**PPHA 33820 Democracy Hacked: Cyber Threats to Modern Governments in the Digital Age**

**Instructors: Noah Praetz, Jake Braun**

**Winter Quarter 2026**

**Th | 5:00pm-7:50pm**

***Introduction:***

A secure election, supported by voters' confidence that every vote will be counted as cast, forms the bedrock of our democracy. However, as evidenced for the past decade, U.S. trust in voting systems has become a serious national security concern. Given cyber interference by foreign adversaries, the matter of "securing the vote" – something that was once almost exclusively the responsibility of state and local officials – has now become a priority of our nation's top cybersecurity, homeland security, military, law enforcement, and intelligence leaders. And the United States is not alone in its vulnerabilities: As more governments do business online, there are more opportunities for states' adversaries to usurp democratic power from citizens.

As we look forward to future elections, we must expect potentially devastating attacks on our voting systems. They are irresistible targets for attackers to attempt to manipulate in order to undermine confidence in our democracy. In addition to Russia, many other groups, including North Korea, Iran, ISIS, China, and large foreign and domestic crime rings, have the resources to successfully attack our current voting systems. In fact, when asked whether Russia would attempt to attack future U.S. elections, as it did in 2016, Robert Mueller replied in his testimony before the House Judiciary Committee that "they're doing it as we sit here." We urgently need to secure our election systems from attack.

***Course Description:***

This course is designed to offer students an overview of the current cybersecurity landscape and the implications for protecting and promoting democracy. Students will hear first-hand insider perspectives from public and private sector cyber professionals and international experts on democratic engagement and protection of civil liberties. Students will gain insight on cybersecurity technology, threats to democratic institutions, and ways to combat cyber predators.

***Instructor Contact and Office Hours:***

Noah Praetz - noah.praetz@gmail.com – Office hours by appointment

Jake Braun - jakebraun@gmail.com

***TA's*:**

Wyatt Hartwig - whartwig@uchicago.edu - Office hours by appointment

Nixi Huang - nixihuang@uchicago.edu - Office hours by appointment

***Class Structure:***

This class will take place synchronously. There will be assignments posted to Canvas.

***Grading/Assignments:***

- Participation (33%)
    - Students are expected to actively participate in the course discussions in two ways:
        - Each week, students will be required to submit 2-3 questions for the speaker based on readings and other course content.
        - A set of discussion questions based on the week's material will be posted to a discussion board on Canvas every Monday/ Students should select one of the discussion questions and post a response (100 word minimum) based on readings and speaker presentations. Students may include information from outside research as well. Students should then respond to at least one other student's post with a meaningful comment or question.
- Policy Brief (33% - 16.5% per brief)
    - Each student will submit two policy briefs that provide a summary and analysis of a current issue in cybersecurity. Students will select from

instructor-provided prompts for these briefs. All briefs should be one page, single spaced, 12-point font, 1-inch margins.

- Final Research Project (34%)
    - The final project will be a comprehensive report on a topic related to election security. For the project, students will draw on knowledge gained from the topics covered during the quarter and through their own research. All papers should be five pages, single spaced, 12-point font, 1-inch margins.

***Attendance Policy**:*

- Students are expected to attend every class in-person. If there are circumstances that arise that prohibit a student from attending class, please email the Teaching Assistants.
- Missing more than one class without consent of the instructor will result in a one-level grade penalty.
    - For example, if a student receives an A in the course but misses two classes without consent of the instructor, their grade will be dropped to an A-. If they miss three classes without consent of the instructor, their grade will be dropped to a B+, etc.

***Teaching and learning in person, dual-modality, and/or remote environments:***

All students are expected to attend each class in person. Lectures will not be provided virtually and will not be recorded.

***General Resources Available to Students:***

- Harris Academic Support Programs and Handbook
- Student Wellness
- University Learning Resources

***Harris School and University of Chicago Policies:***

- Harris School Policies
- University General Policies
- University Academic Polices

- Policies on audio and video recordings and deletion.

***Academic Integrity:***

All University of Chicago students are expected to uphold the highest standards of academic integrity and honesty. Among other things, this means that students shall not represent another's work as their own, use un-allowed materials during exams, or otherwise gain unfair academic advantage. All students suspected of academic dishonesty will be reported to the Harris Dean of Students for investigation and adjudication. The disciplinary process can result in sanctions up to and including suspension or expulsion from the University. I, Congressman Quigley, will impose a grade penalty of 0 for students who have committed academic dishonesty. The Harris School of Public Policy and the University of Chicago policies that outline these expectations are linked above.

***Artificial Intelligence (AI) Usage:***

Course Policy:

- AI cannot be used to compose any content for submittable assignments.
    - AI can be used to conduct research for course assignments, but the information taken from an AI source must be properly cited.

- Responsible Use of AI:
    - Students take full responsibility for the accuracy of AI-generated content.
    - Students should review and edit any generated content to avoid inaccuracies, biased outputs, or misinterpretations. Over reliance on AI content, without proper attribution, may lead to unintentional plagiarism, as LLM models have been accused of plagiarism. Students must exercise caution to ensure their contributions are appropriately credited.
    - Over reliance on LLM models may limit students' accumulation of skills and understanding of the material, so it is advised that students conduct their own research before using AI.

***Required Reading:***

Students must acquire access to the two books listed below. Other readings will come from online publications or publicly available resources.

*Democracy in Danger* - Jake Braun

*The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* - David Sanger

Note: The paperback edition has an extra chapter. You may use any edition for class.

*For required weekly readings please see the modules page. Some readings may require you to login with an institutional ID, this will be your UChicago login information. If you have difficulty opening a reading or encounter a deadlink please email both whartwig@uchciago.edu and nixihuang@uchicago.edu

***Suggested Reading:***

*The Cuckoo's Egg* - Cliff Stoll

*Lifting The Fog Of War* - Admiral Bill Owens

*Neuromancer* - William Gibson

*Snow Crash* - Neal Stephenson