**PubPol 750.004/475.004:   Cybersecurity for Future Leaders**

**Instructors:** Carl Landwehr, Visiting Professor

734-763-6856 (office phone)

[celand@umich.edu](mailto:celand@umich.edu) (email)

3115 EECS (office location)

1120 Weill (class location)

Javed Ali, Towsley Policymaker in Residence

734-647-6684 (office phone)

[alimust@umich.edu](mailto:alimust@umich.edu) (email)

5317 Weill (office location)

1120 Weill (class location)

**Instructor Office Hours:** Carl Landwehr:Tuesdays 1:00 pm-3:00pm, or by appointment\* (virtual)

Javed Ali**:** Mondays 1:00pm-3:30pm or by appointment (in-person or virtual per student preference)

**Course Term:** 14-week session Mondays, 4:00 pm – 6:50 pm

31 August – 7 December (\*no final exam)

**Course Description:** Future leaders will need to understand the science, technology, public policy, and national security 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 in both the public and private spheres, with an increasing interrelationship between what have traditionally been two distinct domains. 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. As we head towards another Presidential election in November 2020, these issues will remain at the forefront given what occurred in the last elections and the use of sophisticated cyber means to influence public opinion, sow political divisions, potentially compromise election results, and demonstrate a capability that was not fully operationalized.

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 into a cybersecurity lens—which will be accentuated by expert perspectives from a range of guest speakers. Graded assignments will entail policy papers designed to explore technical concepts and policy positions, student-led panel discussions on topics related to weekly syllabus themes, 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. Identifying possible solutions or opportunities to address existing cybersecurity challenges.
4. Role-playing key government or private sector positions to simulate potential responses during a crisis simulation involving cybersecurity effects.

**Course to be conducted in “hybrid” mode, Fall 2020:** Because of the risks posed by the current pandemic, the class will be conducted in a hybrid mode. Two professors will conduct the course. Professor Ali will be present in the classroom during the scheduled meeting times; Professor Landwehr will be remote. Students may be present in the classroom or may participate remotely. Remote participation will require the student to have a laptop or other computer equipped with a videocamera. If more students choose to be present than can be accommodated under physical distancing guidelines, they will be divided into groups to participate in person on alternate class sessions. Guest lecturers will also participate remotely. Class sessions will be recorded and made available afterwards so that students unable to participate in a class will be able to review the session. Some lecture materials may also be made available for review in advance of class sessions. The final capstone simulation will be conducted remotely.

**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.For the first class, please come prepared to speak briefly (one-two 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...](http://www.rackham.umich.edu/current-students/policies/academic-policies/section11#112)

**Course Grading:** Due to the impact of COVID on the upcoming semester, we have made adjustments in grading criteria which are captured below.This class requires five graded assignments~~:~~ three two-three page memos; one panel discussion; and one simulation that will involve role-playing different corporate-executive or federal-executive perspectives.In addition, another aspect of the course that will be graded is class participation, which 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 (in-person or virtual) is required for the simulation on 7 December, and failure to attend will significantly impact the grade***.

Class participation and engagement                     10%

    Policy Memos (15% x 3) 45%

Panel Discussion (x1)                    25%

Policy Simulation (x1) 20%

100%

*Class Participation and engagement:* Given the impact of COVID, we will not take conventional attendance since some students may be unable to participate at the regular class time and will watch recorded sessions afterwards. As a result, students will turn in a **total of ten one-page evaluations for one assigned reading from classes 2 through 12** that in total will account for the ten percent component for class participation (1% for each reading evaluation x 10=10%). Each reading evaluation is due within 24 hours after the end of class via email to Professors Ali or Landwehr or posted in Canvass. The evaluations will not be graded.

*Policy Memos:* Three policy memos (two to three pages each) are required for this component, with due dates of 28 September, 19 October, and 9 November; each will comprise 15% with all three equaling 45% 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).** S*tudents 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 academic periodicals; national security policy and research organization websites; 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 Attack Impact
  + Corporate Topic: Review in depth a significant corporate cybersecurity incident, review in depth and 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, 2016 Equifax breach; and the 2017 Wannacry attacks.

