Georgia Institute of Technology

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

Fall 2023	MS in Cybersecurity, School of Public Policy, IAC
Time & Location: M/W, 5:00-6:15 pm; Skiles 202	Canvas for Content Delivery
Dates: 21 August – 14 December 2023	

Instructor Information

Instructor: Dr. Nadiya Kostyuk **Email:** nkostyuk3@gatech.edu **Office Hours:** Mondays 3:30-5 pm, or by appointment **Office:** Rich Building 311	**Teaching Assistant:** Ms. Evgenia (Jen) Sidorova **Email:** esidorova3@gatech.edu **Office Hours:** Thursdays 2-3 pm, or by appointment **Location:** Via Zoom **Link:**https://gatech.zoom.us/j/98444529523?pwd=RXdNNHV2SGhIekZmcS9NYVl5MUVVdz09 **Meeting ID:** 984 4452 9523 **Passcode:** 248004 **Teaching Assistant:** Ms. Vedika Bang **Email:** vedikabang@gatech.edu **Office Hours:** Fridays 11am-12 pm, or by appointment **Location:** Via Zoom **Link:**https://gatech.zoom.us/j/98444529523?pwd=RXdNNHV2SGhIekZmcS9NYVl5MUVVdz09 **Meeting ID:** 984 4452 9523 **Passcode:** 248004

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 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. Students are expected to be familiar with academic research and writing practices, including the proper use of academic citations. This course is best taken in conjunction with CS 6035 (Introduction to Information Security) for an introduction to the more technical aspects of cybersecurity.

Georgia Institute of Technology

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

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 the Canvas in response to relevant ongoing events in cybersecurity.

Course Website and Other Classroom Management Tools

This class will use Canvas to deliver course materials. 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
Organizational Policy (group assignment) **Assignment #1**	September 11	October 1	25%
National Policy (individual assignment) **Assignment #2**	October 15	October 29	25%
Bilateral Cyber Agreement (group assignment) **Assignment #3**	November 6	December 10	30%
Quizzes on lectures and readings **(4 total)**	1 week before due date	End of each Module	10%
Class Attendance and Participation			10%

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. 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 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 the TA immediately. Assignments should be graded with feedback within one week of when learners turn it in.

The class TA 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, the same or a 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, until the assignment become unavailable. At that point 0 points will be received. 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, moved for private or professional reasons, 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. If special circumstances apply, a student has to contact the Office of Student Life, submit a request and provide evidence. OSL will then provide a recommendation to the instructor for possible course of action. Please note that for group assignments, options to accommodate extensions, etc. are very narrow due to the nature of the assignment.

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.

Class participation and attendance

Class participation and attendance will be 10% of your course grade. Half of this grade will be earned simply by attending class and making a good-faith effort to remain engaged. The other half of this grade will be earned by participating actively and thoughtfully in classroom discussion, answering discussion questions on Canvas, and posing questions to our guest speakers on Canvas. Each module will have a discussion question that we will ask you to briefly answer. Every week (generally each Wednesday) starting on 8/28, we will have a guest speaker who is an expert in the area that we are covering that week. I ask you to post questions to this speaker on Canvas the night before (e.g., by 5:00 pm on Tuesday). I will use these questions to moderate our discussion with the speaker on the next day. **Please note that you need to put questions to 10 guest lecturers to get the full credit.**

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%

Once the final grade is posted on or before the registrar's deadline and the semester is finished, grades cannot be changed.

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 an email requesting help with technology issues, whether to the Helpdesk, message board, or the professor/TA 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.).

