Georgia Institute of Technology

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

Spring 2023 Section OCY, O01	MS in Cybersecurity, School of Public Policy, IAC
Delivery: 100% Web-Based, Asynchronous	Canvas for Content Delivery
Dates: 9 January– 30 April 2023	

Instructor Information

Dr. Andreas Kuehn	Office: Remote
Weekly Office Hours Zoom	See Canvas for scheduled times

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 on Canvas or Ed Discussion in response to relevant ongoing events in cybersecurity.

Course Website and Other Classroom Management Tools

This class will use Canvas to deliver course materials to online students. ALL course materials and activities will take place on this platform, with supplemental discussion occurring on Ed Discussion. If you are new to Canvas, you can find Georgia Tech's Canvas Resources for Students here.

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 (group assignment) Assignment #1	January 18	February 4	15%
Organizational Policy (group) Assignment #2	February 5	February 27	25%
Policy Challenge (individual) Assignment #3	February 28	March 7 & March 18	20%
Term Paper(individual) Assignment #4	March 19	April 19	25%
Quizzes on lectures and readings (4 total)	1 week before due date	End of each Module	15%

Assignment Submission and Due Dates

All assignments will be due at the times listed in Canvas. These times are specified in EST and are subject to minor changes so please check Canvas. To convert from EST 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. For group assignments, it is highly recommended to allow time to review your complete work together. 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 Canvas' assignment module. Do not send assignments directly to the instruction team via email. All assignments must be submitted within Canvas, otherwise, they will be considered as not submitted. If there are technical issues, please notify the help desk, as well as the TAs immediately.

TAs will grade and provide feedback within one to two weeks after the assignment's due date. Questions about TA comments and/or regrade requests via a private Ed Discussion post (please select category "regrade requests") are due within seven days (excluding weekends and official holidays) after the release of the graded assignment. Please be specific in your request. Late requests may not be considered. Regrade requests will lead to a review of the entire assignment and may result in a higher or lower grade.

Quizzes

Quizzes become available a week prior to the end of the module. Quizzes are open-book/open-notes and do not have a time limit. Answers to questions can be changed until the entire quiz is submitted at the end. Quizzes 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

Assignments and quizzes are due before midnight on the due date. There is a very simple policy governing late submissions: for all assignments and quizzes, a penalty of two percentage points off your score is applied for every day it is late. 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

During the semester students will fill out a peer evaluation(s) to assess how each group member contributed to the group projects and how the group functioned. 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. Peer evaluation that indicates insufficient contribution may lower a student's final grade.

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 Ed Discussion board; your peers may have suggestions to assist you. You are also directed to contact the Helpdesk 24/7.

When posting or sending an 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 the 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

For course-related communication to the professor/TAs, including grading questions, please create a private Ed Discussion post. For concerns of personal nature, please send an email to the instructor.

Posts/messages will be checked at least twice per day Monday through Friday. On Saturday, posts/messages will be checked once per day. The instruction team will respond to posts/messages within 24 hours; on weekends and holidays, allow up to 48 hours.

Virtual office hours will be held using Zoom. We hold virtual office hours twice per week for half an hour. Special topic office 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 assignments, the course uses Turnitin to identify and quantify material copied from other sources. Students should review their Turnitin scores, and, if necessary, make revisions prior to submitting the assignment. Unacceptably copying, missing quotation marks and/or failure to provide citations to others' work – as indicated by a high Turnitin score – will result in penalties to the grade. In such cases, the instruction team may request to re-do the paper and/or reject the assignment as failed in serious cases. A 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 the instructor 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 catalog 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 via Canvas announcements. It is the responsibility of students to stay current.

