adversarial nation-states in state-sponsored cyber intrusions into U.S. critical infrastructure.

Topics will include: imposing costs on cyber malicious threat actors through the Computer Fraud and Abuse Act, sanctions; potential civil liability; lawful-but-unauthorized access operations; cybercrime as a service, cyber espionage, and military operations.

STUDENT LEARNING OUTCOMES:

At the end of this course, students should be able to:

- Identify the various institutions, policies and legal frameworks involved in cybersecurity;
- Discuss the role of regulators in enhancing cyber incident preparedness and cyber incident reporting obligations;
- Understand potential criminal liability for unauthorized computer access under the Computer Fraud and Abuse Act, potential civil liability, and the use of sanctions against responsible nation-states;

- Discuss the role of U.S. Department and Agencies in combatting malicious cyber intrusions on the private sector through law enforcement investigations, intelligence activities, military operations, and international cooperation.

REQUIRED READING MATERIALS:

The textbook is an interdisciplinary "eCasebook" created by Professor Bobby Chesney, The University of Texas at Austin. He is providing access to this work under the terms of a Creative Commons Attribution 4.0 International (CC BY 4.0) license: https://creativecommons.org/licenses/by/4.0/.

Use should be accompanied by the requested citation: ROBERT M. CHESNEY, CHESNEY ON CYBERSECURITY LAW, POLICY, AND INSTITUTIONS (v.3.1) (2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547103 (this work is licensed under a Creative Commons Attribution 4.0 International license https://creativecommons.org/licenses/by/4.0/).

Please be sure to register for the Canvas course and have any required materials with you in print or easily accessible electronic form in class. You are responsible for checking your Canvas page and the e-mail connected to the page on a regular basis for any class announcements or adjustments.

COURSE EXPECTATIONS AND GRADING EVALUATION:

Your final grade will be based on your response to an issue-spotting essay question on one of several fact patterns you can choose from involving, for instance, a major data breach involving overseas criminal actors, an adversarial nation-state, or an insider threat.

- You may use material from the e-Casebook utilized for this course or other material available in Canvass. You may also use public source legal or policy research in addition to what is available in this e-Casebook.
- Your work should be your own and you should not consult with other people or use artificial intelligence when preparing your essay question responses.

Students will be evaluated based upon their ability to analyze legal issues, voluntary and mandatory reporting laws and regulations, and potential civil or criminal liability arising out of the incident. The essay should demonstrate your understanding of key cybersecurity stakeholders, important client considerations in incident response, relevant cyber incident reporting obligations, and the difference between relevant government departments and agencies in cyber incidents.

CLASS ATTENDANCE AND MAKEUP POLICY:

Attendance in class is required by both the ABA and the Law School. Attendance will be taken at each class meeting.

This is a compressed course and attendance is mandatory. Absences may negatively impact your grade. University attendance policy may be found at:
https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx

Students are responsible for ensuring that they are not recorded as absent if they come in late. A student who fails to meet the attendance requirement will be dropped from the course. The law school's policy on attendance can be found here.

UF LEVIN COLLEGE OF LAW STANDARD SYLLABUS POLICIES:

Other information about UF Levin College of Law policies can be found at this link.

UF ACADEMIC POLICIES AND RESOURCES:

Other information about UF academic policies and resources can be found at this link.

ABA OUT-OF-CLASS HOURS REQUIREMENTS: ABA Standard 310 requires that students devote 120 minutes to out-of-class preparation for every "classroom hour" of in-class instruction. Each daily class, except for the last class, is approximately 3 hours in length, requiring at least **6 hours of preparation** outside of class including [reading the assigned materials, writing critical analyses, and developing your final paper.

COURSE SCHEDULE OF TOPICS AND ASSIGNMENTS

This syllabus is offered as a guide to the direction of the course. Our pace will depend in part on the level of interest and the level of difficulty of each section and is subject to change.

Class Session: Date	Topic	Reading Assignments
1: 01/12/26 (Mon)	Defensive Perspective • Introduction • Case Studies (Solar Winds) • Key Terms and Concepts • Imposing Costs on Attackers • CFAA • Foreign Government Attackers	Pages 3-65
2: 01/13/26 (Tues)	• Encouraging Potential Victims to Defend Better • Role of Regulators • Private Lawsuits and Insurance • Information Sharing	Pages 66-133
3: 01/14/26 (Wed)	• CISA 2015 • How Government Protects Itself • Critical Infrastructure Protection • Organizing to Mitigate Harm • Federal Coordination and Significant Cyber Incidents	Pages 133-199
4: 01/15/26 (Thurs)	Offensive Perspective • Private Sector Hacking • Government Hacking	Pages 199-262

5: 01/16/26 (Fri)	• Case studies (Stuxnet, Olympic Games, Sandworm) • Ransomware crisis Cyber Incident Tabletop Exercise Discussion of Essay Papers	Pages 262-274