Georgia Institute of Technology

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

Course Schedule

Module 1: The Basics (opens August 21)			
Week/Dates	**Topic**	**Deliverables**	**Readings**
Week 1 8/21; 8/23	Topic 1: Cyberspace and the societal "layers," Lessons 1 – 2		Institutional Landscape of Cybersecurity, by B. Kuerbis and Badii, F. (2017)
Week 2 8/28; 8/30	Topic 2: Cybersecurity governance, Lessons 1 – 4	Questions to the guest lecturer (due 8/29)	MONDAY Economics of Cybersecurity, by H. Asghari, van Eeten, M. and Bauer, J. (2016) **WEDNESDAY (Group 1 on-call)** Covenants Without the Sword: Market Incentives for Cybersecurity Investment, by V. Garg (2021). **Guest speaker:** Vaibhav Garg on 8/30 (via Zoom)
Week 3 9/4 (no class, Labor Day); 9/6	Topic 3: Concepts and Vocabulary, Lessons 1 – 4	Questions to the guest lecturer (due 9/5) Quiz 1 on Readings and Lessons (due 9/10)	**WEDNESDAY (Group 2 on-call)** The Diamond Model of Intrusion Analysis, by S. Caltagirone et al (2016) **Guest speaker:** Sergio Caltagirone on 9/6 (via Zoom)
Module 2: Cybersecurity in the Organization			
Week/Dates	**Topic**	**Deliverables**	**Readings**
Week 4 9/11; 9/13	Topic 4: Understanding the risks, Lessons 1 – 4	Organizational Policy Assignment 1 begins (9/11) Questions to the guest lecturer (due 9/12)	**MONDAY (Group 3 on-call)** Empirically Evaluating the Effect of Cybersecurity Precautions on Incidents in Israeli Enterprises by Gandal et al. (2022) **WEDNESDAY (Group 4 on-call)** Information Risk Insights Study by Cyentia Institute (2020) **Guest speaker:** Tyler Moore on 9/13 (via Zoom)
Week 5 9/18; 9/20	Topic 5: Organizational security policies, Lessons 1 – 4	Questions to the guest lecturer (due 9/19)	**MONDAY (Group 1 on-call)** Combating Ransomware by Ransomware Task Force (2021) **WEDNESDAY (Group 2 on-call)** The Ransomware Task Force: One Year On by Ransomware Task Force (2022), pp. 3 – 8 **Guest speaker:** Jenny Jun on 9/20 (via Zoom)

Week 6 9/25; 9/27	Topic 5: Organizational security policies, Lessons 5 – 7	Questions to the guest lecturer (due 9/26) Assignment 1 due (October 1)	**MONDAY (Group 3 on-call)** NIST Cybersecurity Framework, pp. 24 – 45 Updating the NIST Cybersecurity Framework – Journey To CSF 2.0 CSF 2.0 Update Fact Sheet by NIST Success Story: Cimpress-FAIR **WEDNESDAY (Group 4 on-call)** MITRE Launches Cyber Resiliency Engineering Framework Navigator The Mandiant Cyber Threat Intelligence (CTI) Analyst Core Competencies Framework (White Paper, 2022) **Guest speaker:** Sean Madigan on 9/27 (in-person)
Week 7 10/2; 10/4	Topic 6: Industry self-regulatory efforts, Lessons 1 – 6	Questions to the guest lecturer (due 10/3) Quiz 2 on Readings and Lessons due (10/6)	**MONDAY (Group 1 on-call)** **& WEDNESDAY (Group 2 on-call)** 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) **Guest speaker:** Jean Camp (waiting to confirm)
Module 3: Cybersecurity policy at the national level			
Week/Dates	**Topic**	**Deliverables**	**Readings**
Week 8 10/9 (no class, fall break); 10/11	Topic 7: US laws and policies, Lessons 1 – 6	Questions to the guest lecturer (due 10/10) Assignment 2 begins (October 15)	**WEDNESDAY (Group 3 on-call)** Survey of US Laws Read and research proposed policy/rules Bulk Collection of Signals Intelligence, by National Academies (2015) (Section 1.4.1) Listening In, by S. Landau (Chapters 4-5) **Guest speaker:** Susan Landau on 10/11 (via Zoom)
Week 9 10/16; 10/18	Topic 8: Critical infrastructure, Lessons 1-3	Questions to the guest lecturer (due 10/17) Questions to the guest lecturer for **week 10** (due 10/22)	**MONDAY (Group 4 on-call)** **& WEDNESDAY (Group 1 on-call)** Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards, by A. Clark-Ginsberg and Slayton, R. (2019) **Guest speaker:** Rebecca Slayton on 10/18 (via Zoom)

