Georgia Institute of Technology

Course Syllabus: PUBP 8823_Geopolitics of Cybersecurity – WORKING DRAFT

Spring 2026, OCY	School of Public Policy, Ivan Allen College
Delivery: 100% Web-Based, Asynchronous	Content Delivery via Canvas
Dates course will run: January 18 – May 7	

Instructor Information

Professor Jon Lindsay	Email: jlindsay30@gatech.edu
Weekly Office Hours via Zoom (See Canvas schedule)	Teaching Assistants: Daniel A. Fernandez, danielf@gatech.edu Helen Dong, zdong92@gatech.edu Dennis Murphy, dmurphy77@gatech.edu

General Course Information

Description

This course provides students with a framework for interpreting power politics in and through cyberspace. The organizing assumption of the course is that classic concepts from international relations remain useful for understanding modern technologies, but they must be combined in new ways to explain the potential for exploitation and subversion at scale. The course provides tools for analyzing cyber power, which is organized deception via information systems for strategic advantage. Cyber power differs in important ways from military power, bargaining power, and soft power. Different political logics are often combined in practice, which creates complex strategic tradeoffs. Students will learn how to analyze these tradeoffs in modern cyber campaigns and in the use of cyber power for national security objectives.

Pre- &/or Co-Requisites

There are no formal prerequisites for this course. Yet, all students should have some preparation in either the engineering or strategic foundations of cybersecurity. This may include but is not limited to cryptography, security engineering, network security, human behavior, public policy, or international security. This course is an interdisciplinary seminar where students will learn from their peers in other disciplines.

Course Goals and Learning Outcomes

The course is designed with two different kinds of students in mind: students of technology and students of politics. For students of technology, the book provides a gentle introduction to foundational concepts in international relations (IR). Technical knowledge is invaluable for understanding how cyber conflict works, but we also want to understand why it happens. IR is the study of power, wealth, and ideas in the global system. They provide context for technical operations. Upon completion of this course, you will understand how IR concepts of coordination, warfare, coercion, and deception can be applied to analyze cyber campaigns. This course could be called 'IR for hackers.'

For students of politics, the course explores the neglected problem of intelligence and covert action. Philosophers like Sun Tzu, Kautilya, and Machiavelli discuss espionage and deception. But secret statecraft is undertheorized in modern IR. The strategic logic of deception is interesting because it muddies distinctions between institutional cooperation and anarchic conflict, or liberalism and realism. Spies pretend to be trusted colleagues, and malware masquerades as legitimate software. Indeed, large-scale cooperation is the wellspring of cyber conflict. Upon completion of this course, you will understand

how the paradoxical logic of deception is expressed in modern cyber campaigns. This course could be called 'cooperation-enabled conflict.'

Course Level Objectives

Upon successful completion of the course, you will be able to:

1. Recognize the historical origins of modern cyber operations in classical intelligence.
2. Recognize the growing role of nonstate actors in, and increasing scale of, global cyber conflict.
3. Describe how social institutions enable and constrain cyber conflict (and intelligence).
4. Analyze the motivations, constraints, and effectiveness of cyber campaigns.
5. Assess the role of cyber capabilities in national security strategies.

Course Text

There are no required works to purchase for this course. All required learning materials will be linked in the modules or be freely available via Course eReserves or GA Tech Library resources.

Course Requirements, Assignments & Grading

Assignment Distribution and Grading Scale

Grading Type	Description of Graded Assignments	% Grade
Points	Participation (as reflected in participation in live office hour, questions to instructor, TAs, or extra effort in discussion) (Worth up to 100 points)	5%
Points	Perusall Readings [4] (Worth up to 100 points)	10%
Points	Discussion Essays [4] (Worth up to 100 points)	50%
Points	Group Project [4] (Worth up to 100 points)	35%

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%

Description of Graded Components

Participation. Instructors and TAs will track substantive participation as reflected in feedback on discussion groups and office hours questions. Interaction and constructive conversation with other students on the themes of the course are especially encouraged. We especially appreciate engagement in the discussion assignments that goes beyond the minimum requirements and sustains conversations.

Perusall. Read and annotate required readings using the Perusall app. This will help you to begin thinking critically about the issues to address the discussion questions.

Discussion. The discussion assignment is offered in lieu of quizzes or midterms and should be treated with equivalent seriousness. These assignments are offered as discussions in order to encourage class discussion, and to gauge intellectual engagement with course lectures and required readings. The discussion questions are assigned in batches for each module. Within each module there are several topics. For each topic, you will add a new discussion post with a short essay responding to the discussion prompt. Initial answers should reflect the efforts of the individual student, followed by conversational engagement with others (each student must reply to at least one other student for each topic). There are no simple 'right' answers and many questions ask you to reflect on or apply concepts. Your grade is based on a holistic assessment of (complete) responses to each question and the quality (not quantity) of your answers. Be sure to read the detailed instructions on the discussion assignment and include PDF attachments of all AI chat logs.

