Cyber Security Policy (PPPE / PSCI 6303.501)

Instructor: Anton Sobolev

Fall 2021

E-mail: anton.sobolev@utdallas.edu
Office Hours: TBD
Office: GR 3.108

Web: bit.ly/2XClYAz
Class Hours: T 7:00pm-9:45pm
Class Room: FO 1.502

Course Description

This course introduces students to the public policy aspects of cybersecurity. Students apply various game-theoretic, statistical, and causal inference frameworks to provide structure to policy-making. It is divided into four parts. The first involves basic concepts and definitions regarding policy, governance, and threats; the second exposes students to the modern policy analysis toolkit; the third deals with cyber policies for the private sector; the fourth focuses on the state. Topics include cyber piracy, Dark Net markets, data breaches, deplatforming, electoral integrity, misinformation, digital repression, and others.

Learning Objectives

There are three learning objectives for this course:

- Understand the political and economic contexts of cybersecurity. While the cybersecurity has some unique characteristics, it is more tractable when considered in the broader context of international relations, history, and political economy.
- Learn how to discern when a research design has likely identified a causal effect from a simple association between two observable trends. Understanding what a causal effect is, when they can be identified, and when a researcher's causal claim is not justified, is one of the most important skills of a cyber policy analyst.
- Learn how to analyze and empirically assess the negative impact of cyber threats and the effects of existing and proposed cybersecurity policies and regulations. While the importance of fighting cyber threats has been widely recognized by the public, experts, and state officials, a lot of current policies are not based on the rigorous causal evidence. Both the public and private sectors exhibit high demand for specialists with these skills.

These learning objectives will be assessed through class discussion, individual and group assignments and presentations.

Course Modality and Expectations

Instructional Mode

The class will meet at our scheduled time in FO 1.502. International students who are outside the U.S. will be able to attend in this class remotely (via MS Teams). Students who test positive for COVID-19 or who are required to isolate or quarantine will be able to participate in the class remotely

Updates

Keep checking the class website regularly. Please bear in mind that this is a new course, so I reserve the right to make mid-course corrections. I also welcome feedback.

Prerequisites

In addition to a confident level of computer and Internet literacy, certain minimum technical requirements must be met to enable a successful learning experience. Please review the important technical requirements on the Getting Started with eLearning webpage.

The course does not require prior programming skills.

Course Requirements

You are expected to attend every class and to be prepared to discuss all the assigned reading. If you find you cannot attend, please notify your instructor in advance.

Course Access and Materials

This course can be accessed using your UT Dallas NetID account on the eLearning website.

Due to the dynamic nature of our subject matter, no single book exists that meets all course requirements. Readings for each class are listed in the course schedule. All required readings are available via the class website or UTD library.

Recommended readings

- Valeriano, Brandon, et al., *Cyber Strategy: The Evolving Character of Power and Coercion* (2018)
- Buchanan, Ben, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (2016)
- Angrist, Joshua, and Jorn-Steffen Pischke, *Mastering Metrics* (2013)
- Glennerster, Rachel, and Kudzai Takavarasha, *Running Randomized Evaluations: A Practical Guide* (2013)
- Gertler, Paul et al., *Impact Evaluation in Practice* (2011)

Course Assignments and Grading

Your grade will be comprised of seven components: participation, one problem set, two individual reports, one group reports, one group presentation, and peer assessment. The breakdown of each component of your overall grade is as follows:

Component	%
Problem Set	20
Country Cyber Threats Assessment	10
Cyber Threat: Causal Inference Design	20
Group Final Project	20
Group Presentations	10
Peer Assessments	10
Participation	10

Extra Credit	
DataCamp Assignment	5
Problem Set 0	5

Problem Set (20%)

Working on actual problems is central to learning. One mandatory and one optional problem sets will be assigned. These assignments will consist of analysis of cybersecurity problems using game theory and statistical tools (in R). Late submissions will not be accepted without prior permission. Students are encouraged to discuss the problems together, but must independently produce and submit solutions.

