PUBP 8823/4823; INTA8803:
Subversion and Cyber Conflict
Power in the Shadows of World Politics

Fall Term 2026

Tuesday & Thursday 9:30am – 10:45am
Location: Clough 131

Instructors
Dr. Lennart Maschmeyer
Assistant Professor, Carter School

Office Hours: upon request

Introduction

This course introduces students to subversion, an age-old and routinely used yet understudied instrument of power. As geopolitical competition intensifies, there are widespread and growing fears of hybrid threats, cyberwarfare, and disinformation campaigns. Many argue these are novel threats empowered by disruptive technological change that will revolutionize security competition. In this seminar, we will take a step back and look at the big picture to clarify the nature of these threats, identify their strategic heritage, and assess their impact. As we will see, these supposedly new threats are all different sides of the same subversive coin. States have long used shadowy means to interfere in each other's affairs and gain advantages in the shadow of hard power politics—the discipline of International Relations has just never studied these systematically. In the absence of scientific examination, myth, and speculation have taken hold.

This class takes a different route by systematically analyzing the nature of subversion as an instrument of power, its mechanism of action, and its strategic value. Drawing on a wide range of historic and contemporary case studies, we will examine how states have used the diverse tools of subversion to achieve strategic goals. We will identify both the opportunities and challenges that subversion brings, different strategies of subversion and their strategic scope. Building on this groundwork, we will examine how new technologies change these characteristics. This journey will lead us from the Cold War's spy games to today's intensifying Cyber Conflict and the rise of Artificial Intelligence. To that end, we will examine several major cyber operations in detail. Three of these discussions will be led by leading threat intelligence experts who were personally involved in the analysis.

The course is a lecture-seminar, meaning each session starts with a short lecture to summarize the key points and debates in the reading. Next, we will explore these debates in an open discussion. For each session, a set of discussion questions will be uploaded to Canvas in advance to help you prepare.

Required Materials

All required materials will be uploaded to Canvas.

Assignments and Assessment

1. **Participation (20%)**

   This class is primarily a seminar where key questions and insights will come out of our conversations as we collectively engage with the material. That means it is essential to come prepared, and be ready to answer critical questions about the topic, the readings, and the implications. In other words, the more you put in, the more you will get out of it. To prepare effectively, read strategically. Identify the main argument(s) each text is presenting, the theory it is based on (if there is any), and the evidence used to support it. How convincing is this, and what are the weaknesses of the argument and the theory? How systematic and credible is the evidence presented? What do the authors miss, what do they fail to explain?

   When comparing texts, consider the authors in a dialogue. Are they talking about the same thing, reaching different conclusions? If so, why or why not? Or are they talking about different things even though supposedly addressing the same issue? Why is that, how do their approaches differ? Do they make different assumptions to start with, or do they develop theories that make them see concepts, mechanisms, and outcomes in a different way? Are these arguments complementary, meaning both can be true at the same time, or rival, meaning if one is true the other must be false? Why is that the case, or why not? How do we who know is right, and why?

2. **Quizzes (5% each, 20% total)**

   There will be four short multiple-choice quizzes testing your knowledge of the readings and lecture materials.

3. **Essay proposal (800 words) (10%) – Due by Oct 2**

   Prepare a concise proposal for a research essay to be delivered in the second half of the course that identifies an issue, formulates a research question, and lays out a strategy to answer it. Start by choosing an issue relevant to the topic of the course to examine in depth, and explain why it is important to consider. You are free to choose a theoretical or empirical issue, and a past, contemporary, or perhaps future issue. For example, you could focus on the relationship between subversion and war. Consequently, you need to formulate a research question and lay out a strategy to answer it.

   Following on the example above, a possible research question would be *how does subversion complement the use of force?* Or you could consider how the emergence of cyber operations changes the game of power politics.

   In this context, a possible research question could be: *why do states still use traditional subversion although cyber operations promise greater effectiveness?* There are many open questions and issues to pick, and the choice is yours. I recommend you focus on an issue that sparks your interest, rather than a question that seems easy to answer. Ideally, you would identify a puzzle, a development or outcome that existing literature does not answer, and develop an explanation—but having a puzzle is not necessary to get full marks. When formulating a research question, bear in mind that a "why" question involves a causal argument, whereas a "how" question is more process-oriented (constitutive, in the language of constructivist scholars). A "what" question is best avoided since it tends to lead to a descriptive story of what happened, rather than explaining why or how something has transpired.