* + National Security topic: Review in depth a significant government cybersecurity incident; review in depth and 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 Critical Infrastructure
  + Corporate topic: Outline the corporate view of a privately owned critical infrastructure element for a corporation operating in a particular industry (banking, elections, phone, power, water, nuclear energy, aviation, etc.) in the United States. What different technological systems and methods are used, what cybersecurity gaps or vulnerabilities exist, and what tradeoffs must be considered?
  + National Security topic: Outline the federal approach to a key critical infrastructure element, which departments and agencies have lead roles, and identify one recommended course of action to address current cybersecurity gaps and vulnerabilities. How should government relate to privately-owned assets in the sector?
* Policy Memo #3 Future Scenarios
  + Corporate topic: Identify a future technology that could provide enhanced cybersecurity benefits to a Fortune 500 CEO, evaluate the pros/cons of a chosen approach, and deliver a bottom-line recommendation.
  + National Security topic: 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 and potential pros and cons of each to prevent it from occurring.

*Student Panels*: Five one-hour student panels will be convened during the term. Each panel will develop a topic from an assigned policy area, such as law enforcement access to communications, technology for public elections, cybersecurity regulation, cyberwarfare, AI/ML fairness, etc. Each will have up to 8 student participants (will depend on class size). Each participant will be assigned to represent a particular organization and/or viewpoint (e.g. industry group, political party, public interest lobby, NGO, etc.) on a specified policy issue (e.g. legislative proposal, regulatory proposal, national strategy) relative to the panel's topic area. The non-participants in a panel will be the audience and will be required to propose questions for the panelists. Policy positions and student questions must take account of relevant underlying technologies and technical issues covered during the course.

Timing: Panelists will have 5 minutes each to present their positions. Instructors will then pose questions to the panelists based on student submissions and other sources.

Grading: Students will be evaluated on their oral presentation skills, adherence to the recommended presentation format, and research and preparation for their overall assessment. Following the panel presentations, other students in class will engage in a question and answer session with the assembled student panel. Approximately 20% of this grade will be determined by the student’s performance on their assigned panel and 5% (4 panels x 1.25%) will be based on participation as audience members of the non-assigned panels. As an audience member, each student will submit in advance to Professors Landwehr and Ali one or more questions addressed to the panelists. Those questions will account for the 1.25% of the grade for the panels in which they are not active participants.

*Policy Simulations:* Students will have the choice of participating in one of two different simulated policy meetings dealing with a cybersecurity crisis scenario that will be conducted during the 7 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*, Third Edition, John Wiley. Assigned sections will be made available on Canvas.

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

National Security Bibliography

# Buchanan, B. *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*. First Edition, London: Oxford University Press. 2017.

# Buchanan, B. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. First Edition, Boston: Harvard University Press. 2020.

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

Clarke, R and Knake R. *The Fifth Domain: Defending our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. First Edition, New York: Penguin Press. 2019.

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>

Greenberg, A. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers*. First Edition, New York: Doubleday. 2019.

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

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

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

Maurer, T. *Cyber Mercenaries: The State, Hackers, and Power*. First Edition, Boston: Cambridge University Press. 2018.

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

Scheier, B. *Data and Goliath*. First Edition, New York: W. W. Norton and Company. 2015.

Shimer, D. Rigged: *America, Russia, and One Hundred Years of Covert Electoral Interference*. First Edition, New York: Alfred A Knopf. 2020.

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

Singer, P.W. and Brooking, E. *Like War: The Weaponization of Social Media*. First Edition, New York: Houghton Mifflin Harcourt. 2018.

Rid, T. Active Measures: *The Secret History of Disinformation and Political Warfare. First Edition*, New York: Farrar, Straus, and Giroux. 2020.

*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>

Valeriano, B, et al. *Cyber Strategy, the Evolving Character of Power and Coercion*. First Edition, London: Oxford University Press. 2018.

Zegart, A and Lin, H. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. First Edition, Washington, DC: Brookings Institution Press. 2019.