No prior knowledge of R is required. Students will acquire necessary skills during the first part of this course.

Country Cyber Threats Assessment (10%)

You will write a short briefing paper on the cyber threats facing a particular nation (2 pages). The analysis will need to take into account available data on the frequency and the potential costs of cyber attacks of different types, their main targets, and the nation's dependence on cyber, and the level of sophistication of its cyber defense. You will need to rank these threats and justify your ranking. You will also need to formulate feasible policies to address top-3 issues on your list.

Cyber Threat: Causal Inference Design (20%)

You will formulate a research design to study the effect of a cyber policy with the following steps (up to 5 pages). Pick one of the existing cyber threats. Explain how to assess its negative impact on important economic, social, or political outcomes. Describe available data that can be used for this assessment. Describe potential biases in data that can undermine the credibility of this assessment. Formulate a policy to mitigate this cyber threat. Come up with an ideal experiment to test to the performance of your policy. Explain factors that can make your ideal experiment unfeasible or can stop a policy-maker from running it.

Group Final Project: Policy Design and Simulation (20%)

Students will be divided into groups. The group project follows the idea of the previous task with a few extra elements. First, the students will need to review existing studies on a selected cyber threat. Second, they will not only describe the negative impact of the cyber threat but empirically assess it using either real or simulated data (provided by the instructor). In addition to the ideal

experiment, group will formulate feasible non-experimental design and test the performance of the proposed policy with simulated data. The required length of the final report will be 8-10 pages.

Peer Assessments (10%)

Near the end of the semester you will fill out a peer evaluation form to assess how each group member contributed to the group project. To help ensure that all members of the team are actively contributing, you will be asked to evaluate your teammates' contributions, effort, and performance. Students will receive anonymous evaluations from your group. It will help you know how well you are doing and identify areas in need of improvement. Students will also complete a midterm self-evaluation of your own performance. It will help you reflect on your own effort in this class. Your highest and lowest peer-evaluation scores will be dropped.

Group Presentations (10%)

Groups will present intermediate results of their projects in class. The audience will provide a feedback. Groups will be able to update their report before the final submission.

Participation (10%)

You are expected to attend every class and to be prepared to discuss all the assigned reading. Participation will consist of regularly contributing to class discussion and drawing from readings and integrating lessons from earlier meetings.

A Note on Academic Integrity

Please visit the university's Writing Center website on using sources and revisit the university's Academic Integrity Policy. The University takes plagiarism infractions seriously, and penalties for students caught plagiarizing include suspension, lowered or failing grades, and possible expulsion. In general, if you have any questions, please feel free to ask your instructor.

Diversity and Inclusion

This course should serve the needs of students from all backgrounds and perspectives. Students with disabilities enrolled in this course who may need disability-related classroom accommodations are encouraged to make an appointment to see the instructor before the end of the second week of the quarter. All conversations will remain confidential. Please also arrange to have the required documentation sent to `anton.sobolev@utdallas.edu` for any accommodations at your earliest convenience.

Technology in The Classroom

No smart phones may be used in class. Class discussions may not be recorded.

You will frequently make use of computers in this course during lecture periods and discussion sections. Please be respectful to your instructor and your peers by using your computers only for class-related purposes. Please put your phone away before class starts and don't bring it out.

Development of this course

Learning should not happen in a vacuum. To help ensure the best chance for success for the students of this course, this course draws on the format, syllabus, and materials from similar successful courses at peer institutions.

