Georgia Institute of Technology

Course Syllabus: Information Security Strategies and Policies
(PUBP/CS/MGT 6725)

Spring 2020 Section OCY	MS in Cybersecurity, School of Public Policy, IAC
Delivery: 100% Web-Based, Asynchronous	Canvas & edX for Content Delivery
Dates: January 6, – April 26, 2020	

Instructor Information

Professor Milton L Mueller	Office: DM Smith 302
Weekly Office Hours via Blue Jeans	

General Course Information

Description

This course introduces students to the policy and management aspects of cybersecurity. It is based on the idea that cybersecurity policy can be sorted into three "layers" representing different levels of social organization: the organizational level, the national level, and the transnational level. The course is divided into four modules. The first exposes students to basic concepts and definitions regarding policy, governance, and threats. The second deals with cybersecurity policy at the organizational level; the third deals with cybersecurity public policy at the national level; the fourth deals with cyber conflict, policy and diplomacy at the transnational level. This course situates cybersecurity in the overall Internet ecosystem. Student deliverables include small group projects as well as individually completed quizzes, discussions, and a final term paper. This is a required core course for all tracks in the Online MS in Cybersecurity.

Pre- and/or Co-Requisites

Students will be expected to have a basic understanding of computers and data networking and will learn some technical material regarding internet protocols, vulnerabilities, exploits and incident response, but the primary focus of the course is on the public policy, management and international relations aspects of cybersecurity. The course does not require programming skills, although they can be useful in some assignments. Students should be able to blend and integrate economic, technical and political modes of analysis. This course is best taken in conjunction with CS 6035 (Introduction to Information Security) for an introduction to the more technical aspects of cybersecurity.

Course Goals and Learning Outcomes

Upon successful completion of this course, you should be able to:

1. Recognize the different governance structures used to promote cybersecurity
2. Identify key cybersecurity policy frameworks and standards (e.g., NIST framework)
3. Write a cybersecurity policy for an organization
4. Analyze and assess the effects of existing and proposed cybersecurity laws and regulations
5. Propose actions or strategies that respond to the geopolitical dimension of cyber conflict
6. Recognize the intersections of cybersecurity governance with the governance, standards and operations of the Internet

Course Materials

Due to the dynamic nature of our subject matter, no single book exists that meets all course requirements. Each topical area has one or two required readings, which are listed in the course schedule

under the “Readings” column. All required readings are available as pdfs or via the Georgia Tech library. Doing the readings is very important and forms a significant portion of your grade. Quizzes assess your comprehension of the readings. Additional recommended or supplemental materials may be posted in the Canvas site in response to relevant ongoing events in cybersecurity.

Course Website and Other Classroom Management Tools

This class will use Canvas and edX to deliver course materials to online students. ALL course materials and activities will take place on these two platforms. In order to login to Canvas and edX…

Assignment Distribution and Grading Scale

Here is a list of the assignments and activities required in the course. Grading is not “curved;” students will be graded based on how well they have met the requirements of the assignment and accomplished specific learning objectives. With the exception of quizzes, most assignments will have a rubric associated with them so that students can see what criteria are used for grading and what weight is given to them.

Assignment	Release Date	Due Date	Weight
Go Phish (team assignment) Assignment #1	January 13	February 3	15%
Organizational policy (team) Assignment #2	February 3	February 29	25%
Legislative challenge (individual) Assignment #3	March 1	March 23	20%
Term paper (individual) Assignment #4	March 29	April 24	25%
Quizzes on lectures and readings (4 total)		End of each module	15%

Assignment Submission and Due Dates

All assignments will be due at the times listed above. These times are specified in UTC and are subject to minor changes so please check Canvas. To convert from UTC to your local time zone, use a Time Zone Converter. Each assignment will have a separate entry in Canvas that explains in more detail what is expected and what criteria are used to grade it. The weighting of the different assignments in determining your final grade is clear from the table above. Most assignments will be finalized by the student uploading a file in the relevant assignment place in Canvas. Do not send assignments directly to the professors or TA’s via email. All assignments must be submitted within Canvas, otherwise they cannot be graded properly and do not count towards the grade. If there are technical issues, please notify the help desk, as well as each professor immediately. Assignments should be graded with feedback within one week of when learners turn it in.

Quizzes

Quizzes become available for a week before they are due and also have a due date, but your answers are recorded and graded as you enter them. They remain available for three days past the due date – after that they become unavailable. If you fail to take a quiz before it disappears you lose the points. Quizzes are individual assignments – they are intended to provide an incentive to study the readings and

strengthen your recall and understanding of the reading and lecture material. We strongly discourage students from helping other individuals to answer the quiz questions.