   Once you have decided a topic and formulated a research question, think about how you can provide the best answer, and where you can find the evidence for it. For a conceptual

argument, lay out the basic steps involved in developing it. For a case study, identify potential sources of evidence and why you expect it to be useful and reliable in answering your question.

4. **Analytical Essay (2000 words) (20%) – *Due by Dec 4***
Write an analytical essay based on your proposal. A strong essay makes a coherent argument based on systematic analysis backed up by empirical evidence, as needed. Explain how or why something has happened or will likely happen, identify underlying causes and mechanisms, and convince your reader why your argument is the best possible explanation compared to alternatives. Don't tell a story, don't describe what happened or speculate on what may happen. Instead, focus on developing an analytical argument. Identify causal mechanisms behind things we can observe, and collect evidence to support your claims and conclusions. Ideally, consider alternate explanations for your observations, and explain why your own argument or theory is better supported by the evidence (or not).

5. **Group Policy Presentation (15-20 mins) (30%)**
    a. Prepare and deliver a presentation with your colleagues on a solution for a policy problem caused by subversion. Identify a challenge subversion creates for policy-makers both in its offensive use, as well as aiming to counter adversary subversion. Consider whether this challenge is unique, or distinct in some way, or of the same kind as similar challenges caused by other instruments of power and associated threats (diplomacy, sanctions, military strikes, biological warfare, terrorism, etc.) Also consider whether other states have come up with solutions for similar or identical challenges, to what extent these solutions would or would not work in the US context—and why. Next, consider which policy area this challenge falls under, and whether addressing it requires combining multiple policy areas. Finally, develop a solution and explain why it is both feasible and effective.
    b. Each group member individually submits a brief evaluation of their other group members, giving letter grade (A to F). The purpose of this evaluation is to provide accountability and discourage free-riding, but will only be used as input for final grades determined by the instructor.

Schedule

Aug 25 & 27	*Course Introduction*
Sep 1	*From Cyber War to Subversion I*
Sep 8 & 10	*From Cyber War to Subversion II*
Sep 15 & 17	*Subversive Mechanisms*
Sep 18	**Quiz 1 due**
Sep 22 & 24	*Strategies of Subversion*
Sep 29 & Oct 1	*Secret Agents and Covert Operations*
Oct 2	**Proposal Due**
Oct 6	****No Class – Break****
Oct 8 & 13	*Hackers and Cyber Operation*
Oct 15	**Group Presentations**
Oct 16	**Quiz 2 due**
Oct 20 & 22	**Group Presentations II**
Oct 27 & 29	*Cases: Stuxnet and Fast16*
Nov 3 & 5	*Cases: SolarWinds and Salt Typhoon*
Nov 10 & 12	*Cyber in (Hybrid) War: Ukraine*
Nov 13	**Quiz 3 due**
Nov 17 & 19	*AI and Cyber Conflict*

Nov 24	*Agentic AI and Subversio*
Nov 26	****No Class – Break****
Dec 1 & 3	*Cyber Threat Intelligence*
Dec 4	**Essay Due**
Dec 8	*US Cyber Strategy*
Dec 9	**Quiz 4**

Sessions

1. **Introduction (Aug 25 & 27)**
   Cyberwarfare is upon us, and it changes everything! Or does it? Have we been here before?

   Literature
   - Vaughan-Nichols, Steven J. "Will World War III Begin in Cyberspace? | Computerworld." Computerworld, January 25, 2022.
   - Miller, Maggie. "Russian Invasion of Ukraine Could Redefine Cyber Warfare." POLITICO, January 28, 2022.
   - Alexander, Keith."Cyber Warfare in Ukraine Poses a Threat to the Global System." Financial Times, February 15, 2022.
   - Morrison, Sara. "Is the Cyberwar Coming or Is It Already Here?" Vox, February 25, 2022.
   - Gibney, Elizabeth. "Where Is Russia's Cyberwar? Researchers Decipher Its Strategy." Nature 603, no. 7903 (2022): 775–76.

