GERALD R. FORD SCHOOL OF PUBLIC POLICY
UNIVERSITY OF MICHIGAN

PubPol 750.006/475.005: Cybersecurity for Future Leaders

Instructors:

Carl Landwehr, Visiting Professor
734-763-6856 (office phone)
celand@umich.edu (email)
3115 EECS (office location)
1010 Dow (class location)

Javed Ali, Towsley Policymaker in Residence
734-647-6684 (office phone)
alimust@umich.edu (email)
5317 Weill (office location)
1010 Dow (class location)

Instructor Office Hours:

Carl Landwehr: Tuesdays 1:00 pm-3pm
Javed Ali**:** Mondays 1:30pm-3:15pm

Course Term:

14-week session Mondays, 4:00 pm – 7:00 pm
September 9 – December 16

Course Description: Future leaders will need to understand the science, technology, and human considerations behind cybersecurity well enough to make informed decisions when provided advice and options for action. Over the last decade cybersecurity issues have risen in prominence from a U.S. national security perspective, as well as from the perspective of individuals and organizations. There have been near daily reports regarding cyber operations launched by nation states, hacking groups, criminal organizations, and other malign actors against a variety of targets, using different tools and methods, and with different effects. The U.S. government has attempted to reorganize and reorient towards this multi-dimensional threat, in addition to private industry, state and local governments, and academia—but despite this increased focus there are still several gaps and vulnerabilities that deserve technical and policy attention and solutions.

This class will examine the broad landscape of cybersecurity from both a technical and policy perspective. It will introduce fundamental concepts of computing and cyber security, including information theory, computability, cryptography, networking fundamentals, how vulnerabilities arise, and how attacks work. In addition, it will explore foundational ideas including definitions, cyber norms, and ethics; identify existing U.S. laws, authorities and governmental constructs; and frame classic security concepts like deterrence, attribution, offense, defense, and retaliation. The course will also involve guest speakers, short writing assignments

designed to capture technical or policy insights, policy papers designed to explore alternative views on different cybersecurity topics, and a simulated policy meeting where students will have the choice of assuming different corporate or Federal government roles and examine potential courses of action in response to a cybersecurity crisis scenario.

Course Objectives: The objectives of the course include:

1. Enhancing knowledge on technical and policy aspects of cybersecurity.
2. Sharpening critical thinking, executive briefing, and team collaboration skills.
3. Understanding real-world implications of cyber operations.
4. Identifying possible solutions or opportunities to address existing cybersecurity challenges.

Course Grading: This class requires seven graded assignments: three problem sets; three two-three page memos; and one simulation that will involve role-playing different corporate-executive or federal-level perspectives. In addition, another aspect of the course that will be graded is class participation, which has two components and is explained in further detail below. Late work needs to be negotiated ***before*** the day the assignment is due (just like you would do on a job). We are always willing to negotiate a new deadline if you have a reasonable reason for needing an extension. However, assignments that are turned in late without prior discussion or approval will be docked one grade step for every day they are late. ***Likewise, absent an emergency or unexpected illness, full participation is required for the simulation on 9 December, and failure to attend will significantly impact the grade***.

Class participation and engagement	20%
Problem Sets (x3)	30%
Policy Memos (x3)	30%
Policy Simulation (x1)	20%
	100%

Class Participation and engagement: Half of the grade (10%) for this component will account for in-person attendance (any unexcused absence without prior notification will be docked one grade step). The other half (10%) will be based on our assessment of your participation in-class with questions, cross-student discussion, and reflection. **Since there is no class following the Labor Day weekend, students are expected to read the assigned material for the class on 9 September.**

Problem Sets: Technical concepts fundamental to policy questions will be introduced from the beginning of the course. Problem sets will probe students' understanding of these concepts. The problems will not be highly mathematical but may involve binary arithmetic and other aspects of data representation in computers that bear on cybersecurity. These will be assigned on September 16, 23, and October 7; the first two will be due one week after assignment, and the third will be due two weeks after assignment. **Students will be evaluated based on their ability to solve the assigned problems; in some cases, the**

reasoning behind the solution will be evaluated as well. Each problem set will count 10% toward overall course grade. Problems sets are to be done individually.