Week 10 10/23; 10/25	Topic 9: Protecting government networks, Lessons 1 – 2	Assignment 2 (due 10/29) Quiz 3 on Readings and Lessons (due 10/28)	**MONDAY (Group 2 on-call)** U.S. National Cybersecurity Strategy (2023) Where the New National Cybersecurity Strategy Differs From Past Practice by H. Lin (2023) WEDNESDAY 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) **Guest speaker:** Herb Lin on 10/23 (via Zoom)
Module 4: Cybersecurity and International Relations			
Week/Dates	**Topic**	**Deliverables**	**Readings**
Week 11 10/30; 11/1	Topic 10: Cyberspace and inter-state conflict, Lessons 1 – 5	Questions to the guest lecturer (due 10/31)	**MONDAY (Group 3 on-call)** 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) WEDNESDAY Could Confrontation in Cyberspace Escalate the War in Ukraine? by The Soufan Center (22 Jun 2022) Russian Cyber Operations in the Invasion of Ukraine, by H. Lin (2022) The Purposes of U.S. Government Public Cyber Attribution by J. Bateman (2022) Hunting Russian Intelligence "Snake" Malware by CISA (2023) **Guest speaker:** Emily Goldman on 11/1 (via Zoom)
Week 12 11/6; 11/8	**In-class work on the Bilateral Cyber Agreement**	Assignment 3 Bilateral Cyber Agreement begins (November 6)	Read and study samples of the bilateral cyber agreements
Week 13 11/13; 11/15	Topic 11: International Responses	Questions to the guest lecturer (due 11/14) Questions to the guest lecturer for **week 14** (due 11/19)	**WEDNESDAY (Group 4 on-call)** What Israel's Strike on Hamas Hackers Means For Cyberwar The Israeli Odyssey toward its National Cyber Security Strategy, by Dima Adamsky **Guest speaker:** Amit Sheniak on 11/15 (via Zoom)

Week 14 11/20; 11/22 (no class)	Topic 12: Global Internet Governance, Lessons 1 – 5	Questions to the guest lecturer for **week 15** (due 11/26)	**MONDAY (Group 1 on-call)** 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) The EU-U.S. Data Privacy Framework: Background, Implementation, and Next Steps (2022) The new Trans-Atlantic Data Privacy Framework [video] (2022) Schrems II rulling (starting with paragraph 80) **Guest speaker:** Dominika Kuźnicka-Błaszkowska on 11/20 (in-person)
Week 15 11/27; 11/29	Topic 13: International Norms and Treaties, Lessons 1 – 3	Questions to the guest lecturer (due 11/28) Quiz 4 on Readings and Lessons due (December 3)	**MONDAY (Group 2 on-call)** 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) **WEDNESDAY (Group 3 on-call)** 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) **Guest speaker:** Milton Mueller on 11/27 (in-person) **Guest speaker:** Peter Swire on 11/29 (in-person)
Week 16 12/4	**In-class work on the Bilateral Cyber Agreement**	Assignment 3 (due 12/10) Peer evaluation (due 12/10)	

Course Policies

Diversity within the Classroom

The TA and I are fully committed to creating a learning environment that supports diversity of thought, perspectives, experiences, and identities. We urge each of you to contribute your unique perspectives to discussions of course questions, themes, and materials so that we can learn from them, and from each other. I want students to learn to see from each other's points of view even if they disagree with what each

other say, and to learn to accept each other as fellow scholars. Every person in this class will have an equal chance to speak and share their opinion with the understanding that they must give each other the same respect and understanding. This class will explore issues that may be contentious. I expect that all students treat each other with respect. This means that all arguments in the class should be based on factual assertions as opposed to assertions as opposed to demeaning insults. Finally, I will not tolerate the denigration of anyone in the class because of their adopted or prescribed social, religious, political, ethnic, racial, gender-based or sexual identities. If you should ever feel excluded, or unable to fully participate in class for any reason, please let TA/me know.

Online Student Conduct and Netiquette

Communicating appropriately in the online classroom can be challenging. In order to minimize this challenge, please keep communications with your fellow students and the instructions team professional and courteous. 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.

Gender-inclusive Language and Preferred Names/Pronouns

Language is gender-inclusive and non-sexist when we use words that affirm and respect how people describe, express, and experience their gender. Just as sexist language excludes women's experiences, non-gender-inclusive language excludes the experiences of individuals whose identities may not fit the gender binary, and/or who may not identify with the sex they were assigned at birth. Identities including trans, intersex, and genderqueer reflect personal descriptions, expressions, and experiences. Gender-inclusive/non-sexist language acknowledges people of any gender (for example, first year student versus freshman, chair versus chairman, humankind versus mankind, etc.). It also affirms non-binary gender identifications and recognizes the difference between biological sex and gender expression. In our classes, we should all use gender-inclusive words and language whenever possible in the classroom and in writing. Students, faculty, and staff may share their preferred pronouns and names, either to the class or privately to the professor, and these gender identities and gender expressions should be honored.