Academic Calendar

Part 1. Introduction and Theoretical Perspective

Week 01, 08/23 - 08/27: Class Logistics and Introduction

No required readings

Week 02, 08/30 - 09/03: Social Science Framework for Cyber Policy: From Physical Security to Cyber Security

Read *all* associated documents on the course website:

- Olson, Mancur, "Why the Transition from Communism is so Difficult," *Eastern Economic Journal* (1995): 437-461. *Do not be afraid of the title! This paper outlines important theoretical background for understanding security.*
- Tilly, Charles, "State Making as Organized Crime," in *Bringing the State Back In* (1985): 169-91
- Buchanan, Ben, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (2016): ch. 1,8
- Valeriano, Brandon, et al., *Cyber Strategy: The Evolving Character of Power and Coercion* (2018): ch. 1

Part 2. Policy-Analysis Toolkit for Cybersecurity

Week 03, 09/06 - 09/10: Game-Theoretic Approach to Cyber Policy

- Jajodia, Sushil, et al., *Cyber Warfare: Building the Scientific Foundation* (2015): ch. 1,5
- Do, Cuong, et al., "Game Theory for Cyber Security and Privacy," *ACM Computing Surveys (CSUR)* (2017): 1-37

Week 04, 09/13 - 09/17: Statistical Modeling for Policy-Analysis

DataCamp Assignment due

- Wheelan, Charles, *Naked Statistics: Stripping the Dread from the Data* (2013): ch. 4,8
- Angrist, Joshua, and Jorn-Steffen Pischke, *Mastering Metrics* (2013): ch. 2
- Sykes, Alan, *An Introduction to Regression Analysis* (1993)

Week 05, 09/20 - 09/24: Machine-Learning for Policy-Analysis

Problem Set 0 due

- Taulli, Tom, *Artificial Intelligence Basics: A Non-Technical Introduction* (2019): ch. 4
- Benoit, Kenneth, "Text as Data: An Overview," in *Handbook of Research Methods in Political Science and International Relations* (2019): 461-97
- Alammar, Jay, "A Visual and Interactive Guide to the Basics of Neural Networks," (2018): Link

Week 06, 09/27 - 10/01: Causal Inference for Policy-Analysis

Country Cyber Threats Assessment due

- Pearl, Judea, and Dana Mackenzie, *The Book of Why: The New Science of Cause and Effect* (2018): ch.1
- Gerber, Alan, and Donald Green, *Field Experiments: Design, Analysis, and Interpretation* (2012): ch. 1,2
- Angrist, Joshua, and Jorn-Steffen Pischke, *Mastering Metrics* (2013): ch. 3,5

Part 3. Cyber Policy and the Private Sector

Week 07, 10/04 - 10/08: Cyber Piracy

- Adermon, Adrian, and Che-Yuan Liang, "Piracy and Music Sales: The Effects of an Anti-Piracy Law," *Journal of Economic Behavior & Organization* (2014): 90-106
- Danaher, Brett, et al., "Piracy and copyright enforcement mechanisms," *Innovation Policy and the Economy* (2014): 25-61
- Angrist, Joshua, and Jorn-Steffen Pischke, *Mastering Metrics* (2013): ch. 3,5
- *The Economic Impacts of Counterfeiting and Piracy* (2020)
- Fernandez, Rodrigo, et al., "Effects of Software Piracy on Economic Growth," *International Journal of Economics and Finance* (2018): 1-11

Week 08, 10/11 - 10/15: Dark Net Markets

Problem Set 1 due

- Decary-Hetu, David, and Luca Giommoni, "Do Police Crackdowns Disrupt drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous," *Crime, Law and Social Change* (2017): 55-75
- *Malware Trends on 'Darknet' Crypto-Markets: Research Review* (2018)
- Chan, Jason, and Anindya Ghose, "Internet's Dirty Secret: Assessing the Impact of Online Intermediaries on the Outbreak of Sexually Transmitted Diseases" (2012)
- Chan, Jason, et al. "Shedding Light on the Dark: The Impact of Legal Enforcement on Darknet Transactions" (2019)

Week 09, 10/18 - 10/22: Attacks Against Businesses

- Makridis, Christos, and Benjamin Dean, "Measuring the Economic Effects of Data Breaches on Firm Outcomes: Challenges and Opportunities," *Journal of Economic and Social Measurement* (2018): 59-83
- Romanosky, Sasha, "Examining the Costs and Causes of Cyber Incidents," *Journal of Cybersecurity* (2016): 121-135
- Rosati, Pierangelo, et al., "Audit Firm Assessments of Cyber-Security Risk: Evidence from Audit Fees and SEC Comment Letters," *The International Journal of Accounting* (2019): 1950013

- Tosun, Onur, "Cyber-Attacks and Stock Market Activity," *International Review of Financial Analysis* (2021): 101795.