2. **From Cyber War to Subversion (Sep 1)**

   ****No Class on Sep 3****

   This session traces the evolution of strategic thought and debates in cyber conflict. Following a wave of cyberwar theories in the late 1990s and 2000s, contemporary scholarship shows an emerging consensus that cyber conflict primarily takes place below the threshold of armed conflict and belongs more closely to the world of covert operations. Scholars disagree on the impact of technological change on this area of competition and its strategic significance.

   Literature
   - Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (April 1, 1993): 141-158.
   - Lynn, William J III. "Defending a New Domain." *Foreign Affairs*, 2010. https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain.
   - Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32. https://doi.org/10.1080/01402390.2011.608939.

3. **What is Subversion (Sep 8 & 10)**
This session introduces the concept of subversion and the confusion around it. We will look back at how the shadowy nature of subversion has clouded its meaning and driven fears of subversion as an all-consuming threat—both historically, and today. The term's meaning has been as elusive as the activity it describes, complicating analysis.

Literature

- Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. *Cyber Persistence Theory: Redefining National Security in Cyberspace*. 1st ed. Bridging the Gap. New York: Oxford University Press, 2022, Ch. 2.
- Rovner, Joshua. "Cyber War as an Intelligence Contest." *War on the Rocks*, September 16, 2019. https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/.
- Maschmeyer, Lennart. "Subversion, Cyber Operations, and Reverse Structural Power in World Politics." *European Journal of International Relations* 29, no. 1 (March 1, 2023): 79–103.

****

- Christopher S. Chivvis, "Hybrid War: Russian Contemporary Political Warfare," Bulletin of the Atomic Scientists: How Dangerous Is Hybrid War? 73, no. 5 (2017): 316-321.
- Blackstock, Paul W. The Strategy of Subversion: Manipulating the Politics of Other Nations. Chicago: Quadrangle Books, 1964. Pp. 34-40.
- Lee, Melissa M. "Subversive Statecraft," December 6, 2019. https://www.foreignaffairs.com/articles/2019-12-04/subversive-statecraftLinks to an external site.

4. **The Mechanisms: How does Subversion work? (Sep 15 & 17)**
In the third week, we zoom in on how subversion works, what opportunities it provides for states, and what challenges it poses. We examine how subversion produces outcomes and how it compares to other instruments of power, such as war and diplomacy. Consequently, we will discuss why the distinct properties of subversion offer great strategic promise—informing associated fears. Next, we identify operational challenges and see how these limit the impact of subversion.

Literature

- Blackstock, Paul W. *The Strategy of Subversion: Manipulating the Politics of Other Nations*. Chicago: Quadrangle Books, 1964. Pp. 41-78.
- Kastner, Jill, and William C. Wohlforth. "A Measure Short of War." *Foreign Affairs* 100, no. 4 (June 22, 2021).

****

- Maschmeyer, Lennart. *Subversion: From Covert Operations to Cyber Conflict*. Oxford, New York: Oxford University Press, 2024. Ch.1

5. Strategies of Subversion: How and why do states use it? (Sep 22 & 24)
This session turns to the practice of subversion, identifying different strategies of subversion and examining how and why states have used them alongside other instruments of power and associated strategies.

Literature

- Blackstock, Paul W. *The Strategy of Subversion: Manipulating the Politics of Other Nations*. Chicago: Quadrangle Books, 1964. Pp. 23-34, 287-292.
- Beilenson, Lawrence W. *Power Through Subversion*. Washington D.C.: Public Affairs Press, 1972. Pp. 90-103; 139-149

****

- Kastner, Jill, and William C. Wohlforth. *A Measure Short of War: A Brief History of Great Power Subversion*. Oxford Scholarship Online Political Science. New York, NY: Oxford University Press, 2025, pp. 25-39.
- Lee, Melissa M. *Crippling Leviathan: How Foreign Subversion Weakens the State*. Ithaca [New York]: Cornell University Press, 2020. Chapter 2.

6. Classic Means: Secret Agents and Covert Operations (Sep 29 & Oct 1)
This session evaluates subversion's classic means and their track record. We start by examining how infiltration and exploitation looked like in practice, and the challenges involved. Taking a step back, we consider what success and failure look like and look at the evidence of subversive operations. What effects did they achieve, how did they contribute to actors' strategic goals, and to what geopolitical consequence?

Literature

- Andrew, Christopher M., and Vasili Mitrokhin. *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*. 1st ed. New York: Basic Books, 1999. Ch. 12 & 15.
- Blackstock, Paul W. *The Strategy of Subversion: Manipulating the Politics of Other Nations*. Chicago: Quadrangle Books, 1964, Ch. 15.