Policy Memos: Three policy memos (two to three pages each) are required for this component, with due dates of 21 October, 4 November, and 18 November; each will comprise 10% with all three equaling 30% of the total grade. **Similar to the options presented for the class simulation (see below), students will have a choice writing on either a national security or corporate-related topic for the three assignments (we recommend students stick with one topic track for all three, but alternating between both sets is permitted).** *Students will be evaluated on their ability to: write cogently and concisely; present a logical argument within a coherent memo structure; and minimize grammatical or spelling errors and avoid colloquial expressions.* Students will be expected to conduct research to support their assessments beyond the material listed in the course readings, and details on all the potential issues are available via multiple sources through Internet-based sources from major newspapers like the *New York Times* and *Washington Post;* a variety of national security-related periodicals and websites; academic and research organizations; and, U.S. government publications and documents. ***Memos should be singled-spaced in 12-point Times New Roman font, with bolded text to designate headers between key sections, with references captured using footnotes at the bottom of each page.*** They should also be done individually.

- Policy Memo #1 Corporate topic – Attack Impact
    - Objective: Understand what happened technically in a specific commercial system security breach.
    - Approach: Review in depth a significant cybersecurity incident, identify the root causes of the breach, the extent of the damage, and what was done to recover. Numerous potential examples include 2011-2013 Iranian attacks against U.S. banks, 2013/14 Yahoo breaches, 2014 Sony hack, and the 2017 Wannacry attacks.

- Policy Memo #1 National Security topic – Attack Impact
    - Objective: Understand and explain what happened technically in a government system or critical infrastructure cybersecurity breach.
    - Approach: Like corporate, but for a government system and/or involving government actors, review in depth a identify the root causes of the breach, the extent of the damage, and what was done to recover. Potential examples include the 2013 Snowden disclosures, 2016 US Office of Personnel Management (OPM) breach, and 2016 Russian election interference.

- Policy Memo #2 Corporate topic – Decision-making Factors
    - Objective: Understand factors influencing corporate decisions about security and privacy strategy for a product or system.

- Approach: Estimate effects of alternative designs on system cost, time to market, ability to withstand categories of threat, liability, and consumer acceptance. Pick two actual products in the same market space (e.g. Android vs Apple phones, two different Internet of Things devices, two different browsers, etc.) and compare security and privacy aspects.

- Policy Memo #2 National Security topic – Decision-making Factors

  - Objective: Understand factors influencing government decisions about security and privacy strategy for critical infrastructure systems or commercial products.
  - Approach: For a system (e.g., smartphone, air traffic control system, power grid, elections), consider the viewpoints of different departments and agencies, e.g. intelligence, defense, law enforcement, homeland security, commerce, energy, etc. and document positions they might take regarding the technology.

- Policy Memo #3 Corporate topic – Policy Recommendations

  - Objective: Demonstrate ability to develop and defend alternative corporate policy recommendations for security / privacy strategy for a new product or system.
  - Approach: Assess benefits and risks of investing in cybersecurity aspects of a product or system, such as electronic systems for autonomous vehicles, medical devices, power system components, or smartphones. Consider investment costs for pre-market and post-market investments in cybersecurity improvements. Provide three alternative courses of action for business management that could be implemented.

- Policy Memo #3 National Security topic – Policy Recommendations

  - Objective: Demonstrate ability to develop and defend alternative national policy recommendations for security/privacy strategy in a context.
  - Approach: Describe a future cyber threat scenario over the next three-to-five years that could produce catastrophic effects (a major blackout, defense system outage, transportation tie-up) in the United States; assess its likelihood; project which threat adversary would be capable of inflicting such an attack; and, provide a recommendation on three courses of action to prevent it from occurring.

Policy Simulations: Students will have the choice in participating in two different simulated policy meetings dealing with a cybersecurity crisis scenario that will be conducted during the 9 December class, which will comprise 20% of the course grade. One meeting will entail role-playing various corporate-executive positions while the other will entail a National Security Council meeting. Students will provide inputs on their preferences regarding the corporate and federal governmental roles they would like to assume, and the topics for the crisis scenarios. Students will be evaluated on the quality of each individual student/team

presentation, and research and preparation for the role in each simulation.

- Depending on the size of the class, **for the corporate-executive simulation** students can act as individuals or small teams to represent roles from the: Chief Executive Officer, Chief Technology Officer, Chief Information Officer, Chief Privacy Officer, Chief Financial Officer, Chief Operating Officer; Corporate General Counsel, Government Relations representative. Corporate Communications Director, and Consumer Ombudsman.

