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

Instructor: Jake Braun

Fall Quarter 2017: Mondays 3:00 – 5:50 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. There will then be a 20 – 30 minute presentation from guest speakers in the cybersecurity field (public and private sector), followed by Q & A and discussion. 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 speakers and assigned readings. These papers will be submitted (electronic and hard copy versions) on the following dates:
    - Brief #1: October 23 - to cover material covered in Week 4
    - Brief #2: November 13 - to cover material covered in Week 7
- 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 4 (electronically). Students will also present their research at a conference on December 4, 2017.

Week 1: September 25

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 2

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 9
Topic: Cybersecurity Policy and International Norms

Speaker: Jane Holl Lute, President and CEO at SICPA North America; Special Adviser to the Secretary-General of the United Nations; former CEO, Center for Internet Security

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 4: October 16
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 NEXT WEEK

Week 5: October 23
Topic: Current State of "Security" in the US Voting System

Speaker: Harri Hursti, Founding Partner, Nordic Innovation Labs

Readings:
After 2016 Election Hacks, Some States Return to Paper Ballots
By JB Wogan
http://www.governing.com/topics/politics/gov-virginia-paper-voting-machines-georgia.html

The Cyber Threat To Germany's Elections Is Very Real
By Sumi Somaskanda
https://www.theatlantic.com/international/archive/2017/09/germany-merkel-putin-elections-cyber-hacking/540162/

Transforming Election Cybersecurity
By David P. Fidler, Adjunct Senior Fellow for Cybersecurity, Council on Foreign Relations
https://www.cfr.org/report/transforming-election-cybersecurity

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/

FIRST BRIEF DUE TODAY

Week 6: October 30
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 6
Topic: The Dark Tangent: A Hacker's View of Cyber Policy

Speaker: Jeff Moss, Founder and Director, Black Hat and DEFCON cyber conferences; Advisor, U.S. Department of Homeland Security Advisory Council (HSAC)

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

SECOND BRIEF DUE NEXT WEEK

Week 8: November 13
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 20
Topic: Improving Election Security for Residents of Cook County

Speaker: Noah Praetz, Director of Elections, Cook County

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

The One Kernel of Truth at Trump's Voter Fraud Summit
By Issie Lapowsky
https://www.wired.com/story/trump-voter-fraud-committee/

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/

Week 10: November 27
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/

Week 11: December 4
Chicago Council on Global Affairs conference

Suggested Reading:

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

Speaker Biographies

Tony Sager, Senior Vice President and Chief Evangelist, Center for Internet Security

Tony Sager is a Senior Vice President and Chief Evangelist for CIS (The Center for Internet Security). In this role, he leads the development of the CIS Controls, a worldwide consensus project to find and support technical best practices in cybersecurity. Sager also serves as the Director of the SANS Innovation Center, a subsidiary of The SANS Institute.

Sager retired from the National Security Agency (NSA) after 34 years as an Information Assurance professional. He started his career in the Communications Security (COMSEC) Intern Program, and worked as a mathematical cryptographer and a software vulnerability analyst. In 2001, Sager led the release of NSA security guidance to the public. He also expanded the NSA's role in the development of open standards for security.

Sager holds a B.A. in Mathematics from Western Maryland College and an M.S. in Computer Science from The Johns Hopkins University. He is also a civilian graduate of the U.S. Army Signal Officer Basic Course and the National Security Leadership Course.

Jane Holl Lute, President and CEO at SICPA North America; Special Adviser to the Secretary-General of the United Nations; former CEO, Center for Internet Security

Dr. Jane Holl Lute is the President and CEO of SICPA North America, a company that specializes in providing solutions to protect the integrity and value of products, processes, and documents. Lute also serves as Special Advisor to the Secretary-General of the United Nations, where she has held several positions in peacekeeping and peace building. Previously, Lute served as Deputy Secretary for the U.S. Department of Homeland Security from 2009-2013. She also served as Chief Executive Officer of the Center for Internet Security (CIS), an operating not-for-profit organization and home of the Multi-State Information Sharing and Analysis Center (MS-ISAC) providing cybersecurity services for state, local, tribal and territorial governments. Lute is a member of several international commissions focused on cybersecurity and the future of the Internet. She began her distinguished career in the United States Army and served on the National Security Council staff under both Presidents George H.W. Bush and William Jefferson Clinton. Lute holds a Ph.D. in political science from Stanford University and a J.D. from Georgetown University. She is a member of the Virginia bar.

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

Sherri is an advisor to CGA on cybersecurity issues. She is also currently the Senior Advisor to the CEO of CyberPoint International, where she is engaged in strategy development and

planning, partnership development, and marketing. She is a member of the Board of Advisors for the Hume Research Center at Virginia Tech and a member of the Board of Directors for EiQ Networks.