****

- O'Rourke, Lindsey A. *Covert Regime Change: America's Secret Cold War*. Cornell Studies in Security Affairs. Ithaca, NY: Cornell University Press, 2018, Ch. 5.
- Treverton, Gregory F. *Covert Action: The Limits of Intervention in the Postwar World*. I.B. Tauris, 1987. Introduction, pp. 28-44

7. Digital Means: Hackers and Cyber Operations (Oct 8 & 13)
Cyber operations offer a novel means to implement subversive strategies. In this session we explore why and how cyber operations subvert information technology and the way we use it in modern societies. Finally, we turn to a case study of recently indicted Russian hackers to explore how this works in practice.

Literature

- Anderson, James P. "Computer Security Technology Planning Study (Volume II)," October 1972. Pp. 1-4, 12-17.
- Erickson, Jon. *Hacking: The Art of Exploitation*. San Francisco: No Starch Press, 2003. Pp. 1-4, 115-118.
- Mitnick, Kevin, and Steve Wozniak. *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. New York: Back Bay Books, 2012, Ch. 2.

****

- Maschmeyer, Lennart. *Subversion: From Covert Operations to Cyber Conflict*. Oxford, New York: Oxford University Press, 2024. Ch.2

8. Group Presentations (Oct 15)

9. Group Presentations (Oct 20 & 22)

10. Cyber Cases: Stuxnet and Fast16 (Oct 27 & 29)

Cyber operations continue to hold great promise as an instrument of power and evoke correspondingly significant fears among potential victims. Literature on potential futures abounds. Yet when it comes to the actual track record of cyber operations, the air quickly thins. This week we will examine this mismatch based on a classic case, the Stuxnet operation against Iran's nuclear program. Next, we take a look at its only recently discovered predecessor, the insidiously subversive Fast16 operation.

Literature

- Farwell, J.P., and R. Rohozinski. "Stuxnet and the Future of Cyber War." *Survival* 53, no. 1 (2011): 23–40. https://doi.org/10.1080/00396338.2011.555586.
- Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (2013): 365–404. https://doi.org/10.1080/09636412.2013.816122.

****

- "Fast16 | Mystery ShadowBrokers Reference Reveals High-Precision Software Sabotage 5 Years Before Stuxnet." *SentinelOne*, April 23, 2026. https://www.sentinelone.com/labs/fast16-mystery-shadowbrokers-reference-reveals-high-precision-software-sabotage-5-years-before-stuxnet/.
- Symantec. "Fast16: Pre-Stuxnet Sabotage Tool Was Built to Subvert Nuclear Weapons Simulations." Accessed June 5, 2026. https://www.security.com/threat-intelligence/fast16-nuclear-sabotage.
- Zetter, Kim. "Experts Confirm the Fast16 Malware Was Sabotaging Nuclear Weapons Tests, Likely in Iran." ZERO DAY, May 16, 2026. https://www.zetter-zeroday.com/experts-confirm-the-fast16-malware-was-sabotaging-nuclear-weapons-tests-likely-in-iran/.

11. Cyber Cases: SolarWinds and Salt Typhoon (Nov 3 & 5)

Guest lecturer: Silas Cutler, Principal Security Researcher at Censys

Having looked at (allegedly…) US-sponsored operations, this week we focus on the US as the target. We will examine two landmark espionage operations sponsored by the United States' two key geopolitical adversaries – Russia and China. The SolarWinds operation ingeniously exploited a supply-chain vulnerability to gain access to US government communication. We are lucky to have one of the researchers who worked on the actual investigation as a guest lecturer: Silas Cutler, now Principal Security Researcher at Censys. Following that, we will take look under the hood of the Salt Typhoon breach whose impact still reverberates around the national security community. We will see how this operation exploited a vulnerability created by the United States own intelligence community, illustrating the dilemma between visibility and vulnerability intelligence agencies face in cyber conflict.