Late assignments, Missed Quizzes, Re-scheduling

The major assignments are due before midnight on the due date. There is a very simple policy governing late assignments: for every day it is late, you lose two percentage points off what your score would have been. This policy will be applied regardless of the reason for your lateness; it doesn't matter whether you just forgot, your day job intervened, you had family problems, etc. The only special circumstances that will be accommodated are those that literally incapacitate the student for a significant period of time, such as injury and hospitalization, floods, hurricanes, power outages for several days, etc. Please do not waste the instructors' time asking for extensions for any other reasons.

Peer evaluations

Near the end of the semester students will fill out a peer evaluation form to assess how each group member contributed to the group projects. This allows group members to praise their peer for their contribution, to identify "free riders" who did not contribute, or to identify and explain problems with group coordination or behavior that affected the quality or timeliness of the project.

Grading Scale

Your final grade will be assigned as a letter grade according to the following scale:

A	90-100%
B	80-89%
C	70-79%
D	60-69%
F	0-59%

Technology Requirements and Skills

To participate in this class, you need the following computer hardware and software:

- Broadband Internet connection
- Laptop or desktop computer with a **minimum** of a 2 GHz processor and 2 GB of RAM
- Windows for PC computers or Mac iOS for Apple computers.
- Complete Microsoft Office Suite or comparable applications and ability to use Adobe PDF software (install, download, open and convert)
- Mozilla Firefox, Chrome and/or Safari browsers

Technology Help Guidelines

30-Minute Rule**:** When you encounter struggles with technology, give yourself 30 minutes to 'figure it out.' If you cannot, then post a message to the discussion board; your peers may have suggestions to assist you. You are also directed to contact the Helpdesk 24/7.

When posting or sending email requesting help with technology issues, whether to the Helpdesk, message board, or the professor use the following guidelines:

- Include a descriptive title for the subject field that includes 1) the name of course 2) the issue.
- List the steps or describe the circumstance that preceded the technical issue or error. Include the exact wording of the error message.
- When possible, include a screenshot(s) demonstrating the technical issue or error message.
- Also include what you have done to try to remedy the issue (rebooting, trying a different browser, etc.).

Communication Policy

Email personal concerns, including grading questions, to the professor privately using the Canvas platform's messaging. Do NOT submit posts of a personal nature to the discussion board.

Email will be checked at least twice per day Monday through Friday. On Saturday, email is checked once per day. During the week, I will respond to all emails within 24 hours; on weekends and holidays, allow up to 48 hours. If there are special circumstances that will delay my response, I will make an announcement to the class.

Student Forum/Q&A discussion boards will be checked twice per day Monday through Friday; Saturday, these discussion boards will be checked once per day.

Virtual office hours will be held using the Bluejeans. I will hold Virtual Office Hours weekly, and the TAs will arrange special office hours if needed for dedicated topics, such as a large, upcoming assignment. Special topic hours will be announced in advance.

Online Student Conduct and Netiquette

Communicating appropriately in the online classroom can be challenging. In order to minimize this challenge, it is important to remember several points of "internet etiquette" that will smooth communication for both students and instructors:

Read first, Write later. Read the ENTIRE set of posts/comments on a discussion board before posting your reply, in order to prevent repeating commentary or asking questions that have already been answered.

Avoid language that may come across as strong or offensive. Language can be easily misinterpreted in written electronic communication. Review email and discussion board posts *before* submitting. Humor and sarcasm may be easily misinterpreted by your reader(s). Try to be as matter-of-fact and professional as possible.

Follow the language rules of the Internet. Do not write using all capital letters, because it will appear as shouting. Also, the use of emoticons can be helpful when used to convey nonverbal feelings.

Consider the privacy of others. Ask permission prior to giving out a classmate's email address or other personally identifiable information.

Keep attachments small. Avoid gigantic files; if it is necessary to send pictures, minimize the size.

No inappropriate material. Do not forward virus warnings, chain letters, jokes, porn, etc. to classmates or instructors. The instructor reserves the right to remove posts that are not collegial in nature and/or do not meet the Online Student Conduct and Etiquette guidelines listed above.

University Use of Email

A university-assigned student e-mail account is the official university means of communication with all students at Georgia Institute of Technology. Students are responsible for all information sent to them via their university-assigned e-mail account. If a student chooses to forward information in their university e-mail account, he or she is responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

Plagiarism & Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members,

departments, schools and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied. For information on Georgia Tech's Academic Honor Code, please visit http://www.catalog.gatech.edu/policies/honor-code/ or http://www.catalog.gatech.edu/rules/18/.

For written papers and projects the course uses Turnitin to identify and quantify material copied from other sources. An unacceptably high amount of copying will result in penalties to the score and a request to re-do the paper; in the worst cases the project will simply be rejected as a failure. Any student suspected of cheating or plagiarizing on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services at (404)894-2563 or http://disabilityservices.gatech.edu/, as soon as possible, to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible in order to set up a time to discuss your learning needs.