- Depending on the size of the class, **for the federal simulation** students can act as individuals or small teams to represent roles from the: President, Vice President, or Chief of Staff; National Security council (multiple positions); Central Intelligence Agency; Department of Defense and Joint Chiefs of Staff (includes Cyber Command); Department of Homeland Security; Attorney General; Federal Bureau of Investigation; Department of State; Director of National Intelligence; National Security Agency; and Treasury Department.

Required Texts: There are only two required texts for the course which focus on technical aspects of cybersecurity. The policy readings are all drawn literature will all be publicly available via Internet sources. We have included a recommended bibliography list for those who wish to read more on national security-related aspects.

Anderson, R. *Security Engineering*, Second Edition, John Wiley. Available free online at: https://www.cl.cam.ac.uk/~rja14/book.html

Kernighan, B. *Understanding the Digital World*. First Edition, New York: Princeton University Press. 2017.

National Security Bibliography

Carlin, J. *Dawn of the Code War*. First Edition, New York: PublicAffairs, 2018.

Dion-Schwarz, C, Manheim, D., and Johnston, P. *Terrorist Use of Cryptocurrencies*. First Edition, Santa Monica: RAND Corporation. 2019. https://www.rand.org/pubs/research_reports/RR3026.html

Husain, A. and Allen, J. *Hyperwar: Competition and Conflict in the 21st Century*. Paperback Edition. SparkCognition Press. 2018.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. Paperback Edition, New York: Simon & Schuster. 2016.

Libicki, M. *Cyberdeterrence and Cyberwar*. First Edition, Santa Monica: RAND Corporation. 2009. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, M. *Crisis and Escalation in Cyberspace*. First Edition, Santa Monica: RAND Corporation. 2012.
https://www.rand.org/pubs/monographs/MG1215.html

Libicki, M., Ablon, L. and Webb, T. *The Defender's Dilemma: Charting a Course Towards Cybersecurity*. First Edition, Santa Monica: RAND Corporation. 2015.
https://www.rand.org/pubs/research_reports/RR1024.html

Lucas, George. *Ethics and Cyberwarfare*. First Edition, London: Oxford University Press. 2016.

Sanger. D. *The Perfect Weapon.* First Edition, New York: Crown. 2018.

Singer, P.W. and Friedman, A. *Cybersecurity and Cyberwar*. Paperback Edition, New York: Oxford University Press. 2014.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Paperback Edition, London: Cambridge University Press. 2017.

Tehan, R. *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*. Washington, D.C.: Congressional Research Service. 8 November 2018.
https://fas.org/sgp/crs/misc/R43317.pdf

FORD SCHOOL OF PUBLIC POLICY INCLUSIVITY STATEMENT

Members of the Ford School community represent a rich variety of backgrounds and perspectives. We are committed to providing an atmosphere for learning that respects diversity. While working together to build this community we ask all members to:

- share their unique experiences, values and beliefs
- be open to the views of others
- honor the uniqueness of their colleagues
- appreciate the opportunity that we have to learn from each other in this community
- value one another's opinions and communicate in a respectful manner
- keep confidential discussions that the community has of a personal (or professional) nature
- use this opportunity together to discuss ways in which we can create an inclusive environment in Ford classes and across the UM community

Accommodations for Students with Disabilities: If you believe you need an accommodation for a disability, please let your instructor know at your earliest convenience. Some aspects of courses may be modified to facilitate your participation

and progress. As soon as you make your instructor aware of your needs, they can work with the Services for Students with Disabilities (SSD) office to help determine appropriate academic accommodations. Any information you provide will be treated as private and confidential.