Literature

- *https://www.crowdstrike.com/en-us/blog/sunspot-malware-technical-analysis/*

  ****

- Krouse, Sarah, Robert McMillan, and Dustin Volz. "Exclusive | China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack." Politics. *Wall Street Journal*, September 25, 2024. https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835.
- "Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System | CISA." September 3, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

12. Cyber in (Hybrid) War: Ukraine (Nov 10 & 12)

This week is dedicated to the case of Ukraine, in several respects the most important case study in the modern history of cyber conflict. It is simultaneously the most significant and long-running case of a leading actor (Russia) pursuing cyber campaigns below the threshold of war, and the first case of cyber operations in war involving a major military power (Russia). We will see how the actual effectiveness and impact of cyber operations we observed here challenge prevailing expectations and theories.

Literature

- Greenberg, Andy. "How An Entire Nation Became Russia's Test Lab for Cyberwar." *WIRED*, June 20, 2017. https://www.wired.com/story/russian-hackers-attack-ukraine/.
- Maschmeyer, Lennart. *Subversion: From Covert Operations to Cyber Conflict*. Oxford University Press, 2024, Ch. 4

  ****

- Maschmeyer, Lennart. *Subversion: From Covert Operations to Cyber Conflict*. Oxford University Press, 2024, Ch. 5

13. AI and Cyber Conflict (Nov 17 & 19)

The rise of AI brings a host of critical questions: How do rapid advancements in artificial intelligence change cyber conflict? What new opportunities and challenges does this technology offer to actors? Do cyber operations become more dangerous, or do defenders gain the upper hand? What does it mean if they do? There is ample speculation and hype about these questions, not least by the frontier AI labs themselves. Systematic evidence and analysis remains scarce, but we will pick up what is there to figure out some of these answers.

Literature

- Taddeo, Mariarosaria, and Luciano Floridi. "Regulate Artificial Intelligence to Avert Cyber Arms Race." *Nature* 556, no. 7701 (April 2018): 296–98. https://doi.org/10.1038/d41586-018-04602-6.
- Burton, Joe, and Simona R. Soare. "Understanding the Strategic Implications of the Weaponization of Artificial Intelligence." *2019 11th International Conference on Cyber Conflict (CyCon)* 900 (May 2019): 1–17. https://doi.org/10.23919/CYCON.2019.8756866.
- Sims, Jeff. *BlackMamba: Using AI to Generate Polymorphic Malware*. July 31, 2023. https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware.

****

- Maschmeyer, Lennart. "Deception and Detection: Why Artificial Intelligence Empowers Cyber Defense over Offense." *International Security* 50, no. 3 (2026): 86–126. https://doi.org/10.1162/ISEC.a.398.
- Anthropic. "Claude Mythos Preview." April 7, 2026. https://red.anthropic.com/2026/mythos-preview/.

14. Agentic AI and Subversion (Nov 24)

AI agents are a new and revolutionary way not only to use computers, but to empower them to take autonomous action. Much of the current hype around revolutionary impacts of AI center around the capabilities of Agentic AI. As with any other technology, however, its adoption brings both opportunities and threats. While AI agents are a cutting-edge technology, they face a set of very human vulnerabilities that go right back to the core of subversion. In this session we will explore these vulnerabilities and implications for (cyber)security.

- Schiffman, Noah, and Jimmy Ardis. "Bridging Human Deception to AI Exploitation: A Systematic Review of Psychological Strategies in LLM Model Manipulation." No. 2026050075. Preprint, Preprints, May 4, 2026. https://doi.org/10.20944/preprints202605.0075.v1.
- "AI Hacking: Deceptive Behaviors as Cyber Weapons." *CSIAC*, n.d. Accessed June 1, 2026. https://csiac.dtic.mil/articles/ai-hacking-deceptive-behaviors-as-cyber-weapons/.
- Larcher, Hugo, Adrien Carreira, raphael g, and Christophe Rannou. "Anatomy of a Frontier Lab Agent Intrusion: A Technical Timeline of the July 2026 Incident." July 27, 2026. https://huggingface.co/blog/agent-intrusion-technical-timeline.
- Black Hat USA 2026: The 'Breaking' News: The OpenAI–Hugging Face Incident

15. Counterintelligence and Cyber Threat Intelligence (Dec 1 & 3)

Guest Lecturer: Cristiana Brafman-Kittner, Senior Manager of Threat Research Engineering at Proofpoint

Having established how actors can use different means of subversion to achieve various ends, this session focuses on how to defend against it. We will look at intelligence literature as well as historical and contemporary cases to identify effective counterstrategies to subversive threats.
Literature