Ms. Ramsay is the former Director of the National Security Agency/Central Security Service Threat Operations Center (NTOC) and a former member of the Armed Forces Communications Electronic Administration (AFCEA) Board of Directors. As the NTOC Director, she led discovery and characterization of threats to national security systems, providing situational awareness for those threats, and coordinating actionable information to counter those threats to the DOD, DHS, and FBI. At NSA, she also served as a senior leader in the Signals Intelligence Directorate, the Technology Directorate, and the Information Assurance Directorate. Prior to joining NSA, she taught high school mathematics.

Ms. Ramsay graduated Magna Cum Laude with General Honors from the University of Georgia with a Bachelor of Science degree in Mathematics and Education. She also graduated with Honors from the Johns Hopkins University with a Master's Degree in Computer Science. Additionally, she is a graduate of the Industrial College of the Armed Forces (ICAF), National Defense University, with a Master's in National Resource Strategy. Ms. Ramsay also received a Certificate in Leadership from the University of Virginia.

Harri Hursti, Founding Partner, Nordic Innovation Labs

Mr. Harri Hursti is a world-renowned data security expert, internet visionary and serial entrepreneur. He began his career as the prodigy behind the first commercial, public email and online forum system in Scandinavia. He founded his first company at the age of 13 and went on to cofound EUnet-Finland in his mid- 20's. Today, Harri continues to innovate and find solutions to the world's most vexing problems. He is among the world's leading authority in the areas of election voting security and critical infrastructure and network system security.

Mr. Hursti is considered one of the world's foremost experts on the topic of electronic voting security, having served in all aspects of the industry sector. He is considered an authority on uncovering critical problems in electronic voting systems worldwide. In the last 10 years, Mr. Hursti has pursued this important area out of a sense of duty to his fellow citizens of the world, here are several of his critical findings and projects.

As a consultant, he has conducted and co-authored many studies, both academic and commercial, on various election systems' data security and vulnerability. These studies have come at the request of officials, legislators and policy makers in 5 countries; including the U.S. government, at both the state and federal level.

As an ethical hacker, Mr. Hursti is famously known for his successful attempt to demonstrate how the Diebold Election Systems' voting machines could be hacked, ultimately altering final

voting results. Mr. Hursti was hired by the nonprofit elections watchdog group Black Box Voting, where he performed two voting machine hacking tests, which became widely known as the Hursti Hacks. The first Hursti Hack was set up in Leon County, Florida with the authorization of Supervisor of Elections and these tests examined a Diebold Election Systems Accu-Vote OS 1.94w (optical scan) voting machine. The second Hursti test was conducted for Black Box Voting in collaboration with the County Clerk of Emery County, Utah, on a Diebold TSx touch-screen.

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

Luukas is Counsellor for Digital Affairs at Estonia's Permanent Representation to the EU, where he leads the ICT policy team and is coordinating Estonia's digital agenda for its EU Presidency in the second half of 2017.

Luukas has previously served as Head of International relations for RIA (Estonia's agency for e-government and cybersecurity), where he lead Estonia's push to integrate its e-government systems with neighbouring countries and the EU. He has also worked as a policy planner in the Estonian Ministry of Defence, and as a national expert at the European Commission (in the Cabinet of VP Neelie Kroes). Luukas is a graduate of Stanford University and a reserve officer in the Estonian Defence Forces.

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

Ambassador Douglas Lute is the former United States Permanent Representative to the North Atlantic Council, NATO's standing political body. Appointed by President Obama, he assumed the Brussels-based post in 2013 and served until 2017. During this period he was instrumental in designing and implementing the 28-nation Alliance's responses to the most severe security challenges in Europe since the end of the Cold War.

A career Army officer, in 2010 Lute retired from active duty as a lieutenant general after 35 years of service. In 2007 President Bush named him as Assistant to the President and Deputy National Security Advisor to coordinate the wars in Iraq and Afghanistan. In 2009 he was the senior White House official retained by President Obama and his focus on the National Security Council staff shifted to South Asia. Across these two Administrations, he served a total of six years in the White House.

Before being assigned to the White House, General Lute served as Director of Operations (J3) on the Joint Staff, overseeing U.S. military operations worldwide. From 2004 to 2006, he was Director of Operations for the United States Central Command, with responsibility for U.S.

military operations in 25 countries across the Middle East, eastern Africa and Central Asia, in which over 200,000 U.S. troops operated.

Through his military-diplomatic career, he received numerous honors and awards, including three awards of the Defense Distinguished Service Medal, the State Department's Distinguished Honor Award, the Grand Officer of the Order of Merit for the Italian Republic, and the Commander's Cross of the Order of Merit for the Federal Republic of Germany.

General Lute holds degrees from the United States Military Academy at West Point and from the Kennedy School of Government at Harvard University. He is a Senior Fellow at the Belfer Center at Harvard University; a member of the Council on Foreign Relations; and a charter member of the Flag Officer Advisory Group of the United States Institute of Peace.

