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

Instructors: Jake Braun and Noah Praetz

Winter Quarter 2024

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 since the 2016 election, 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:

Jake Braun - jakebraun@gmail.com- Office hours by appointment
Noah Praetz - noah.praetz@gmail.com – Office hours on Thursday 3-5 pm.

TA's:
Alex Littell - alittel0@chicagobooth.edu - Office hours by appointment
Camelia Valldejuly - cameliav@uchicago.edu - Office hours on …

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.

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 honest. 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.

Suggested Reading:
The Cuckoo's Egg - Cliff Stoll
Lifting The Fog Of War - Admiral Bill Owens
Neuromancer - William Gibson
Snow Crash - Neal Stephenson

Course Schedule and Readings:
Note: Some readings may be subject to change. Updated information will be posted to Canvas.

Week 1:
Topic: Democracy and Cybersecurity: The Scale of the Problem

- Review syllabus and final project
- Defining "cybersecurity" from the technical and policy perspectives
- 2020 presidential election and confidence in results
- Current cybersecurity policies

Readings:
U.S. Department of Homeland Security Cybersecurity Strategy
https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

National Cyber Strategy of the United States of America
2018 -
https://digital.library.unt.edu/ark:/67531/metadc1259394/m1/1/ or
2023 - https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/latest-activities/national-cyber#:~:text=National%20Cyber%20Strategy.%20In%20September%202018%2C%20the%20White,priority%20action%20on%20developing%20a%20superior%20cybersecurity%20workforce.

A Civil Perspective on Cybersecurity
By Jane Holl Lute and Bruce McCall
http://www.wired.com/2011/02/dhs-op-ed/

Working to Preserve the Stability of Cyberspace
By Paul Nicholas
https://thediplomat.com/2017/09/working-to-preserve-the-stability-of-cyberspace/

Week 2:
Topic: The Basics of Cybersecurity: The Top 20 Critical Security Controls

Speaker*:* Tony Sager, Former Chief Operating Officer of National Security Agency (NSA) Information Assurance Directorate; Currently, Senior Vice President at Center for Internet Security (CIS), where he leads the development of the CIS Critical Security Controls.

Readings:
CIS Controls v8
https://www.sans.org/blog/cis-controls-v8/

The Executive's Guide to the CIS Controls
https://static.fortra.com/tripwire/pdfs/guides/tw-executives-guide-to-the-top-20-csc-gd.pdf

Overview of above via Infosec
https://resources.infosecinstitute.com/the-center-for-internet-security-cis-top-20-critical-security-controls/#gref

OWASP Top Ten
https://owasp.org/www-project-top-ten/

The Perfect Weapon by David Sanger - Preface, Prologue, Chapters 1 & 2

Note: *Democracy in Danger* must be finished by next week. You may want to start reading it this week.

Week 3:
Topic: Current State of "Security and Confidence" in the US Voting System

Speaker*:* Matt Masterson, former Senior Cybersecurity Advisor and election security lead for the Cybersecurity and Infrastructure Security Agency (CISA) and now Director of Information Integrity and democracy program lead at Microsoft.

Readings:
Election-Hacking Lessons From the 2018 DEF CON Hackers Conference
By Sue Halpern
https://www.newyorker.com/news/dispatch/election-hacking-lessons-from-the-2018-def-con-hackers-conference

Democracy in Danger by Jake Braun

States and localities are on the front lines of fighting cyber-crimes in elections
https://www.brookings.edu/blog/fixgov/2019/08/15/states-and-localities-are-on-the-front-lines-of-election-security/

National Academies report
https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

The Perfect Weapon by David Sanger - Chapters 3-4

BRIEF DUE NEXT WEEK

Week 4:
Topic: The Promise & Peril of New Technologies

Speaker: Luukas Ilves, Former Counselor for Digital Affairs for Estonia's Permanent Representation to the European Union

Readings:

