Information Security Strategies and Policies

PUBP/CS 6725, PUBP 4823
Wednesdays, 3:05 – 5:45, D.M. Smith Hall, Room 203

Professor:

Milton L Mueller (School of Public Policy)
Room 302 DM Smith
404-385-4281
milton@gatech.edu

Office hours:
Wednesdays 12 – 2:00
Or by appointment (request by email)

The security of cyberspace is one of the newest and most significant public policy challenges of the 21st century. As a policy domain, cybersecurity spans domestic and global perspectives and touches on national security and inter-state relations as well as the security of corporations, commercial transactions and end users. The course welcomes students from public administration, policy studies, communications and computer science. Students will be expected to understand some basic aspects of Internet technology and will learn some technical material regarding internet protocols, vulnerabilities, exploits and incident response techniques and methods, but the course is focused on the public policy and political economy aspects of cybersecurity and does not require advanced computer science expertise.

Learning Objectives:

Students will learn:

- Basic concepts regarding vulnerabilities, exploits, threat actors, cyber risk assessment
- How cybersecurity problems are related to the nature of the Internet ecosystem
- The responsibilities and roles of private sector platform and network operators, end users, national governments, Internet governance institutions, and technical standards organizations.
- The distinction between the national security and end user/organizational levels of cybersecurity. Understanding cyberspace as a domain, the definition of cyberwar, cyberweapons, and how concepts related to military conflict (e.g., deterrence) apply or are modified by cyber conflict
- To critically assess when law and public policy are appropriate responses to cybersecurity problems and when organization-level or market-based solutions are preferable.

Main textbook and readings

- Singer and Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford Univ. Press (2014)

Due to the dynamic nature of our subject matter, no single book exists that meets all our requirements. Thus, in addition to the textbook, readings will be assigned on specific topics. Graduate students have different and more challenging reading assignments. All additional readings will be available online through the course web site. Some reading assignments will be drawn from these books:

- National Research Council. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, DC: The National Academies Press, 2014. Free download here.
- Healey and Grindal, (eds.) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Washington, DC: Atlantic Council (2013).

Assignments

1. Go Phish (team assignment) 15%
2. CyberCIEGE simulations. 15%
3. Analysis of a corporate cybersecurity incident. 20%
4. Interview a practitioner in the cybersecurity field and present the results to the class 20%
5. Role play exercise + analytical paper. 20%
6. Attendance, class participation, readings 10%

(Students must come prepared to discuss the topics in class and show through their participation that they have done the readings.)

Date	Topic	Required readings
		1. Basics of Cybersecurity Policy
Aug. 24	Nature of cyberspace Security as private and public good	• All: Singer and Friedman, Part 1, pages 12 – 66. • Grad students: Economics of Cybersecurity, Asghari et al
Aug. 31	Vulnerabilities and Threats Categories of actors 'Cyber weapons' and exploit markets	• Singer and Friedman, Part 2 pages 67 – 119. • Grad students: Lillian Ablon, Martin C. Libicki, Andrea A. Golay, *Markets for cybercrime tools and stolen data, RAND Corporation* • Undergrads: NAS book, Chapters 3 and 4: http://www.nap.edu/openbook.php?record_id=18749&page=29 http://www.nap.edu/openbook.php?record_id=18749&page=53 Begin Assignment #1 & #2
Sept. 7	PKI and trust models Internet standards and governance institutions The DNS Changer incident	• Undergrads and grads: Trend Micro blog: "Digital Certificates: Who Can You Trust?" and Laurie & Doctorow: "Secure the Internet" • Grad students: Mueller, Schmidt and Kuerbis, Internet Security and Networked Governance in International Relations, (2013) • Optional: J Nye, The regime complex for Internet Governance.
Sept 12		Assignment #1 due
		2. Cybersecurity in the private sector
Sept. 14	Cyber Risk analysis	• Grads AND Undergrads: read Slayton, Measuring Risk
Sept. 21	Corporate policy, liability, and insurance Private production of cybersecurity	• Undergrads: Booklet from Zurich Insurance on Cyber Risk • Grads: Allison Miller, Defending Debit: A Historical Study of the Indirect Effects of the Durbin Amendment on Investment in Debit Card Security , WEIS 20
Sept. 28	Class visit to CyberSummit, Tech Square	• Reading to prepare for panel discussion (all): Segal, The Hacked World Order, Chapter 8: Realpolitik meets the Internet pages 206-222. Finish Assignment 2; Begin Assignment 3
		3. National Cybersecurity and International Relations