Project. Read the detailed instructions on the group project, which specify exactly what the deliverables should contain. The overall project is an application of the cyber power framework to compare the strategy and operations of two historical cyber or intelligence campaigns. Groups of 4-5 students will be assigned at the beginning of the course. The assignments are cumulative, which will enable you to get feedback along the way. All members of the group will receive the same grade for each of the four group assignments (worth 25% of your grade); an additional component (worth 10%) will be assessed by the instruction team based on private assessments by each group member of the contributions of each other group member (thus if all members are happy with the equal contributions of all others, then it should be easy for everyone to get full marks).

Extra Credit Opportunities

Students have the option of analyzing emerging cybersecurity incidents in the news during the term. There is always something happening, and it is a good exercise to apply the concepts of the course to make sense of emerging and uncertain events. This should be in the form of a 500-word op-ed that applies some concept from the lectures or reading to an event that has transpired sometime in the past two months. Students can turn in at most one each week and at most three during the term. Each is worth up to a 2% bonus for a total of up to 6% bonus added on top of your final grade (meaning you could conceivably get 106% in the course, which would still be just an A).

Submitting Assignments
See the assignment schedule.

Assignment Due Dates
All assignments a will be due at the times listed above. These times are subject to change so please check back often. Please convert from UTC to your local time zone using a Time Zone Converter.

Late and Make-up Work Policy

Late assignments will be penalized 5 points per 24 hours, which means a full letter grade deduction every two days. Make-up work will be at the discretion of the instructor on a case-by-case basis.

Timing Policy

- The Modules follow a logical sequence that includes knowledge-building and experience-building.

- Assignments should be completed by their due dates, for timely peer assessment. Peer assessments should also be completed by their due dates, to give timely feedback.
- You will have access to the course content for the scheduled duration of the course.

Grading and Feedback
Instructors will aim to provide feedback on assignments one week after the due date.

Technology Requirements and Skills

Computer Hardware and Software

- High-speed 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 and ability to use Adobe PDF software (install, download, open and convert)
- Mozilla Firefox, Chrome and/or Safari browsers

Technology Skills
Students will learn to create online presentations and write group reports as part of their group project. Online presentations can be recorded using Zoom and slides on PowerPoint, but student groups are welcome to use any other software. Reports will typically be written in Word, but any editor that produces PDF output is acceptable.

Canvas and Course Materials
This class will use Canvas to deliver course materials to online students. ALL course materials and activities will take place on these two platforms. To login to Canvas visit canvas.gatech.edu. The course textbook is Jon Lindsay, *Age of Deception: Cybersecurity and Secret Statecraft* (Cornell, 2025). Chapters will be available through Perusall. An open access (free) digital copy can be obtained from Cornell University Press: www.cornellpress.cornell.edu . Paperback copies can be found for purchase, optionally.

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, or message board, use the following guidelines:

- Include a descriptive title for the subject field that includes 1) the name of course 2) the issue. Do NOT just simply type "Help" into the subject field or leave it blank.
- List the steps or describe the circumstance that preceded the technical issue or error. Include the exact wording of the error message.
- When possible, always include a screenshot(s) demonstrating the technical issue or error message.
- Also include what you have already tried to remedy the issue (rebooting, trying a different browser, etc.).

Course Policies, Expectations & Guidelines

Attendance and/or Participation
This is an asynchronous course. Students are expected to watch all lectures. Students are also required to participate in discussions, as detailed in the assignments section.

Collaboration & Group Work

Learning to work together productively in a group is an important life skill. This course is built around a group project that includes several deliverables. Students are expected to organize tasks themselves and fairly divide the work into subtasks. This does not mean that all students are expected to do the same thing. For instance, it would be permissible to have some group members take on more responsibility for research if others take more responsibility for presentation. The important thing is that all members share a sense of fairness and equity in the division of labor. Students will be expected to include a statement reflecting on their group experience in the final project.
Students should find a forum to meet often to discuss their group project.
I expect that groups will make efforts to address and resolve any disagreements that emerge. If groups cannot do this themselves, they should contact the instructor to intervene.

Extensions, Late Assignments, & Re-Scheduled/Missed Exams

Assignments are due on the date posted. Late assignments will be penalized 5 points per 24 hours, which means a full letter grade deduction every two days. Extensions will be granted on a case-by-case basis. Students must request extensions in advance.

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 the student body. See Student-Faculty Expectations for an articulation of some basic expectation that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, 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 email, Piazza, and/or Canvas announcement tool. It is the responsibility of students to check email messages and course announcements to stay current in their online courses.