Student Mental Health and Well-Being Resources: The University of Michigan is committed to advancing the mental health and wellbeing of its students. We acknowledge that a variety of issues, such as strained relationships, increased anxiety, alcohol/drug problems, and depression, directly impacts students' academic performance. If you or someone you know is feeling overwhelmed, depressed, and/or in need of support, services are available. For help, contact Counseling and Psychological Services (CAPS) and/or University Health Service (UHS). For a listing of other mental health resources available on and off campus, visit: http://umich.edu/~mhealth/

Class Expectations. We intend to conduct the class along the following lines, so that it:

- **Prepares students for the rigors** associated with drafting products for senior executive consumption, with an emphasis on clarity of analysis, concise summation of complex cybersecurity topics, and well-structured formats.
- **Develops interpersonal and team bonds** since these are important attributes in the national security field. During the first class on 9 September, please come prepared to speak briefly (two-three minutes) regarding your academic and/or professional background, your interest in the course and motivation for taking it, and whether you hope to pursue a career in cybersecurity.
- **Expects punctuality.** We will start promptly at 4:00 p.m. and end promptly at 6:50 p.m. each session; we will have one break between 5:20 p.m. and 5:30 p.m. each class. Other than the schedule break, please refrain from going in and out of the room during class unless necessary.
- **Prefers that during class, you do not check** your cell phone to send text messages/tweets, or video/audio record the contents of each session. This request preserves the integrity of the discussion and eliminates distractions. Note-taking via laptop is appropriate but also expect no sending of text or instant messages/tweets, social media posting, or video or audio recording of classroom dialogue.
- **Takes seriously academic misconduct, to include** cheating, misrepresenting one's own work, taking credit for the work of others without acknowledgement and without appropriate authorization, and the fabrication of information. Any form of misconduct will be taken very seriously. Academic dishonesty also includes using something you produced for another class for an assignment without permission. Information regarding academic dishonesty, plagiarism and misconduct and their consequences is available at: http://www.rackham.umich.edu/current-students/policies/academic-policies...

Please review additional information and policies regarding academic expectations and resources at the Ford School of Public Policy at this link:
http://fordschool.umich.edu/academics/expectations

September 9, 2019 Introduction to Cybersecurity

Guest: (none)

Summary: Roadmap for the course, procedures, ethics, grading
Technical: Survey of notable cybersecurity attacks and incidents,
Policy: Structure of the U.S. government: executive, including agencies and responsibilities, judicial, legislative, state and local.

Assignments: Readings and class questionnaire

Technical

Landwehr, C. *Cybersecurity for Future Presidents (DRAFT)*. Chapter 1.

Policy

Brumfield, Cynthia. "The Cybersecurity Legislation Agenda: Five Areas to Watch." CSO Online. 21 February 2019.
https://www.csoonline.com/article/3341383/the-cybersecurity-legislation-agenda-5-areas-to-watch.html

Charlet, Kate. "Understanding Federal Cybersecurity." *Belfer Center for Science and International Affairs*. April 2018.
https://www.belfercenter.org/sites/default/files/files/publication/Understanding%20Federal%20Cybersecurity%2004-2018_0.pdf

September 16, 2019 Cyber Ethics and Norms, Computing and Networking Fundamentals

Guest: (none)

Summary: Technical: Data representation in computers. Basic information theory. Networking fundamentals: History of telephony; circuit switching and packet switching.
Policy: Concepts and ideas regarding cyber ethics and norms, and their impact on current dimensions of cybersecurity policy, and cyberwarfare legal concepts.

Assignments: Readings and problem set #1 (due Sep 23)

Technical

Kernighan, B. *Understanding the Digital World*, pp. 1-36 (through end of Chapter 2).

Anderson, R. *Security Engineering, 2nd. Ed*. Chapter 1 What is Security Engineering? pp. 3-15.
https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c01.pdf

Policy

Bradbury, Danny. "In Search of an Ethical Code for Cybersecurity." *Infosecurity-Magazine*." 17 August 2017.
https://www.infosecurity-magazine.com/magazine-features/search-ethical-code-cybersecurity/

Dipert, Randall. "The Ethics of Cyberwarfare." *Journal of Military Ethics* (9:4). 2010.
https://www.law.upenn.edu/live/files/1700-dipert-r-the-ethics-of-cyberwarfare-2010

Schmitt, Michael. "Tallinn Manual 2.0 on the International Law of Cyber Operations." *Justsecurity.org*. 17 February 2017.
https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/

September 23, 2019 **Surveillance and Cryptography Technology and Policy (Problem Set #1 Due)**

Guest: Professor Barbara McQuade, University of Michigan School of Law (confirmed)
Bio: Link to Professor McQuade's bio
https://www.law.umich.edu/FacultyBio/Pages/FacultyBio.aspx?FacID=bmcquade

Summary: Technical: what a leader needs to know about crypto, covering perfect secrecy, randomness, symmetric and asymmetric cryptography.
Policy: Purposes and legislation controlling government surveillance in the U.S. from Writs of Assistance through the USA Freedom Act.