Communication Policy

Email personal concerns, including grading questions, to the professor/TA 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.

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/.

Georgia Tech's Library provides rich resources to make your research and writing a success. Consult the Library's Public Policy Research Guide (https://libguides.library.gatech.edu/public-policy), take a class at the library (https://www.library.gatech.edu/research-help-support/library-classes), and/or use the library's help & support (https://library.gatech.edu/research-help-support).

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, resulting in 0 points. In addition, 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.

Policy on the Use of ChatGPT

You may not use ChatGPT for homework assignments.

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.

Children in Class

Currently, the university does not have a formal policy on children in the classroom. The policy described here is thus a reflection of my own beliefs and commitments to students who happen to also be parents. I ask that all students work with me to create a welcoming environment that is respectful of all forms of diversity, including diversity in parenting status.

Babies are welcome in class as often as necessary to support their feeding relationship (breast-feeding or bottle).

For older children, I understand that minor illnesses and unforeseen disruptions in childcare often put parents in the position of having to miss class. While this is not meant to be a long-term child-care solution, occasionally bringing a child to class to cover gaps in care is perfectly acceptable.

In all cases where babies and children come to class, I ask that you sit close to the door so that if your little one needs special attention and is disrupting learning for other students, you may step outside until their need has been met. Non-parents in the class, please reserve seats near the door for your parenting classmates.

Campus Resources for Students

In your time at Georgia Tech, you may find yourself in need of support. Below you will find someresources to support you both as a student and as a person.

Academic support

- **Center for Academic Success** http://success.gatech.edu
  - 1-to-1 tutoring https://tutoring.gatech.edu/tutoring/
  - Peer-Led Undergraduate Study (PLUS) https://tutoring.gatech.edu/plus-sessions/
  - Academic coaching https://advising.gatech.edu/academic-coaching
- **Residence Life's Learning Assistance Program** https://housing.gatech.edu/learning-assistance-program
  - Drop-in tutoring for many 1000 level courses
- **OMED: Educational Services** https://omed.gatech.edu/academic-support
  - Group study sessions and tutoring programs
- **Communication Center** (http://www.communicationcenter.gatech.edu)
  - Individualized help with writing and multimedia projects
- **Academic advisors for your major** http://advising.gatech.edu/

Personal Support

Georgia Tech Resources

- **The Office of the Dean of Students**: https://studentlife.gatech.edu/content/dean-students or https://studentlife.gatech.edu/content/get-help-now; **404-894-6367**; Smithgall Student Services Building 2nd floor
  - You also may request assistance at https://studentlife.gatech.edu/content/get-help-now
- **Counseling Center**: http://counseling.gatech.edu; **404-894-2575**; Smithgall StudentServices Building 2nd floor
  - Services include short-term individual counseling, group counseling, couplescounseling, testing and assessment, referral services, and crisis intervention. Their website also includes links to state and national resources.
  - *Students in crisis may walk in during business hours (8am-5pm, Monday throughFriday) or contact the counselor on call after hours at **404-894-2204**.*

- **Students' Temporary Assistance and Resources (STAR):** https://studentlife.gatech.edu/content/star-services
  - Can assist with interview clothing, food, and housing needs.
- **Stamps Health Services**: https://health.gatech.edu; **404-894-1420**
  - Primary care, pharmacy, women's health, psychiatry, immunization and allergy,health promotion, and nutrition
- **OMED**: Educational Services: http://www.omed.gatech.edu
- **Women's Resource Center: http://www.womenscenter.gatech.edu; 404-385-0230**
- **LGBTQIA Resource Center: http://lgbtqia.gatech.edu/; 404-385-2679**
- **Veteran's Resource Center: http://veterans.gatech.edu/; 404-385-2067**
- **Georgia Tech Police: 404-894-2500**

National Resources:

- The National Suicide Prevention Lifeline provides free and confidential support 24/7 to those insuicidal or emotional distress at **1-800-273-8255**
- The Trevor Project provides crisis intervention and suicide prevention support to members ofthe LGBTQ+ community and their friends. They are available 24/7 by telephone (**1-866-488- 7386**), chat (http://www.thetrevorproject.org; 3-10pm Eastern, 7 days a week), and text (Text"Trevor" to **1-202-304-1200**; available 3-10pm, M-F).

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.