Luukas Ilves on the Digital Priorities for the Estonian Presidency
Video
https://www.euractiv.com/section/digital/video/luukas-ilves-counsellor-for-digital-affairs-permanent-representation-of-estonia-to-the-eu-on-the-digital-priorities-for-the-estonian-presidency/

e-Residency 2.0 White Paper
https://s3.eu-central-1.amazonaws.com/ereswhitepaper/e-Residency+2.0+white+paper+English.pdf

Budapest Convention on Cybercrime
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

Email and Internet Voting: The Overlooked Threat to Election Security
https://www.commoncause.org/page/email-and-internet-voting-the-overlooked-threat-to-election-security/

The Democratic Party deepfaked its own chairman to highlight 2020 concerns by Donie O'Sullivan
https://us.cnn.com/2019/08/09/tech/deepfake-tom-perez-dnc-defcon/index.html

(Optional) *Tech Expert Ben Buchanan on the Links Between Artificial Intelligence and National Security* - Intelligence Matters podcast:
https://www.google.com/url?q=https://pandora.app.link/DeWDHD5tDFb&sa=D&source=docs&ust=1703047111074970&usg=AOvVaw2cE8lhC5iiXLoOS4h5s_n5

The Perfect Weapon by David Sanger - Chapters 5-6

POLICY BRIEF DUE TODAY - UPLOAD TO CANVAS BY 11:59 PM CT

Week 5:
Topic: Improving Election Security for at the local level

Speaker: TBD or Noah Praetz

Readings:
2020 Vision: Election Security in the Age of Committed Foreign Threats
By Noah Praetz
https://www.electioncenter.org/white-paper-2020-vision-election-security-in-the-age-of-committed-foreign-threats.html

Election security in 2020 means a focus on county officials, DHS says
https://www.cnet.com/news/election-security-in-2020-means-a-focus-on-county-officials-dhs/

A Voter's Guide to Election Security
https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/11/01/a-voters-guide-to-election-security

3 years after Russian hackers tapped Illinois voter database, officials spending millions to safeguard 2020 election
https://www.chicagotribune.com/politics/ct-illinois-election-security-russian-hackers-20190805-qtoku33szjdrhknwc7pxbu6pvq-story.html

The Unsexy Threat to Election Security
https://krebsonsecurity.com/2019/07/the-unsexy-threat-to-election-security/

The Perfect Weapon by David Sanger - Chapters 7-8

BRIEF DUE NEXT WEEK

Week 6:
Topic: Technical Vulnerabilities in the US Election System

Speaker: Sherri Ramsay, Former Director of National Security Agency (NSA) / Central Security Service Threat Operations Center (NTOC) where she led discovery and characterization of threats to national security systems, providing situational awareness of those threats, and coordinating actionable information to counter those threats.

Readings:

DEF CON 25 Voting Machine Hacking Village Report
By Matt Blaze, Jake Braun, Harri Hursti, Joseph Lorenzo Hall, Margaret MacAlpine, and Jeff Moss
https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf?data1=v1

DEFCON 26 Voting Machine Village Hacking Report
By Matt Blaze, Jake Braun, Harri Hursti, Margaret MacAlpine, and Jeff Moss
https://harris.uchicago.edu/files/cpi_-_def_con_26_voting_village_report_-_final_4.pdf

DEFCON 27 Voting Machine Village Hacking Report
By Matt Blaze,Harri Hursti, Margaret MacAlpine, Mary Hanley, and Jeff Moss
https://harris.uchicago.edu/files/def_con_27_voting_village_report.pdf

Voting System Security and Reliability Risks
Brennan Center for Justice
https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf

Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials
https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

The scramble to secure America's voting machines
https://www.politico.com/interactives/2019/election-security-americas-voting-machines/.
https://edition.cnn.com/2023/09/20/politics/voting-machines-cybersecurity-2024/index.html

The Perfect Weapon by David Sanger - Chapters 9-10

POLICY BRIEF DUE TODAY - UPLOAD TO CANVAS BY 11:59 PM CT

Week 7:
Topic: Cyber Threats to Democracy: Russia and the Geopolitical Landscape

Speaker: Ambassador Douglas Lute, Former Ambassador to NATO; Former Assistant to the President and Deputy National Security Advisor for Iraq and Afghanistan; Former President Obama's Special Assistant and Senior Coordinator for Afghanistan and Pakistan.