- Taylor, Stan A. "Definitions and Theories of Counterintelligence." In *Strategic Intelligence, Volume 4: Strategic Intelligence: Counterintelligence and Counterterrorism*, edited by Loch K. Johnson, 4:1–14. Intelligence and the Quest for Security. Westport, Conn: Praeger Security International, 2007.
- Eichensehr, Kristen E. "Public-Private Cybersecurity." *Tex. L. Rev.* 95 (2016), pp. 467-500

****

- Work, JD. "Evaluating Commercial Cyber Intelligence Activity." *International Journal of Intelligence and CounterIntelligence* 33, no. 2 (2020): 278–308. https://doi.org/10.1080/08850607.2019.1690877.
- Bouwman, Xander, Harm Griffioen, Jelle Egbers, Christian Doerr, Bram Klievink, and Michel van Eeten. "A Different Cup of TI? The Added Value of Commercial Threat Intelligence." 2020, 433–50. https://www.usenix.org/conference/usenixsecurity20/presentation/bouwman.

16. US Cyber Strategy (Dec 8)

In this final session we will examine how United States Cyber Strategy has evolved over the years, how to evaluate its effectiveness, and what that tells us about cyber operations as an instrument of power.

- US DoD, "Summary Department of Defense Cyber Strategy 2018", 2018.
- Lindsay, Jon R. "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem." *Intelligence and National Security* 36, no. 2 (2021): 260–78. https://doi.org/10.1080/02684527.2020.1840746.
- Pomerleau, Mark. "With a Replacement Named, a Look Back at US Cyber Command's Transformational Years under Gen. Nakasone." *DefenseScoop*, May 23, 2023. https://defensescoop.com/2023/05/23/with-a-replacement-named-a-look-back-at-us-cyber-commands-transformational-years-under-gen-nakasone/.
- Lyu, Jinghua. "A Chinese Perspective on the Pentagon's Cyber Strategy: From 'Active Cyber Defense' to 'Defending Forward.'" *Lawfare* (blog), October 19, 2018. https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward.

Course Objectives

Upon completion of the course, students will:

1) Have a thorough understanding of what subversion is and how it works
2) Know what cyber operations have in common with subversion
3) Understand the limitations of subversion under different circumstances
4) Be able to distinguish feasible from possible outcomes in subversive conflict and cyber conflict
5) Be able to distinguish subversive operations from other grey zone means of aggression
6) Have a basic grasp of the history of subversion

7) Have a systematic understanding of how new technologies impact subversion
8) Be able to make empirically-grounded threat assessments for different subversive operations
9) Understand the policy and strategic challenges involved in both running subversive operations and responding to them

Grading Criteria

A: Exceptionally good performance demonstrating a superior understanding of the subject matter, a foundation of extensive knowledge, and a skillful use of concepts and/or materials.

B: Good performance demonstrating capacity to use the appropriate concepts, a good understanding of the subject matter, and an ability to handle the problems and materials encountered in the subject.

C: Adequate performance demonstrating an adequate understanding of the subject matter, an ability to handle relatively simple problems, and adequate preparation for moving on to more advanced work in the field.

Other grades awarded include:

D: Minimally acceptable performance demonstrating at least partial familiarity with the subject matter and some capacity to deal with relatively simple problems, but also demonstrating deficiencies serious enough to make it inadvisable to proceed further in the field without additional work.

F: Failed. Has not demonstrated familiarity with the subject matter, nor the capacity to deal with simple problems in a manner recognizable to the consensus of mainstream academic practitioners within the field.

Conduct

Students will treat each other and the professor with respect. Constructive questioning and criticism are welcome and encouraged. Personal attacks and insults are not. The rule of thumb here is that critical comments and questions should be maturely phrased in a manner that encourages constructive and open debate. They should not be phrased as insults, threats, or in a manner that shuts down conversation or debate. Put another way, you can attack a hypothesis, theory, data, or method of analysis all you like; but do *not* attack the speaker either directly or by implication.

Students are expected to read and abide by the Georgia Tech Student Codes of Conduct and the Academic Honor Code. All violations will be reported. The complete text of these Codes may be found at:

http://www.policylibrary.gatech.edu/student-life/academic-misconduct
http://www.policylibrary.gatech.edu/student-life/student-code-conduct
http://www.policylibrary.gatech.edu/student-affairs/academic-honor-code

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. 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/.
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.