Assignments: Readings and problem set #2 (due Sep 30)

Technical

Kernighan, *Understanding the Digital World*. Chapter 12: Privacy and Security. (pp.203-216).

Policy

Foreign Intelligence Surveillance. *Brennan Center for Justice*.
https://www.brennancenter.org/analysis/foreign-intelligence-surveillance-fisa-section-702-executive-order-12333-and-section-215

Foreign Intelligence Surveillance Act (FISA) of 1978. *Department of Justice, Office of Justice Programs*.
https://it.ojp.gov/privacyliberty/authorities/statutes/1286

Kris, David. "How the FISA Court Really Works." *Lawfareblog.com*. 2 September 2018.
https://www.lawfareblog.com/how-fisa-court-really-works

September 30, 2019 **Cybersecurity Fundamentals and U.S. Laws, Authorities, and Policies (Problem Set #2 Due)**

Guest: (none)

Summary: Technical: What a leader needs to know about computing and cybersecurity technology. Computer architecture, access control, information flow, side channels.
Policy: U.S. cybersecurity policy evolution and strategy comparisons.

Assignments: Readings

Technical

Kernighan, *Understanding the Digital World*. Chapter 3 and Wrap up on Hardware (pp. 37-52)

Anderson, *Security Engineering, 2nd. Ed*., Chapter 4, Access Control, through Section 4.2.3 (pp. 93-101)
https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c04.pdf

Policy

Department of Defense Cyber Strategy. *Department of Defense*. September 2018.
https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

DHS Cybersecurity Strategy. *Department of Homeland Security*. May 2018.
https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

National Cyber Strategy of the United States of America. *White House*. September 2018.
https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

October 7, 2019 **Classic Security Theory and Cybersecurity; Vulnerabilities, Attacks, Cyber Operations**

Guest: Peter Honeyman, University of Michigan (invited)

Summary**:** Technical: How technical vulnerabilities arise and how they are exploited. Social engineering.
Policy: Classic security theory concepts like deterrence, retaliation, and attribution from a cybersecurity perspective; overview of different attack methods, capabilities, and adversary intentions.

Assignments: Readings, and problem set #3 and policy memo #1 (both due Oct 21)

Technical

Kernighan, *Understanding the Digital World*. Part II Software (pp. 53-54), Chapter 4, (pp. 55-65)

Stojano, Frank and Paul Wilson. Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM*, Vol. 54, No.3, (March 2011) pp. 70-75.
https://www.cl.cam.ac.uk/~fms27/papers/2011-StajanoWil-scam.pdf

Policy

Efrony, Dan. "Is it Time to Regulate Cyber Conflicts?" *Lawfareblog.com*. 4 May 2018.
https://www.lawfareblog.com/it-time-regulate-cyber-conflicts

Miller, James and Pollard, Neal. "Persistent Engagement, Agreed Competition, and Deterrence in Cyberspace." Lawfareblog.com. 30 April 2019.
https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace

Nye, Joseph. "Deterrence and Dissuasion in Cyberspace." *International Security* (41:3). Winter 2016/2017.
https://www.belfercenter.org/sites/default/files/files/publication/isec_a_00266.pdf

October 14, 2019 **No Class, Fall Study Break**

October 21, 2019 **Privacy Concepts, Policy, and Technology (Problem Set #3 and Policy Memo #1 Due)**

Guest: TBD

Summary: Technical: Cryptography for privacy/anonymity, secure multiparty computation, differential privacy overview
Policy: Meanings of "privacy," styles of regulation, US regulatory history vs. Europe, GDPR, etc.

Assignments: Readings and policy memo #2 (due Nov 4)

Technical

Kernighan, *Understanding the Digital World*. Chapter 10 (The World Wide Web) and 11 (Data and Information) pp. 163-202.

