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

Instructor: Jake Braun

Fall Quarter 2018: Mondays 5:00 – 7:50 PM, Harris School

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 in the 2016 election, U.S. voting systems have become a serious national security concern. Given the recent cyber interference by a foreign adversary, 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.

Americans may be under the false impression that an attack on our vote counting systems would be detected because of reassurances by U.S. government agencies that they were not compromised in 2016, but this optimistic assessment is not based on actual examination of those systems. 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.

While we may have dodged a bullet in 2016, we must expect future, potentially devastating attacks on our voting systems. They are irresistible targets for attackers to attempt to manipulate in order to "elect" the leaders of their choice. 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 the words of former FBI director James Comey: "[t]hey're coming after America" and "they'll be back." 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.

Class Structure:

Each class will begin with a discussion of the week's readings. Students should expect to come to class prepared to discuss and ask questions about the assigned readings. Additionally, each week students will research and come prepared to discuss an issue related to election security.

Projects/Exams

- Response and Analysis Briefs (2)
    - Each student will submit a one-page policy brief that provides a summary and analysis of the information gleaned from assigned readings. These papers will be submitted (electronic and hard copy versions) on the following dates:
    - Brief #1: October 29
    - Brief #2: November 19
- Final Research Project
    - 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. The paper should be five pages long and should be submitted by December 10 (electronically).

Week 1: October 1

Topic: Democracy and Cybersecurity: The Scale of the Problem

- Review syllabus and final project
- Defining "cybersecurity" from the technical and policy perspectives
- Current cybersecurity policies
- Elections 2016: What happened?

Week 2: October 8

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

Speaker*:* Tony Sager, Senior Vice President & Chief Evangelist, Center for Internet Security; former Chief Operating Officer of the National Security Agency Information Assurance Directorate

Readings:

Top 20 Critical Security Controls
http://www.sans.org/critical-security-controls/control/3

Top 4 Critical Security Controls
http://www.tripwire.com/state-of-security/security-data-protection/top-four-critical-security-controls/

Week 3: October 15

Topic: Current State of "Security" in the US Voting System

Speaker: Harri Hursti, Founding Partner, Nordic Innovation Labs

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

Tensions Flare as Hackers Root Out Flaws in Voting Machines
By Robert McMillan and Dustin Volz
https://www.wsj.com/articles/tensions-flare-as-hackers-root-out-flaws-in-voting-machines-1534078801

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

Which voting machines can be hacked through the Internet?
By Andrew Appel
https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/

Week 4: October 22
Topic: Cyber Threats to Democracy: Russia and the Geopolitical Landscape

Speaker: Ambassador Douglas Lute, Robert F. McDermott Distinguished Chair of Social Sciences, United States Military Academy at West Point; former US Ambassador to NATO

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/

A Guide to Russia's High Tech Tool Box for Subverting US Democracy
By Garrett M. Graff
https://www.wired.com/story/a-guide-to-russias-high-tech-tool-box-for-subverting-us-democracy/

The US Gives Cyber Command the Status It Deserves
By Lily Hay Newman

https://www.wired.com/story/cyber-command-elevated/

FIRST BRIEF DUE NEXT WEEK

Week 5: October 29
Topic: Technical Vulnerabilities in the US Election System

Speaker: Sherri Ramsay, Senior Advisor to the CEO, CyberPoint International; Advisor, Cambridge Global Advisors

Readings:

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

Countdown to Zero Day
By Kim Zetter
--Prologue
--Chapter 1 - Early Warning
--Chapter 2 - 500 Kilobytes of Mystery
--Chapter 3 - Natanz
--Chapter 4 - Stuxnet Deconstructed
--Chapter 9 - Industrial Weapons Out of Control
--Chapter 12 - A New Fighting Domain
--Chapter 18 - Qualified Success
--Chapter 19 - Digital Pandora

FIRST BRIEF DUE TODAY

Week 6: November 5
Topic: The Future of e-Government

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

Readings:

Estonia's advance towards an e-state also brings about a new challenge in foreign policy
By Luukas Ilves
https://www.diplomaatia.ee/en/article/e-estonian-foreign-policy/

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/

How Estonia is Leading the Way for Business and Technology Startups
By James Conroy
http://irishtechnews.ie/how-estonia-is-leading-the-way-for-business-and-technology-startups/

Week 7: November 12
Topic: Improving Election Security for Residents of Cook County

Speaker: Noah Praetz, Director of Elections, Cook County, Illinois

Readings:
2020 Vision: Election Security in the Age of Committed Foreign Threats
By Noah Praetz
https://mma.prnewswire.com/media/617112/DEFCON_Voting_Village_Report.pdf

Many County Elections Officials Still Lack Cybersecurity Training
By Likhitha Butchireddygari
https://www.nbcnews.com/politics/national-security/voting-prep-n790256

Securing Elections as Critical Infrastructure
National Association of Secretaries of State
http://www.nass.org/index.php/nass-initiatives/nass-cybersecurity-elections-critical-infrastructure/

Election Commission Wants to Work With DHS on Election Cybersecurity
By Joseph Marks
http://www.nextgov.com/cybersecurity/2017/08/election-commission-wants-work-dhs-election-cybersecurity/140296/

SECOND BRIEF DUE NEXT WEEK

Week 8: November 19
Topic: Elections 2016: What We Know Now and What to Do About It

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

President's Executive Order Will Strengthen Cybersecurity for Federal Networks and Critical Infrastructure
U.S. Department of Homeland Security
https://www.dhs.gov/news/2017/05/11/president-s-executive-order-will-strengthen-cybersecurity-federal-networks-and

Senators propose 9/11-style commission on Russian interference
By Morgan Chalfant
http://thehill.com/policy/cybersecurity/350859-senators-move-to-create-national-commission-on-election-cyberattacks

SECOND BRIEF DUE TODAY

Week 9: November 26
Topic: Cybersecurity Policy and International Norms

Speaker: TBA

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

Defending a New Domain
By William Lynn
http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

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

Week 10: December 3
Topic: The Dark Tangent: A Hacker's View of Cyber Policy

Speaker*:* Tony Sager, Senior Vice President & Chief Evangelist, Center for Internet Security; former Chief Operating Officer of the National Security Agency Information Assurance Directorate

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

Suggested Reading:

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