Oct. 5	US laws and policies affecting business cybersecurity NIST framework	• Overview of US laws handout • Harknett, Richard J. & Stever, James A. (2011). The New Policy World of Cybersecurity. *Public Administration Review*, May/June 2011, 455-460 • NIST Framework
Oct. 12	Cyberspace as domain for military and inter-state conflict	• Singer and Friedman, Part 2, pp. 120 – 165 • William Lynn, Defending a new domain, Foreign Affairs, September/October 2010. Assignment 3 due
Oct. 19	International crypto regulation and standards Export controls	• N. Saper. *International Cryptography Regulation and the Global Information Economy*. Northwestern Journal of Technology and Intellectual Property, 11:7, September 2013. (pdf available) Confirm Assignment 4 interview subjects by this date
Oct. 26	Sources and Nature of International Law; Law of Armed Conflict Cybersecurity in international politics and Internet governance	• UN Group of Government Experts 2015 report • Excerpts from *Tallinn Manual* • Cybercrime Convention summary • Mueller, Is there sovereignty in cyberspace?
4. Current issues and Problems in Cybersecurity		
Nov. 2	Cryptocurrencies: Hacks and security	• Primer on Bitcoin and financial regulation • Is Bitcoin legal? http://www.coindesk.com/information/is-bitcoin-legal/ • News accounts of the Bitfinex hack and the Ethereum DAO attack Assignment 4 due
Nov. 9	"Information sharing" laws and practices	• Singer and Friedman, Part III pages 166-246. Begin Assignment 5 (in class)
Nov. 16	US-China interactions on cybersecurity	• Ellen Nakashima, "Indictment of PLA hackers is part of broad U.S. strategy to curb Chinese cyberspying," Washington Post. May 14, 2014, • Mandiant, APT1: Exposing One of China's Cyber Espionage Units February 18, 2013 Continue Assignment 5 (in class)
Nov. 23	Current legislative and policy initiatives	• Singer and Friedman, Conclusions, p. 247 - end Continue Assignment 5 (in class)
Nov. 30	Continue Current legislative and policy initiatives. Class wrap up	Continue Assignment 5 (in class)
Dec 8		Write-ups of Assignment 5 due

Administrative

Course Policies

Attendance is required and graded as part of your participation and readings score. Absences are governed by Institute Approved Absences Policy at http://www.catalog.gatech.edu/rules/4b.php. Students with a good reason to miss a class, such as a job interview or illness should inform the instructor (in advance, when possible). Students are expected to do the assigned readings prior to the class. Students are permitted to use computers or tablets to take notes and to supplement the classroom discussions and lectures, but if it becomes evident that devices are being used to do unrelated work the professor reserves the right to ask that students turn them off and/or to dock their participation grade. Questions and comments during lectures are encouraged.

Academic integrity

Enrollment in this course indicates that you have read, acknowledge and agree to abide by the following:

- Policy on academic performance and incompletes - see Georgia Tech School of Public Policy Student Handbook.
- Georgia Tech Honor Code - including Addendum for Graduate Students. You are informed that student papers may be reviewed by plagiarism detection software.

Enrollment for the course indicates that you agree to attend all scheduled classes on time. With instructor's permission, one or two absences from class *may* be forgiven for good reason. Absences beyond this or repeated non-timeliness will likely result in a lower final grade. Access to an email account is a necessary requirement for effective course participation and interaction. All class emails will be sent to official Georgia Tech student email addresses, which are generally on prism. You are responsible for ensuring that you have access to this prism account. If you wish to use a private email address, it is your responsibility to redirect your prism mail to your preferred address. For more information, see E-mail guidance and also Georgia Tech Office of Information Technology.

Disability

The Georgia Institute of Technology is committed to providing reasonable accommodation for all students with disabilities. A ny student in this course who has a disability that may prevent them from fully meeting requirements should contact the Office of Disability Services (ODS) to discuss accommodations necessary to ensure full participation and facilitate their educational opportunities. Students who are seeking services must self-identify to the Office of Disability Services. Because some accommodations require significant pre-planning, we recommend that you begin the application process well in advance of the start of your first semester. Students are eligible to register with Disability Services at any time during their academic career at Georgia Tech. The ODS is at 353 Ferst Drive, Suite 221, Smithgall Student Services Building Atlanta, GA 30332-0285. dsinfo@gatech.edu.