Policy

Meyer, David. "In the Wake of GDPR, Will the U.S. Embrace Data Privacy?". *Fortune*. 30 November 2018.
http://fortune.com/2018/11/29/federal-data-privacy-law/

"Reforming the U.S. Approach to Data Protection and Privacy." *Council on Foreign Relations*. 30 January 2018.
https://www.cfr.org/report/reforming-us-approach-data-protection

"State Laws Relating to Internet Privacy." *National Council of State Legislatures*. 28 February 2019.
http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

October 28, 2019 Cybersecurity Aspects of Elections

Guest: (none)

Summary: Technical: Identification and authentication technology, including biometrics. Overview of election system technical architectures.
Policy: U.S. election system enterprise, impact of 2016 Russian interference, technical and policy recommendations to strengthen election systems.

Assignments: Readings

Technical

Kernighan, Part III Communications, Chapter 8 Networks and Chapter 9 The Internet. Pp 119-161.

Anderson, *Security Engineering*, *2nd Ed*. Chapter 15, Biometrics, pp. 457-482.
https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c15.pdf
[Note this reading dates from 2008; technology, particularly in facial and DNA recognition, has advanced since then.]

National Academies of Sciences, Engineering, and Medicine 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25120. Read Preface and Chapter 5, Assuring the Integrity of Elections, pp. 85-106.

Policy

Carter, William. CSIS Cybersecurity Election Scorecard. *Center for Strategic and International Studies*. 29 October 2018.
https://www.csis.org/analysis/csis-election-cybersecurity-scorecard-outlook-2018-2020-and-beyond

Mook, Robby, Rhoades, Matt, Rosenbach, Eric. The State and Local Cybersecurity Playbook. *Belfer Center for Science and International Affairs*. February 2018.
https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

November 4, 2019 Private Sector Views on Cybersecurity (Policy Memo #2 due)

Guest: Steve Block, Amazon Web Services (confirmed)
Bio: Forthcoming

Summary: Technical: Current enterprise cybersecurity system architectures. Security, economics, and human behavior.
Policy: This module will examine how the private sector is confronting the threat of cyber operations and what partnerships and relationships with the government are yielding benefits.

Assignments: Readings and policy memo #3

Technical

Kernighan Chapter 5. Programming and Programming Languages, pp. 65-86.

Anderson, Ross. *Security Engineering, 2nd. Ed*. Chapter 1 What is Security Engineering? pp. 3-15.
https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c01.pdf

Policy

Executive Order 13691. Promoting Private Sector Cybersecurity Information Sharing. *White House*. 15 February 2015.
https://www.dhs.gov/sites/default/files/publications/2015-03714.pdf

Knake, Robert. "Sharing Classified Cyber Threat Information with the Private Sector." *Council on Foreign Relations*. 15 May 2018.
https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector

Saboni, Gabi and Ida Sivan-Sevilla. "The Role of the State in the Private Sector Cybersecurity Challenge." *Georgetown Journal of International Affairs*. 27 May 2018.
https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/5/27/the-role-of-the-state-in-the-private-sector-cybersecurity-challenge

November 11, 2019 Cyber - Physical System Cybersecurity

Guest: TBD

Summary: Technical: Automotive system structure, vulnerabilities, attacks. New issues for autonomous vehicles. Other cyber physical systems and how they are different/alike.
Policy: automotive regulation, National Transportation Safety Board approaches vs Federal Aviation Administration; rail, other transportation modes.

Assignments: Readings

Technical

Kernighan, *Understanding the Digital World*. Chapter 6. Software Systems. Pp.87-104.

Hanna, Mina J., Shawn C. Kimmel. Current US Federal Policy Framework for Self-Driving Vehicles: Opportunities and Challenges. IEEE COMPUTER, December 2017, pp. 32-40.

Burns, A. J., Johnson, M. E., and Honeyman, P. A Brief Chronology of Medical Device Security. *Communications of the ACM, 59*(10), 66–72. (2016, September).
https://doi.org/10.1145/2890488

November 18, 2019 Blockchain and Digital Currencies (Policy Memo #3 due)

Guest: (none)

Summary**:** Technical: Structure of blockchain, security assumptions, pseudonymity/ vs. anonymity.

Policy: Regulations and legal history of money laundering, currency tracing.

Assignments: Readings

Technical

Sherman, Alan T., Farid Javani, Haibin Zhang, Enis Golaszewski. On the Origins and Variations of Blockchain Technologies. *IEEE Security & Privacy Magazine, Vol. 17*, No. 1 (Jan-Feb. 2019) pp. 12-22.