Week 10, 10/25 - 10/29: Cyber Policies of Digital Platforms

- Wilson, Tom, and Kate Starbird, "Cross-Platform Information Operations: Mobilizing Narratives and Building Resilience Through Both 'Big' and 'Alt' Tech ," *PACM on Human-Computer Interaction* (2021): 345
- Mitts, Tamar, "Banned: How Deplatforming Extremists Mobilizes Hate in the Dark Corners of the Internet" (2021)
- Muller, Karsten, and Carlo Schwarz, "Fanning the Flames of Hate: Social Media and Hate Crime," *Journal of the European Economic Association* (2021): 2131-2167
- Bursztyn, Leonardo, et al, "Social Media and Xenophobia: Evidence from Russia," *National Bureau of Economic Research* (2019)

Part 3. Cyber Policy and the State

Week 11, 11/01 - 11/05: Attacks Against the State

Cyber Threat: Causal Inference Design due

- Valeriano, Brandon, et al., *Cyber Strategy: The Evolving Character of Power and Coercion* (2018): ch. 3,4
- Kostyuk, Nadiya, and Yuri Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* (2019): 317-347
- Henschke, Adam, et al., "Countering Foreign Interference: Election Integrity Lessons for Liberal Democracies" *Journal of Cyber Policy* (2020): 180-198
- Kumar, Sumeet, et al., "The Impact of US Cyber Policies on Cyber-Attacks Trend" *JIEEE Conference on Intelligence and Security Informatics* (2016)

Week 12, 11/08 - 11/12: Misinformation

- Bago, Bence et al., "Fake News, Fast and Slow: Deliberation Reduces Belief in False (but not true) news headlines," *Journal of Experimental Psychology* (2020): 1608-1613
- Bovet, Alexandre, and Hernan Makse, "Influence of Fake News in Twitter During the 2016 US Presidential Election," *Nature: Communications* (2019): 1-14
- Nyhan, Brendan, and Jason Reifler, "Displacing Misinformation about Events: An Experimental Test of Causal Corrections," *Journal of Experimental Political Science* (2015): 81-93
- Pennycook, Gordon, et al., "Shifting Attention to Accuracy Can Reduce Misinformation Online," *Nature* (2021): 590-595

Week 13, 11/15 - 11/19: Authoritarian Cyber Policy

- Frantz, Erika, et al., "Digital Repression in Autocracies," *V-Dem* (Mar 2020) Link
- Pan, Jennifer, and Tongtong Zhang, "How Companies Perpetuate and Resist Chinese Government Censorship" (2020)

- Sobolev, Anton, "How Pro-Government "Trolls" Influence Online Conversations in Russia" (2021)
- Pan, Jennifer, and Alexandra Siegel, "How Saudi crackdowns fail to silence online dissent," *American Political Science Review* (2020): 109-125

Week 14, 11/22 - 11/26: Fall Break: No Classes

Week 15, 11/29 - 12/03: Group Project Presentations #1

Week 16, 12/06 - 12/10: Group Project Presentations #2

Group Final Project due December 10

Classroom Safety and COVID-19

To help preserve the University's in-person learning environment, UT Dallas recommends the following:

Adhere to the University's CDC Updated Guidelines issued on July 30, 2021. All Comets are strongly encouraged to wear face coverings indoors regardless of vaccination status. Please note this represents a change in the campus guidance issued on May 20, 2021.