Communication Policy

- Please use professional etiquette when communicating with your professors, your TAs, and your peers.
- Email course questions and personal concerns, including grading questions, to Dr. Rubin privately. Do NOT submit posts of a personal nature to the discussion board.
- Email will be checked regularly, Monday – Friday. During the week, we strive to respond to all emails within 24 hours; on weekends and holidays, allow up to 48 hours. If there are special circumstances that will delay a response, we will make an announcement to the class.
- Student Forum/Q&A discussion boards will be checked twice per day Monday through Friday; Saturday and Sunday, these discussion boards will be checked once per day.
- Virtual office hours will be held using the Zoom link on Canvas. The instructor will hold Virtual Office Hours once a week for 60 minutes, or by appointment. Special topic hours may be announced in advance. Teaching Assistants are also available to schedule separate office hours if instructor times are inconvenient or students/groups desire additional discussion/assistance.
- For questions related to technology, please contact: Digital Learning Support.

Online Student Conduct and (N)etiquette

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:

1. *Read first, Write later*. It is a good idea to read the ENTIRE set of posts/comments on a discussion board before posting your reply, to prevent repeating commentary or asking questions that have already been answered.
2. *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.
3. *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. ☺
4. *Consider the privacy of others.* Ask permission prior to giving out a classmate's email address or other information.
5. *Keep attachments small*. If it is necessary to send pictures, consider changing the size to 250kb or less (one free, web-based tool to try is picresize.com).
6. *No inappropriate material*. Do not forward virus warnings, chain letters, jokes, etc. to classmates or instructors. The sharing of pornographic material is forbidden.

***NOTE**: 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 Electronic 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 Academic Honor Code.

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 to set up a time to discuss your learning needs.

Copyright

- *"The Educators Guide to Copyright, Fair Use, and Creative Commons"*
- You cannot simply use everything you find on the Web because some content is copyrighted, pirated, misleading, hallucinated, or intentionally deceptive
- Yet there are many online resources you can use in your research and reproduce in your assignments. Consider:
    - Understanding Fair Use
    - What Can Be a Violation
- What is Creative Commons?
    - Look for a Creative Commons License
    - Finding Creative Commons Images
    - Creative Commons and Image Attribution
    - Adapting Creative Commons Images
- What are Free and Public Domain Images?
    - Attributing free to use and public domain images
    - Suggested free and public domain image Websites
        - Pixabay
        - Openclipart
        - Wikimedia Commons
        - The Commons
        - Getty Open Content Images
        - Getty Images
- Copyright and Videos
    - YouTube Copyright Basics
    - Curriculum and Text

Georgia Institute of Technology

Course Syllabus: PUBP 8823_Geopolitics of Cybersecurity – WORKING DRAFT

Course Readings

Module 1: What is Cyber Conflict?

- Topic 1: Overview
  - SentinelOne. 2023. "The New Frontline of Geopolitics: Understanding the Rise of State-Sponsored Cyber Attacks." *SentinelOne*. https://www.sentinelone.com/blog/the-new-frontline-of-geopolitics-understanding-the-rise-of-state-sponsored-cyber-attacks/ (January 29, 2024).
  - Recommended: Yarhi-Milo, Keren, Charles L. Glaser, Manjari Chatterjee Miller, Michael W. Doyle, Stephen G. Brooks, and Tanisha M. Fazal. "The Real Rules of International Relations [Six Parts]." *Foreign Affairs*, 2024. https://www.foreignaffairs.com/content-packages/real-rules-international-relations.
- Topic 2: The Cyberwar narrative
  - Panetta, Leon E. "Remarks by Secretary Panetta on Cybersecurity." Presented at the Business Executives for National Security, New York, October 11, 2012. Video: https://www.c-span.org/video/?308750-1/secretary-leon-panetta-cybersecurity. Transcript: https://nsarchive.gwu.edu/document/21479-document-78.
  - Neuberger, Anne. 2025. "China Is Winning the Cyberwar." *Foreign Affairs* 104(5). (October 30, 2025). https://www.foreignaffairs.com/china/china-winning-cyberwar-artificial-intelligence
  - Dunn Cavelty, Myriam. 2013. "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse." *International Studies Review* 15(1): 105–22. https://www.jstor.org/stable/pdf/24033170.pdf .
- Topic 3: The intelligence turn
  - Lindsay, Jon. *Age of Deception*. Introduction and Chap. 1.