**Ford School Public Health Protection Policy:** In order to participate in any in-person aspects of this course, including meeting with other students to study or work on a team project, you must follow all safety measures mandated by the State of Michigan, the University of Michigan and the Ford School. This includes maintaining physical distancing of six feet from others and properly wearing a face covering at all times while on campus. In addition, it is expected that you will protect and enhance the health of everyone in the Ford School community by staying home and following self-isolation guidelines if you are experiencing any symptoms of COVID-19, have been exposed to someone with COVID-19, are awaiting a test result, or have engaged in a higher-exposure activity such a flying or attending an indoor social gathering of more than 10 people.  If you are unable or unwilling to adhere to all prescribed safety measures, you will be accommodated through remote access to all aspects of this course.  Additional information on public health safety measures is described in the [Wolverine Culture of Care](https://campusblueprint.umich.edu/uploads/Wolverine_Culture_of_Care%20sign_8.5x11_UPDATED_071520.pdf) and the [University’s Face Covering Policy for COVID-19](http://ehs.umich.edu/wp-content/uploads/2020/07/U-M-Face-Covering-Policy-for-COVID-19.pdf).

**Ford School 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 impact 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](https://caps.umich.edu/) (CAPS) and/or [University Health Service](https://www.uhs.umich.edu/mentalhealthsvcs) (UHS). For a listing of other mental health resources available on and off campus, visit: <https://uhs.umich.edu/stressresources>

**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)**.**

**SYLLABUS**

**Class 1 – August 31, 2020 Introduction to Cybersecurity**

Guest:(none)

Student Panel: (none)

Summary: Roadmap for the course, procedures, ethics, grading

Technical: What a leader needs to know about computing and cybersecurity technology. Basic computer architecture, digital vs. analog, information, data representation, encryption.

Policy: Overview of US cybersecurity landscape and Executive Branch roles and responsibilities. Introduction to cybersecurity policy and legal evolution.

Assignments: Readings and class questionnaire

*Technical*

Kernighan, *Understanding the Digital World*. pp. 1-52.

*Policy*

Fischer, Eric. “Federal Cybersecurity Roles.” *Congressional Research Service*. 13 Feb 2017. 2 pages.

https://crsreports.congress.gov/product/pdf/IF/IF10602

Norris, Donald, et al. “Cyberattacks at the Grass Roots Level: American Local Governments and the Need for High Levels of Cybersecurity.” *Public Administration Review*. Vol 79, No 6. 2019. 10 pages.

(Instructor will provide .pdf)

Multimedia: (optional)

<https://www.buzzsprout.com/1225250/4976432-blips-and-bytes-a-conversation-with-former-nsa-director-mike-rogers>

**Class 2 - September 14, 2020** **Surveillance, Privacy, and Law Enforcement Access - Technical**

Guest: Barbara McQuade, University of Michigan Law School

<https://www.law.umich.edu/FacultyBio/Pages/FacultyBio.aspx?FacID=bmcquade>

Student Panel: (none)

Summary: Technical: Telephony, digital networking, protocols, cryptography in networks.

Assignments: Readings

*Technical*

Kernighan, *Understanding the Digital World*. Kernighan 119-161 (Communications, Networks, The Internet)

**Class 3 - September 21, 2020 Surveillance, Privacy, and Law Enforcement Access - Policy**

Guest:(none)

Student Panel #1: Privacy and law enforcement access

Summary: Policy: Overview on US surveillance policy and legislation; introduction to policy issues regarding individual privacy in digital age and law enforcement access to communications; examine policy and legal implications of November 2015 San Bernardino and December 2019 Pensacola attacks.

Assignments: Readings

*Policy*

Crowell, Donald. “The Privacy of “Things: How the Stored Communications Act Has Been Outsmarted by Smart Technology.” *Federal Communications Law Journal*. Vol 70, No 2. 2018. 27 pages.

<http://www.fclj.org/wp-content/uploads/2018/08/70.2-Crowell.pdf>

Maras, Marie Helen and Wandt, Adam. “Enabling Mass Surveillance: Data Aggregation in the Age of Big Data and the Internet of Things.” *Journal of Cyber Policy*. Vol 4, No 2. 2019. 19 pages.

(Instructor will provide .pdf)

Morrison, Carren. “Private Actors, Corporate Data, and National Security: What Assistance Do Tech Companies Owe Law Enforcement?” *William & Mary Bill of Rights Journal*, Vol 26, No 2. 2017. 31 pages.

