Class meets for two hours on Tuesdays at 5:45 p.m.

Overview and Student Learning Outcomes. The course will explore why securing the Nation’s computer systems, which has been a goal of multiple successive administrations and has broad bipartisan and public support, has proven to be so difficult to achieve. The topics presented will include the roles and responsibilities of U.S. government agencies and the private sector, information sharing, cyber incident response, the application of international law to nation state activity in cyberspace, data privacy, and internet governance. Upon completion of the course, students will be expected to have a general understanding of the legal and policy framework for cybersecurity and to be able to apply the principles taught in class to novel fact patterns.

Office Hours and Availability. I do not have an office at GULC but am available for telephone conferences or meetings after class. To schedule a telephone conference, please use my Georgetown email address.

Class Organization. Class participation is required and will be taken into account in the final grade. Laptops will be allowed in the classroom, but use of the Internet for any activity other than accessing course materials is not allowed. No audio or visual recording devices are permitted in the classroom. Classes will not be taped.

Reading Assignments. The assigned textbook for this class is Cybersecurity and Cyberwar: What Everyone Needs to Know by P.W. Singer and Allan Friedman. It is available on Amazon in new and used versions. I will supplement this textbook with academic and general media articles, judicial decisions, statutes, regulations, and executive branch documents. Assignments denoted in the syllabus as “reading for class” should be completed prior to class to facilitate discussion. I have endeavored to keep this list short, and suggest that if time permits students also complete some or all of the background reading prior to class. (Note: some of the background readings are lengthy government documents that may be skimmed.) Additional reading on topical issues may be added to Canvas after the start of the semester. Students are responsible for checking Canvas before class each week.


Tabletop Exercise Preparation. There will be a short (1-2 pages) credit/no credit writing assignment to assist students in preparing for the exercise that we will be conducting in class 7. The assignment will be due before the start of that class and will constitute students’ opportunity for midterm feedback. To receive credit for its completion, students must turn it in on time. The assignment will not be graded, but at my discretion or upon a student’s request I will provide oral or written feedback.

Class Presentation. Students will be asked to select a partner and rank their top three topic choices from the list provided. I will email assignments and presentation dates to the class. Students will then
have approximately two months to prepare a ten minute class presentation, with an additional five minute Q&A session. Active participation by class members in the audience is expected.

Exam and Final Grade. Students will have four hours to write a short take-home exam DURING THE FIRST WEEK OF THE EXAM PERIOD. The exam will consist of two essay questions and will cover concepts from class and the readings. The exam will be graded anonymously and on the recommended curve, and will be the primary determinant of the final grade. However, class participation, including in the tabletop exercise, and performance on the presentation assignment may result in a difference of up to one letter grade from that received on the exam.

Course Syllabus and Reading Assignments.

1. **January 17, 2017: Cyber Insecurity**
   - Reading for class:
   - Background reading:
     - What is the Internet: A Four Layer Model, * [0:00 to 14:35], available at https://www.youtube.com/watch?v=7k9QuXzw2Y&list=PLcRQyo3dz9rSepr5OLkxWX9y6neuq&index=2
     - A Day in the Life of a Packet, *available at* https://www.youtube.com/watch?v=d0TJ8szp4AE&list=PLcRQyo3dz9rSepr5OLkxWX9y6neuq&index=7
   - Key points:
     - a. Why was the Internet created and what purposes was it intended to serve?
     - b. How did this vision of the Internet influence its subsequent development and use?
     - c. What are the cyber threats that pose the greatest risk to information systems?
     - d. Which agencies in the federal government are tasked with responding to cyber incidents?

2. **January 24, 2017: Cyber Threats: Motives and M.O.’s**
   - Key points:
     - a. What are some common attack methods?
     - b. Why is it difficult to deter offensive use of the Internet?
     - c. How do threat actors frustrate attribution?

   - Key points:
     - a. How do we incentivize adoption of good cyber hygiene?
     - b. What are the goals of information sharing?
     - c. What legal and policy issues may impede information sharing?
     - d. Should the government have a role in mandating that critical infrastructure entities maintain a certain standard of network defense?
     - e. Should the government be expected to defend the private sector from network attacks perpetrated by nation states?
4. **February 7, 2017: Private Sector Responsibilities**

**Key points:**
- a. Who manages cyber risk in an organization?
- b. Who should bear the cost of a breach?

5. **February 14, 2017: Cybersecurity Incident Response**

**Key points:**
- a. Who in the government is in charge of cyber incident response? Who in the private sector is involved in incident response?
- b. How do relevant parties respond to cyber incidents? What factors determine how such response is carried out?
- c. Can a victim “hack back” to secure its stolen data?
- d. What tools of national power can the government use to respond to a cyber incident?

[NO CLASS FEBRUARY 21]

6. **February 28, 2017: Regulatory Responses to Data Breach Incidents**

**Key points:**
- a. What is FTC’s authority to regulate data security?
- b. Are regulatory agencies required to provide notice through rule-making?
- c. What is the relationship between/among criminal, regulatory, and civil responses to data breach incidents?

7. **March 7, 2017: Table Top Exercise**

_The Exercise Scenario will be provided to students on or before February 28. The preparatory reflection must be submitted by 5:30 p.m. on March 6._

[NO CLASS MARCH 14]

8. **March 21, 2017: Norms, Legal Rules and Principles that Shape Nation State Conduct in Cyberspace**

**Key points:**
- a. Do the laws of war provide an adequate framework for nation state activity on the Internet?
- b. What constitutes a ‘use of force’ in cyberspace?
- c. When does a cyber attack amount to an “armed attack?”
- d. How does uncertain attribution impact a state’s response to a cyber attack?
- e. What non-military action might the US Government take in response to a network attack by a nation state?
- f. What are stability measures?
9. **March 28, 2017: Cyberspace as a Military Domain**

**Key points:**

a. In what ways are military organizations making use of the Internet to conduct their activities?
b. Does recognizing that international law applies in cyberspace encourage or shape military activity on the Internet?

10. **April 4, 2017: Governing the Internet**

**Key points:**

a. How is the Internet governed?
b. Does the current model of governance need to be changed? If so, how?
c. What are the pros and cons of a cybersecurity treaty? What should such an instrument regulate?

11. **April 11, 2017: STUDENT PRESENTATIONS AND CONFERENCES**

12. **April 18, 2017: STUDENT PRESENTATIONS AND CONFERENCES**

13. **April 25, 2017: Course Wrap-Up** (review, Q&A, exam overview, class evaluations)