Module 2: Components of Cyber Power

- Topic 1: The Logic of Coordination
  - Locke, John. Second Treatise of Government. (1688), Chap IX ("Of the Ends of Political Society and Government").
  - Slayton, Rebecca, and Brian Clarke. "Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005." Technology and Culture 61, no. 1 (2020): 173–206.
  - Lindsay, Jon. *Age of Deception*. Chap. 3.
- Topic 2: The Logic of Warfare
  - Clausewitz, Carl von. *On War*. Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976. [OK to use other versions including Project Gutenberg eBook.] Focus on:
    - Book 1, Ch 1 ("What is War?), pp. 75-89,
    - Book 1, Ch 6 ("Intelligence in War"), pp. 117-118,
    - Book 1, Ch 7 ("Friction in War"), pp. 119-121
  - Rovner, Joshua, Rory Cormac, and Lennart Maschmeyer. 2025. "Sand in the Gears: Sabotage in World Politics." *European Journal of International Security*: 1–20. doi:10.1017/eis.2025.10025.
  - Smeets, Max. "Cyber Arms Transfer: Meaning, Limits and Implications." *Security Studies* 31, no. 1 (2022): 65–91.
- Topic 3: The Logic of Coercion
  - Schelling, Thomas C. Arms and Influence: With a New Preface and Afterword. New Haven, CT: Yale University Press, 2008. Ch 1.

- Jackson, Colin F. 2016. "Information Is Not a Weapons System." *Journal of Strategic Studies* 39(5–6): 820–46. doi:10.1080/01402390.2016.1139496.
- Lonergan, Erica D., and Shawn W. Lonergan. "Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises." *Security Studies* 31, no. 1 (January 1, 2022): 32–64. https://doi.org/10.1080/09636412.2022.2040584.

- Topic 4: The Logic of Deception
  - Sun Tzu. The Art of War. Translated by Michael Nylan. New York: W. W. Norton & Co., 2020. [OK to use other versions including Project Gutenberg eBook.] Focus on Ch 13.
  - Hassner, Ron E. 2025. "How to Deceive: A Supply-Side Approach." *Intelligence and National Security* 40(5): 838–62. doi:10.1080/02684527.2025.2546248.
  - Lindsay, Jon. *Age of Deception*. Chap. 2.

Module 3: Cyber Campaign Analysis

- Topic 1: Espionage—Bletchley Park
  - Lindsay, Jon. *Age of Deception*. Chap. 4.
- Topic 2: Sabotage—Stuxnet
  - Lindsay, Jon. *Age of Deception*. Chap. 5.
- Topic 3: Subversion—2016 Election
  - Lindsay, Jon. *Age of Deception*. Chap. 6.
- Recommended—Films
  - Topic 1: "The Imitation Game," 2014 [Fictionalization of Bletchley Park starring Benedict Cumberbatch]
  - Topic 2: "Zero Days," 2016 [Documentary on Stuxnet by Alex Gibney]
  - Topic 3: "Agents of Chaos," 2020 [Documentary on the 2016 US election by Alex Gibney]

Module 4: Cyber Strategy

- Topic 1: US Cyber Strategy
  - Lonergan, Erica D., and Michael Poznansky. 2024. "Competing Visions for US Grand Strategy in Cyberspace." *Security Studies* 33(4): 607–39. doi:10.1080/09636412.2024.2393862.
  - Schneider, Jacquelyn. 2025. "The Digital Cult of the Offensive and the US Military." *Journal of Strategic Studies* 48(1): 36–59. doi:10.1080/01402390.2024.2376542.
- Topic 2: Chinese Cyber Strategy
  - Creemers, Rogier. 2024. "The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy." *Journal of Contemporary China* 33(146): 173–88. doi:10.1080/10670564.2023.2196508.
  - Lindsay, Jon. *Age of Deception*. Chap. 7.
- Topic 3: Private Intelligence
  - Deibert, Ronald J. 2022. "Subversion Inc: The Age of Private Espionage." *Journal of Democracy* 33(2): 28–44. doi:10.1353/jod.2022.0016.
  - Work, J. D. "Evaluating Commercial Cyber Intelligence Activity." *International Journal of Intelligence and CounterIntelligence* 33, no. 2 (April 2, 2020): 278–308. https://doi.org/10.1080/08850607.2019.1690877.
- Topic 4: Special Topics
  - Pavur, James, and Ivan Martinovic. "Building a Launchpad for Satellite Cyber-Security Research: Lessons from 60 Years of Spaceflight." *Journal of Cybersecurity* 8, no. 1 (January 1, 2022): tyac008. https://doi.org/10.1093/cybsec/tyac008.
  - King, Anthony. "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence." *Journal of Global Security Studies* 9, no. 2 (June 1, 2024): ogae009. https://doi.org/10.1093/jogss/ogae009.

- Quinn, Doug, Patrick Wolverton, and Scott Storm. "Quantum Computing: A New Competitive Factor with China." *Joint Force Quarterly*, no. 110 (July 2023). https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-110/jfq-110_35-45_Quinn-Wolverton-Storm.pdf.
- Lindsay, Jon. *Age of Deception*. Conclusion.