See schedule next page

Course Schedule

Module 1: The Basics (opens January 9)			
Week/Dates	**Topic**	**Deliverables**	**Readings**
January 9-February 4	Topic 1: Cyberspace and the societal "layers," Lessons 1 – 2	Engage with Discussion Question 1: "Cyberspace??" Go Phish Assignment 1 begins (January 18)	Institutional Landscape of Cybersecurity, by B. Kuerbis and Badii, F. (2017)
	Topic 2: Cybersecurity governance, Lessons 1 – 4		Economics of Cybersecurity, by H. Asghari, van Eeten, M. and Bauer, J. (2016)
	Topic 3: Concepts and Vocabulary, Lessons 1 – 4	Assignment 1 due (February 4) Quiz 1 on Readings and Lessons due	The Diamond Model of Intrusion Analysis, by S. Caltagirone et al (2016)
Module 2: Cybersecurity in the Organization			
Week/Dates	**Topic**	**Deliverables**	**Readings**
February 5-February 27	Topic 4: Understanding the risks, Lessons 1 – 4	Organizational Policy Assignment 2 begins (February 5)	Empirically Evaluating the Effect of Cybersecurity Precautions on Incidents in Israeli Enterprises by Gandal et al. (2022) Information Risk Insights Study by Cyentia Institute (2020)
	Topic 5: Organizational security policies, Lessons 1 – 4	Engage with Discussion Question 2: "Is Information Operations (IO) part of cybersecurity?"	Combating Ransomware by Ransomware Task Force (2021) The Ransomware Task Force: One Year On by Ransomware Task Force (2022), pp. 3 – 8
	Topic 5: Organizational security policies, Lessons 5 – 7		NIST Cybersecurity Framework, pp. 24 – 45 Updating the NIST Cybersecurity Framework – Journey To CSF 2.0

			CSF 2.0 Update Fact Sheet by NIST
	Topic 6: Industry self-regulatory efforts, Lessons 1 – 6	Assignment 2 due (February 27) Quiz 2 on Readings and Lessons due	A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents, by H. Hadan, N. Serrano and J. Camp (2021)

Module 3: Cybersecurity policy at the national level

Week/Dates	Topic	Deliverables	Readings
February 28-March 18	Topic 7: US laws and policies, Lessons 1 – 6	Policy Challenge Assignment 3 begins (February 28)	Survey of US Laws Read and research proposed policy/rules
	Topic 8: Protecting government networks, Lessons 1 – 2	Assignment 3 post initial statement due (March 7) Debate of the proposed policy/rules	Read Assignment 3 discussion board Regulation in Cyberspace, Chapter 2, "Literature Review.", by Siboni and Sivan-Sevilla, Israeli Institute for National Security Studies (2019) China's Cybersecurity Regime: Securing the Smart State by Creemers (2022)
	Topic 9: Critical infrastructure, Lessons 1-3	Assignment 3 discussion board closes (March 18) Quiz 3 on Readings and Lessons due	Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards, by A. Clark-Ginsberg and Slayton, R. (2019)

Module 4: Cybersecurity and International Relations

Week/Dates	Topic	Deliverables	Readings
March 19-April 23	Topic 10: Cyberspace and inter-state conflict, Lessons 1 – 5	Assignment 4 Term Paper begins (March 19) Engage with Discussion question 3: "Defend Forward?"	Chapter 1: Defend Forward and Persistent Engagement, by G. Corn and E. Goldman (2022) Comments by E. Noor at Defending Forward: U.S. Cyber Strategy and Its Implications for Cybersecurity in Asia (2021) (video) Facts and Findings: Outward Defense, by S. Soesanto (2021) Could Confrontation in Cyberspace Escalate the War

			in Ukraine? by The Soufan Center (22 Jun 2022)
	Topic 11: International Norms and Treaties, Lessons 1 – 3	Engage with Discussion question: 4 “Cyber-offense or cyber-defense?”	Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads by Ruhl et al. (2020) The United Nations’ cyberstability processes: surprising progress but much left to do, by C. Painter (2021) Letter from Mykhailo Fedorov to Göran Marby (28 Feb 2022) Letter from Göran Marby to Mykhailo Fedorov (2 Mar 2022) Is true multi-stakeholderism failing? FIRST fears so by FIRST (21 Jul 2022)
	Topic 12: Global Internet Governance, Lessons 1 – 5	Quiz 4 on Readings and Lessons due **Term Paper due (April 19)**	Sovereignty in Cyberspace: Governance for a non-territorial domain, by M. Mueller (2019) Internet Impact Brief: Mandated Browser Root Certificates in the European Union’s eIDAS Regulation on the Internet (2021)