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

Francis X. Taylor is the former Under Secretary for Intelligence and Analysis at the U.S. Department of Homeland Security. In that role, he provided the Secretary, DHS senior leadership, the DHS components, and state, local, tribal and private sector partners with the homeland security intelligence and information they need to keep the country safe, secure and resilient. I&A is a member of, and the Department's liaison to, the National Intelligence Community.

Prior to his assignment at DHS I&A, Mr. Taylor was Vice President and Chief Security Officer for the General Electric Company in Fairfield, Conn. At GE, he was responsible for managing the security operations and crisis management processes designed to ensure the security of GE employees and operations globally.

Before GE, Mr. Taylor had a distinguished 35-year career in government service, where he held several senior positions managing investigations, security and counterterrorism issues.

Most recently, he served as the Assistant Secretary of State for Diplomatic Security and Director of the Office of Foreign Missions, with the rank of Ambassador. He was responsible for the global security of all U.S. diplomatic personnel and facilities. Ambassador Taylor also served as the U.S. Ambassador at Large and Coordinator for Counterterrorism for the Department of State from July 2001 to November 2002. In this role, he was responsible for implementing U.S. counterterrorism policy overseas and coordinating the U.S. government response to international terrorist activities.

During his 31 years of military service, Ambassador Taylor served with distinction in numerous command and staff positions, rising to the rank of Brigadier General in September 1996. In his final active duty assignment, Brigadier General Taylor was the Commander, Air Force Office of

Special Investigations, and was responsible for providing Air Force leaders with comprehensive criminal, fraud, counterintelligence and security investigation and operations to protect global Air Force operations.

Mr. Taylor has received numerous awards and decorations, including the U.S. Distinguished Service Medal, the National Intelligence Distinguished Service Medal, the Legion of Merit, the Defense Superior Service Medal and the U.S. Department of State Honor Award.

Mr. Taylor holds a Bachelor's and Master's Degree in Government and International Studies from the University of Notre Dame. He is a Distinguished Graduate of the Notre Dame Air Force ROTC program.

Noah Praetz, Director of Elections, Cook County

Noah runs elections in Cook County Illinois. He believes that free and fair elections remain our core value and organizing principle. He is responsible for the overall management of elections in Cook County, Illinois, one of the largest election jurisdictions in the country. Each year his team serves 1.5 million voters, facilitates democracy for thousands of candidates, and train and support thousands more volunteers to administer democracy. They do so with a range of 100-400 employees and operating budgets north of 20 million dollars. Cook County can be a rough place to manage democracy, with strong parties and a strong press. But Cook County elections has a strong team and a great leader in Cook County Clerk David Orr. Noah believes Cook County is the best place in America to vote.

He started as temporary worker hired help doing data entry prior to the 2000 president election. Bush v. Gore had him hooked. He worked his way through the ranks doing nearly every job in the department - learned all the pain points and all the opportunities. He went to law school at night. In 2007 became Deputy Director of Elections, helping manage everything. In 2013 he was appointed Director.

Noah has focused his department on measuring for success. They are focused on using data to ensure they are serving their voters, candidates and pollworkers successfully. They try to take no action without purpose; constantly adjusting processes to get desired outcomes.

He is a board member of the International Association of Government Officials. He is also active in the Election Center and the Illinois Association of County Clerks and Recorders. He has presented on Election Security, Sustainability, Election Day Management, Online Registration, Voter Registration Modernization and other Election Related items.

Jeff Moss, Founder and Director, Black Hat and DEFCON cyber conferences; Advisor, U.S. Department of Homeland Security Advisory Council (HSAC)

Black Hat Founder and Director Jeff Moss is becoming one of the most sought-after voices in information security. He has spent the last 17 years as founder and director of Black Hat and DefCon, two of the most important security conferences in the world. Moss is uniquely qualified with his ability to bridge the gap between the underground researcher community and law enforcement, between the worlds of pure research and responsible application.

Moss speaks frequently before a wide range of audiences on the topic of computer and information security. Recently in 2009 Moss was appointed to the Homeland Security Advisory Council to provide advice and recommendations to the Secretary on matters related to homeland security. He moderated a panel at RSA 2009 on core infrastructure security threats. Moss also was a keynote speaker at the DOD Cybercrime Conference in St. Louis in 2009, spoke at the first CodeGate conference in South Korea in 2008, the first DeepSec conference in Vienna in 2007, as was a panelist at the Democracy, Terrorism and the Open Internet panel in 2005 in Madrid. He has also been a frequent panelist at RSA. Moss has been interviewed and appeared on TV shows ranging from CNN to G4 TechTV, in magazines Business Week to Computer World, as well as numerous documentaries dealing with internet, law, ethics, hacking, and privacy. In addition Moss has contributed to “Stealing the Network,” a series of books that combine stories that are fictional with technology that is real.

Prior to Black Hat Briefings, Jeff was a director at Secure Computing Corporation where he helped establish the Professional Services Department in the United States, Asia, and Australia. Jeff has also worked for Ernst & Young, LLP in their Information System Security division. Jeff graduated with a BA in Criminal Justice from Gonzaga University.