Readings:

U.S. NATO Envoy Warns Of Russian 'Malign Influence' Ahead Of Talks
https://www.rferl.org/a/us-envoy-nato-russia-council-influence-cyberattacks/28183839.html

Everything We Know About Russia's Election-Hacking Playbook

By Andy Greenberg
https://www.wired.com/story/russia-election-hacking-playbook/

The US Gives Cyber Command the Status It Deserves
By Lily Hay Newman
https://www.wired.com/story/cyber-command-elevated/

US Senate, "Report on Russian Election Hacking"
https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

NYT's David Sanger on the Perils of Cyber Conflict - Intelligence Matters Podcast
https://www.stitcher.com/podcast/cbs-radio-news/intelligence-matters/e/60697185?autoplay=true

The Application of International Law in Cyberspace: State of Play
https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/

The Perfect Weapon by David Sanger - Chapters 11-12 & Afterword (& chapter 13 recommended if using paperback edition)

Week 8:
Topic: Elections 2016: What We Knew Then and What to Do About 2024

Speaker: General Francis X. Taylor, Former Under Secretary for Intelligence and Analysis at the U.S. Department of Homeland Security

Readings:
Cybersecurity Lessons From the 2016 Presidential Election
By Rick M. Robinson
https://securityintelligence.com/cybersecurity-lessons-from-the-2016-presidential-election/

Written testimony of NPPD Office of Cybersecurity and Communications Assistant Secretary Andy Ozment for a House Committee on Oversight and Government Reform, Subcommittee on Information Technology hearing titled "Cybersecurity: Ensuring the Integrity of the Ballot Box"
U.S. Department of Homeland Security
https://www.dhs.gov/news/2016/09/28/written-testimony-nppd-house-oversight-and-government-reform-subcommittee

We hired the author of 'Black Hawk Down' and an illustrator from 'Archer' to adapt the Mueller report so you'll actually read it
https://www.insider.com/mueller-report-rewritten-trump-russia-mark-bowden-archer-2019-7

2020 election security to face same vulnerabilities as in 2016
https://searchsecurity.techtarget.com/news/252468837/2020-election-security-to-face-same-vulnerabilities-as-in-2016

DHS warns about 2024's cyberthreats: https://www.washingtonpost.com/politics/2023/09/15/dhs-warns-about-2024s-cyberthreats/
(the DHS report has just one page on the 2023 election season: https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf)

Threat of AI (as Alex suggested):

Intelligence nominee warns generative AI poses threat to 2024 elections: https://www.politico.com/news/2023/07/20/intelligence-chief-nominee-warns-of-threats-from-ai-to-2024-elections-00107375

Deepfakes emerge as a top security threat ahead of the 2024 US election: https://www.csoonline.com/article/1251094/deepfakes-emerge-as-a-top-security-threat-ahead-of-the-2024-us-election.html

S.1540 - Election Security Act of 2019
https://www.congress.gov/bill/116th-congress/senate-bill/1540/text

FINAL DUE NEXT WEEK

Week 9:
Topic: A Hacker's View of Cyber Policy

Speaker*:* Harri Hursti, Data Security and Election Security Expert; Co-founder of Voting Village at DEF CON Hacking Conference.

Readings:
Voting Machine Hackers Have 5 Tips to Save the Next Election
By Carsten Schurmann and Jari Kickbusch
https://www.wired.com/story/voting-machine-hackers-5-tips/

To Fix Voting Machines, Hackers Tear Them Apart
By Lily Hay Newman
https://www.wired.com/story/voting-machine-hacks-defcon/

Political campaigns prep for battle with hackers
By Daniel Strauss and Scott Bland
http://www.politico.com/story/2017/09/19/hackers-political-campaigns-242863

Hackers were told to break into U.S. voting machines. They didn't have much trouble.
https://www.washingtonpost.com/business/2019/08/12/def-con-hackers-lawmakers-came-together-tackle-holes-election-security/

FINAL PAPER DUE TODAY - UPLOAD TO CANVAS BY 11:59 PM CT