Zohar, Aviv. Bitcoin: Under the Hood. Communications of the ACM, Vol. 58, No. 9 (Sept. 2015).
http://tau-crypto-f16.wdfiles.com/local--files/course-schedule/bitcoin-zohar-cacm.pdf

CreditCards.com: How a Credit Card is Processed, 2013.
https://www.creditcards.com/credit-card-news/assets/HowACreditCardIsProcessed.pdf

Policy

"Blockchain Technology: The Future of Cybersecurity?" *StrongerTech.com*. 26 April 2018.
https://stronger.tech/blockchain-the-future-of-cyber-security/

Chamberlin, Kelly. "Cyber Threats: How Banks Can Share Information More Effectively." *ABA Banking Journal*. 5 November 2018.
https://bankingjournal.aba.com/2018/11/cyber-threats-how-banks-can-share-information-effectively/

November 25, 2019 **Data Science, Artificial Intelligence/Machine Learning, Privacy and Security**

Guest: (none)

Summary: Technical: basics of artificial intelligence/machine learning, adversarial learning. More on differential privacy.
Policy: Issues for achieving algorithmic transparency and detecting / reporting bias; ethics for autonomous systems.

Assignments: Readings and simulation preparations

Technical

National Academy of Sciences 2018. *The Frontiers of Machine Learning: 2017 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25021. Pp. 4-23. Available at:

http://nap.edu/25021

Policy

"Algorithmic Transparency: End Secret Profiling." *Electronic Privacy Information Center*. Accessed 25 March 2019.
https://epic.org/algorithmic-transparency/

Goosen, Ryan, et. al. "AI is a Threat to Cybersecurity. It's Also a Potential Solution." *BCG.com*. 13 May 2018.
https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx

West, Darrell and John Allen. "How Artificial Intelligence is Transforming the World." *Brookings Institution*. 24 April 2018.
https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/

Supplementary:

Online tutorials:
An Introduction to Machine Learning Theory and Its Applications: A Visual Tutorial with Examples. https://www.toptal.com/machine-learning/machine-learning-theory-an-introductory-primer
Digital Ocean. An Introduction to Machine Learning. Available at:
https://www.digitalocean.com/community/tutorials/an-introduction-to-machine-learning

Another introductory article
Royal Society. *Machine learning: the power and promise of computers that learn by example*. Chapter 1.
https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf
For a deeper read in machine learning, more mathematical:
Murphy, Kevin. *Probabilistic Machine Learning*. Chapter 1, Introduction, pp. 1-25. MIT Press. Available at:
https://www.cs.ubc.ca/~murphyk/MLbook/
https://www.cs.ubc.ca/~murphyk/MLbook/pml-intro-22may12.pdf

December 2, 2019 **Health information Technology and Policy issues; Cybersecurity Roundtable**

Guests: Brent Ciezsynki, Michigan Blue Cross Blue Shield (invited)
Kevin Fu, University of Michigan (invited)
Ellen Nakashima, Washington Post (invited)

Eric Schmitt, New York Times (confirmed)

Summary: Technical: basics of human genetics, healthcare information processing, biometrics.
Policy: HIPAA, GINA, genetic databases and law enforcement, biometric policies.

Assignments: Prepare for Capstone simulations (on Dec 9)

Technical

Ayday, Erman, Emiliano De Cristofaro, Jean-Pierre Hubaux, and Gene Tsudik. Whole Genome Sequencing: Revolutionary Medicine or Privacy Nightmare? IEEE COMPUTER, February 2015, pp. 58-66.

Policy

Kruse, Scott, Benjamin Frederick, Taylor Jacobson, and D. Kyle Montague. "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends." *Technology and Health Care*, 25 (2017).
https://content.iospress.com/download/technology-and-health-care/thc1263?id=technology-and-health-care%2Fthc1263

Le Bris, Aurora and Walid el Asri. *State of Cybersecurity and Cyber Threats in Healthcare Organizations*. ESSEC Business School. Accessed 10 April 2019.
https://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf

December 9, 2019 Capstone Simulations

Summary: This module involves simulated corporate-executive and National Security Council meetings where students will assume different roles and respond to different cybersecurity scenarios. Each meeting will evaluate different options presented for consideration and seek to provide a formal recommendation for further action if consensus is reached.