(Instructor will provide .pdf)

**Class 4 - September 28, 2020 Cybersecurity Aspects of Elections – Technical (Policy Memo #1 due)**

Guest:Jeremy Epstein, National Science Foundation

Student Panel (none)

Summary: Technical: Algorithms, programs, vulnerabilities. Overview of election system technical architectures.

Assignments: Readings

*Technical*

Kernighan, pp. 53-86 (Part II Software, Chapters 4 and 5)

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 Chapter 3, Voting in the United States, pp. 31-54, and Chapter 5, Assuring the Integrity of Elections, pp. 85-106.

**Class 5 - October 5, 2020 Cybersecurity Aspects of Elections – Policy**

Guest:Thomas Rid, Johns Hopkins University and Richard Clarke, former National Coordinator for Cybersecurity and Homeland Defense

Student Panel #2: Election Security

Summary: Policy: U.S. election system enterprise, impact of 2016 Russian interference, technical and policy recommendations to strengthen election systems.

Assignments: Readings

*Policy*

Graff, Garrett. “8 Big Reasons Election Day 2020 Could be a Disaster.” *Politico.com*. 24 July 2020. 12 pages.

<https://www.politico.com/news/magazine/2020/07/24/2020-election-disaster-perfect-storm-372778>

Manpearl, Eric. “Securing U.S. Election Systems: Designating U.S. Election Systems as Critical Infrastructure and Instituting Election Security Reforms.” *Boston University Journal of Science and Technology Law*, Vol 24, No 1. 2018. 28 pages.

(Instructor will provide .pdf)

Westrope, Andrew. “When Cybersecurity and Democracy Collide: Locking Down Elections.” *Government Technology.com*. October/November 2019. 8 pages.

<https://www.govtech.com/security/Cybersecurity-and-Democracy-Collide-Locking-Down-Elections.html>

Multimedia: (optional)

<https://www.cbsnews.com/news/nsa-cybersecurity-directorates-anne-neuberger-on-protecting-the-elections/>

**Class 6 - October 12, 2020 Cyber System Security – Technical**

Guest:Peter Honeyman, University of Michigan, EECS

Student Panel: (none)

Summary: Technical: Software layering, system software architectures, root of trust, thinking like an attacker.

Assignments: Readings

*Technical*

Kernighan, *Understanding the Digital World*. Kernighan, pp. 87-118, (Chapters 6 and 7 and Wrapup on Software)

**Class 7 - October 19, 2020 Cyber System Security – Policy** **(Policy Memo #2 due)**

Guest:(none)

Student Panel #3: Cybersecurity Regulation: Supply Chain cybersecurity

Summary: Policy: Standards, frameworks, rules, authorities, and legislation regarding cyber aspects of physical system security.

Assignments: Readings

Smith, Don. “Enhancing Cybersecurity in the Energy Sector: a Critical Priority.” *Journal of Energy and Natural Resources Law*. Vol 36, No 3. 2018. 10 pages.

(Instructor will provide .pdf)

Duncan, Susan, et. al. “Cyberbiosecurity: A New Perspective on Protecting US Food and Agricultural System.” *Frontiers in Bioengineering and Biotechnology*. Vol 7, Article 63. March 2019. 7 pages.

(Instructor will provide .pdf)

Taeihagh, Araz and Lim, Hazel Si Min. “Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks.” *Transport Reviews*. Vol 39, No 1. 2019. 27 pages.

(Instructor will provide .pdf)

**Class 8 – October 26, 2020 Cyberwarfare and cyberoperations - Technical**

Guest:Current or former reps from NSA/DHS/FBI; private sector CISO; white hat hacker

Student Panel: (none)

Summary: Technical: How technical vulnerabilities arise and how they are exploited. Social engineering.

Assignments: Readings

*Technical*

Anderson, *Security Engineering, Third Edition*, Chapter 21, Network Attack and Defence.

Supplementary: Van Oorschot, *Computer Security and the Internet*, Chapter 7, Malware.