Accommodations for Students Who Must Isolate or Quarantine Due to COVID-19

Students who test positive for COVID-19 or who are required to isolate or quarantine will be able to participate in the class remotely. Records of the seminar meetings will be available for those students during the period the students must isolate or quarantine. Students should not attend class in person until cleared by campus tracers. Visit Comets United webpage to obtain the latest information on the University's guidance and resources for campus health and safety.

Communication

This course utilizes online tools for interaction and communication. Some external communication tools such as regular email and a web conferencing tool may also be used during the semester. For more details, please visit the Student eLearning Tutorials webpage for video demonstrations on eLearning tools.

Student emails and discussion board messages will be answered within 3 working days under normal circumstances.

Distance Learning Student Resources

Online students have access to resources including the McDermott Library, Academic Advising, The Office of Student AccessAbility, and many others. Please see the eLearning Current Students webpage for more information.

Server Unavailability or Other Technical Difficulties

The University is committed to providing a reliable learning management system to all users. However, in the event of any unexpected server outage or any unusual technical difficulty which prevents students from completing a time sensitive assessment activity, the instructor will provide

an appropriate accommodation based on the situation. Students should immediately report any problems to the instructor and also contact the online eLearning Help Desk. The instructor and the eLearning Help Desk will work with the student to resolve any issues at the earliest possible time.

Class Materials

The Instructor may provide class materials that will be made available to all students registered for this class as they are intended to supplement the classroom experience. These materials may be downloaded during the course, however, these materials are for registered students' use only. Classroom materials may not be reproduced or shared with those not in class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Classroom Conduct Requirements Related to Public Health Measures

UT Dallas will follow the public health and safety guidelines put forth by the Centers for Disease Control and Prevention (CDC), the Texas Department of State Health Services (DSHS), and local public health agencies that are in effect at that time during the Fall 2021 semester to the extent allowed by state governance. Texas Governor Greg Abbott's Executive Order GA-38 prohibits us from mandating vaccines and face coverings for UT Dallas employees, students, and members of the public on campus. However, we strongly encourage all Comets to get vaccinated and wear face coverings as recommended by the CDC. Check the Comets United: Latest Updates webpage for the latest guidance on the University's public health measures. Comets are expected to carry out Student Safety protocols in adherence to the Comet Commitment. Unvaccinated Comets will be expected to complete the Required Daily Health Screening. Those students who do not comply will be referred to the Office of Community Standards and Conduct for disciplinary action under the Student Code of Conduct – UTSP5003.

Class Participation

Regular class participation is expected. Students who fail to participate in class regularly are inviting scholastic difficulty. A portion of the grade for this course is directly tied to your participation in this class. It also includes engaging in group or other activities during class that solicit your feedback on homework assignments, readings, or materials covered in the lectures (and/or labs). Class participation is documented by faculty. Successful participation is defined as consistently adhering to University requirements, as presented in this syllabus. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Class Recordings

Students are expected to follow appropriate University policies and maintain the security of passwords used to access recorded lectures. Unless the Office of Student AccessAbility has approved the student to record the instruction, students are expressly prohibited from recording any part of this course. Recordings may not be published, reproduced, or shared with those not in the class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

The instructor may record meetings of this course. These recordings will be made available to all students registered for this class if the intent is to supplement the classroom experience. If the instructor or a UTD school/department/office plans any other uses for the recordings, consent of the students identifiable in the recordings is required prior to such use unless an exception is allowed by law.

Comet Creed

This creed was voted on by the UT Dallas student body in 2014. It is a standard that Comets choose to live by and encourage others to do the same: *"As a Comet, I pledge honesty, integrity, and service in all that I do."*

Academic Support Resources

The information contained in the following link lists the University's academic support resources for all students. Please go to Academic Support Resources webpage for these policies.

UT Dallas Syllabus Policies and Procedures The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus. Please review the catalog sections regarding the credit/no credit or pass/fail grading option and withdrawal from class.

Please go to UT Dallas Syllabus Policies webpage for these policies.

The descriptions and timelines contained in this syllabus are subject to change at the discretion of the Professor.