Info Security Policies - PUBP-4725-6725-LM

PUBP/CS 4725/6725 Spring 2027	
Classroom: TBD Tue – Thu 9:30am – 10:45am	**Dates:** January 13 – April 24, 2026

Instructor Information

Professor Lennart Maschmeyer	Office: DM Smith 304
Office Hours by appointment	lennart.maschmeyer@gatech.edu

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 problems can be sorted into three different levels of social organization: the organizational level, the national level, and the transnational level. The course is divided into four modules. The first module exposes students to basic concepts and definitions regarding policy, governance, and threats. The second module deals with cybersecurity policy at the organizational level; the third module deals with cybersecurity public policy at the national level; the fourth module deals with cyber conflict, policy and diplomacy at the transnational level. 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 MS Cybersecurity.

Course Schedule

Module 1: The Basics

Week/Dates	Topic	Deliverables	Readings	Discussion Questions
Week 1 **Jan 14, 16**	**1.1 Cyberspace & the societal "layers." Governance structures**		"Institutional Landscape of Cybersecurity", by Kuerbis and Badii (2017)	Friday session
Week 2 **Jan 21, 23**	**1,2 CIA framework, Cryptography, Content**	Group Assignment 1 (phish) begins Jan 23	"Information as Power", by Mueller and Grindal (2022) "A World Without Trust" by Schneider (2022)	Wednesday session Friday session
Week 3 **Jan 28,30**	**1.3 Diamond Model**	Quiz 1 on readings and lessons (due Feb 3)	"The Diamond Model of Intrusion Analysis", Caltagirone et al (2013)	Wednesday session Friday session
Module 2: Cybersecurity in the Organization				
Week 4 **Feb 4, 6**	**2.1 Policy in the org layer; NIST CSF, infra domains** **2.2 Cyber Risk**	Phish Assignment 1 due (Feb 6)	NIST Cybersecurity FrameworkLinks to an external site. p 1-5, 15-23 Information Risk Insights Study, Cyentia Institute (2025)Links to an external site.;	Wednesday session Friday session

Week 5 **Feb 11, 13**	**2.2 Cyber risk** **2.3 PKI**		Slayton, "Measuring Risk" IEEE Annals of the History of Computing (2015) Woods, Bohme, et al "Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach AttorneysLinks to an external site." UseNix (2023)	Wednesday session
Week 6 **Feb 18, 20**	**2.3: PKI Case studies** **2.4: Compliance** **2.5: Industry level efforts**		IGP blog post on Compliance lawsuitLinks to an external site.	Wednesday session Friday session
Week 7 **Feb 25, 27**	**2.5: Industry level efforts** **3.1: Cybersecurity and public policy**	Group Assignment 2 due (Feb 27)		Wednesday session Friday session
Module 3: Cybersecurity policy at the national level				
Week 8 **March 4, 6**	**3.2: US legal framework**	Quiz 2 opens (March 2)	SIPRI, Cyber Risk Reduction in China, Russia, the US, and the European UnionLinks to an external site. (2024)	Wednesday session Friday session

Week 9 **March 11, 13**	**3.2: US laws and agencies**	Quiz 2 due (March 9)	What the Cloud Act means for privacy pros, by Peter Swire and Jennifer Daskal,Links to an external site. (2018)	Wednesday session
Week 10 **March 18**	**3.2 Encryption policy** **Discussion of legislative assignment**	Online Debate of proposed bill	Read proposed bills for legislative challenge CISA 2015 Senator Paul amendments	Wednesday session
Week 11 **March 25, 27**	***** No Class - Holiday *****			
Week 12 (Part one) **April 1**	**3.3: Critical infrastructure**	Quiz 3 on readings and lectures opens (March 30)	Juan Villareal, "Battery Energy Storage Systems from China" (2024)	Wednesday session
Module 4: Cybersecurity and International Relations				
Week 12 (Part Two) **April 3**	**4.1 Sovereignty & Anarchy; Cybersecurity and International Law**	Assignment 3 due (April 3)	Mueller, "Against Sovereignty in Cyberspace" (2020)	Discussion Questions

Week 13 **April 8, 10**	**4.2 Cyber Conflict and Strategy**	Begin Final Term Paper (due May 1) Quiz 3 due (April 10)	Maschmeyer (2023), "Cyber Operations, Subversion, and Reverse Structural Power"	Wednesday session Friday session
Week 14 **April 15, 17**	**4.3 Cybercrime** **4.4 Global Cybersecurity Governance**			
Week 15 **April 22, 24**	**4.4 The Future of Cybersecurity: AI and Quantum Computing**	Quiz 4 on readings and lectures (due April 24)	"Deception and Detection", Maschmeyer (2026)Links to an external site. Anthropic Mythos PreviewLinks to an external site.	Wednesday Questions
April 28		**Final Paper due**		

Pre- and/or Co-Requisites

Students should 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
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 deliver course materials to online students. ALL course materials and activities will take place on these two platforms.

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. Except 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**
#1 Go Phish (group)	23 Jan	6 Feb	15%
Quiz on Module 1	27 Jan	3 Feb	7%

#2 Organization Policy (group)	11 Feb	27 Feb	15%
Quiz on Module 2	2 March	9 March	7%
#3 Legislative challenge (individual)	16 March	3 April	15%
Quiz on Module 3	3 April	10 April	7%
#4 Final Paper	6 April	28 April	20%
Quiz on Module 4	20 April	24 April	7%
Attendance	-	-	7%

Assignments and Due Dates

All assignments will be due at the times listed above. 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. 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 and professor immediately.

Quizzes

Quizzes become available for a week before they are due and must be completed by the due date. Your answers are recorded and graded as you enter them. They remain available for two days past the due date; after that they become unavailable. Late quizzes are deducted 2% per day. If you fail to take a quiz before it disappears, you lose the points. Quizzes are individual assignments intended to provide an incentive to study the readings and strengthen your recall and understanding of the reading and lecture material. Students should not help other individuals 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. 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.

Peer evaluations
Two assignments (#1 and #2) are group assignments. All students in the group will receive the same grade. 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 peers 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%

Communication Policy
Email personal concerns, including grading questions, to the professor privately via email. Do NOT submit posts of a personal nature to the discussion board. Face to face meetings can be arranged by emailing the Professor or by meeting before or after class.

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 makean 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 expectations 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 in class or via Canvas and/or Ed Discuss. It is the responsibility of students to stay current.