(instructor will provide pdf)

**Class 9 - November 2, 2020 Cyberwarfare and Cyberoperations - Policy**

Guest:(none)

Student Panel #4: Cyberwarfare concepts: Deterrence in Cyberspace

Summary: Policy: Classic security theory concepts like deterrence, retaliation, and attribution from a cybersecurity perspective; overview of different attack methods, capabilities, and adversary intentions; legal authorities and international law.

Assignments: Readings

Alexander, Keith and Jaffer, Jamal. “Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition.” *Georgetown Journal of International Affairs*. Vol 18. Fall 2018. 17 pages.

(Instructor will provide .pdf)

*Cyberspace Solarium Commission – Executive Summary*. March 2020. 22 pages.

(Instructor will provide .pdf)

Ferrell, Henry and Glaser, Charles. “Chapter 3 - How Effects, Saliencies, and Norms Should Influence U.S. Cyberwar Doctrine.” *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. First Edition, Washington, DC: Brookings Institution Press. 2019. 36 pages.

(Instructor will provide .pdf)

Multimedia: (optional)

<https://www.buzzsprout.com/1225250/4757903-election-security-and-cyber-warfare-with-ellen-nakashima>

**Class 10 – November 9, 2020 Artificial Intelligence – Technical (Policy Memo #3 due)**

Guest:Patrick McDaniel, Penn State University

Student Panel: (none)

Summary:Technical: basics of artificial intelligence/machine learning, adversarial learning. More on differential privacy.

Assignments: Readings

*Technical*

Bita Darvish Rouhani, Mohammad Samragh, Tara Javidi, and Farinaz Koushanfar, "Safe Machine Learning and Defeating Adversarial Attacks," *IEEE Security & Privacy Magazine*, March/April 2019 pp. 31-38. (instructor will provide pdf)

Ian Goodfellow, Patrick McDaniel, Nicolas Papernot. "Making machine learning robust against adversarial inputs," *Communications of the ACM, vol. 61*, No. 7 (July 2018) pp. 56-66. (instructor will provide pdf)

**Class 11 - November 16, 2020 Artificial Intelligence - Policy**

Guest:(none)

Student Panel #5: Artificial intelligence

Summary:Policy: AI in national security domains (intelligence, surveillance, battlefield weaponry; federal approaches to AI (DoD, IC, Law enforcement, Congress); National AI Commission.

Assignments: Readings

*Policy*

Calo, Ryan. “Artificial Intelligence Policy: A Primer.” *University of Washington School of La*w. 8 August 2017. 28 pages.

(Instructor will provide .pdf)

Johnson, James. “The AI-Cyber Nexus: Implications for Military Escalation, Deterrence, and Strategic Stability.” *Journal of Cyber Policy*. Vol 4, No 3. 2019. 20 pages.

(Instructor will provide .pdf)

Scharre, Paul. “Killer Apps – The Real Dangers of an AI Arms Race.” *Foreign Affairs*. May/June 2019. 11 pages.

(Instructor will provide .pdf)

**Class 12 – November 23, 2020 Cybersecurity Futures; Capstone Simulations preparation**

Guests:(none)

Student Panel: (none)

Summary:Combined technical and policydiscussion regarding future issues.

Assignments: Readings and Prepare for Capstone simulations (on 7 December)

# Ferrante, Anthony. “2020 cybersecurity predictions: Evolving vulnerabilities on the horizon.” *The Hill.com*. 22 January 2020. 3 pages.

<https://thehill.com/opinion/cybersecurity/479316-2020-cybersecurity-predictions-evolving-vulnerabilities-on-the-horizon>

Kimani, Kenneth, et. al. “Cybersecurity Challenges for IoT-based Smart Grid Networks.” *Journal of Critical Infrastructure Protection*. Vol 25, June 2019. 14 pages. (Instructor will supply .pdf)

**Class 13 – November 30, 2020 Cybersecurity Roundtable; Capstone Simulations preparation**

Guests:National journalists/government experts/private sector executives/academic specialists

Student Panel: (none)

Summary:Roundtable discussion with select cybersecurity experts, student-led question and answer session.

Assignments: Readings and Prepare for Capstone simulations (on 7 December)

Anderson, *Security Engineering*, Third Edition. Chapter 11: Inference Control, pp. 337-361.

TBD

**Class 14 – December 7, 2020 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.