Student-Faculty Expectations Agreement

At Georgia Tech we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and students. See the GT catalogue for an articulation of some basic expectation that you can have of me and that I have of you. In the end, respect for knowledge, hard work, and cordial interactions will help build the environment we seek. I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Subject to Change Statement

The syllabus and course schedule may be subject to change. Changes will be communicated via the Canvas announcement tool and/edX bulk email and or the class Piazza discussion forum. It is the responsibility of students to stay current.

See schedule next page

Georgia Institute of Technology

Course Syllabus: Information Security Strategies and Policies
(PUBP/CS/MGT 6725)

Course Schedule

Module 1: The Basics			
Week/Dates	**Topic**	**Deliverables**	**Readings**
Week 1 **Jan 6 - 13**	**Topic 1: Cyberspace and the societal "layers,"** Lessons 1 – 2	Engage with discussion question	Institutional Landscape of Cybersecurity, by Kuerbis and Badii (2017)
Week 2 **Jan 13 – 20**	**Topic 2: Cybersecurity governance,** Lessons 1 – 4	Go Phish assignment begins	Economics of Cybersecurity, by Asghari, van Eeten and Bauer (2016)
Week 3 **Jan 20 – 27**	**Topic 3: Concepts and Vocabulary,** Lessons 1 – 3	Quiz 1 on readings and lessons due (Jan 27)	The Diamond Model of Intrusion Analysis, by S. Caltagirone et al
Module 2: Cybersecurity in the Organization			
Week/Dates	**Topic**	**Deliverables**	**Readings**
Week 4 **Jan 27-Feb 2**	**Topic 4: Understanding the risks,** Lessons 1 – 3		Sasha Romanosky, "Examining the costs and causes of cyber incidents," Journal of Cybersecurity, 2(2), 2016, 121–135
Week 5 **Feb 3 – 10**	**Topic 5: Organizational security policies** Lessons 1 – 4	Phish Assignment 1 due Begin Assignment 2	Measuring Risk: Computer Security Metrics, Automation and Learning, by R. Slayton. (2015)
Week 6 **Feb 10 – 17**	**Topic 5: Organizational security policies,** Lessons 5 – 7		NIST Cybersecurity Framework, pp. 24 – 45 Link to NIST Cybersecurity Framework
Week 7 **Feb 17 – 24**	**Topic 6: Industry self-regulatory efforts,** Lessons 1 – 6	Quiz 2 on readings and lessons.	Berkowsky, J.A. and Hayajneh, T., Security issues with certificate authorities. (2018); T. Chung et al, A Longitudinal, End-to-End View of the DNSSEC Ecosystem (2017)
Module 3: Cybersecurity policy at the national level			
Week/Dates	**Topic**	**Deliverables**	**Readings**
Week 8 **Feb 24 – Mar 1**	Topic 7: US laws and policies, Lessons 1 – 6	Assignment 2 due (Mar 1)	Siboni and Sivan-Sevilla, Regulation in Cyberspace, Chapter 2, "Literature Review." Israeli Institute for National Security Studies 2019.
Week 9 **Mar 1 – 8**	Topic 8: Protecting government networks, Lessons 1 – 2	Begin Assignment 3	Read and study proposed bill for legislative challenge
Week 10 **Mar 8 – 15**	Discussion and debate of legislative assignment		Read and study proposed bill for legislative challenge
Week 11 **Mar 15 – 22**	Spring break		

Week 12 **Mar 22 – 29**	Topic 9: Critical infrastructure Lessons 1-4	Final votes due on Assignment 3 (Mar 23) Quiz 3 on readings and lectures due (Mar 29)	

Module 4: Cybersecurity and International Relations

Week/Dates	Topic	Deliverables	Readings
Week 13 **Mar 29 – Apr 5**	Topic 10: Cyberspace and inter-state conflict Topic 10, Lessons 1 – 5	Begin Final Term Paper (due April 24)	Buchanan, Chapter 1 in The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations (2017). US Cyber Command, "Achieve and Maintain Cyberspace Superiority" (2018)
Week 13 **Apr 5 – 12**	Topic 11: International Norms and Treaties Topic 11, Lessons 1 – 3		What the Cloud Act means for privacy pros, by Peter Swire and Jennifer Daskal, (2018)
Week 14 **Apr 12 – 19**	Topic 12: Global Internet Governance Topic 12, Lessons 1 – 5		Sovereignty in Cyberspace: Governance for a non-territorial domain (2019), by Milton Mueller
Week 15 **Apr 19 – 26**	Discussion and debate of cyber diplomacy	**Final Paper due April 24** Quiz 4 on readings and lectures due April 26	