The Graduate School of Political Management

THE GEORGE WASHINGTON UNIVERSITY

M.P.S. in Legislative Affairs
Summer Semester, Frist Session
May 16, 2022 – June 25, 2022

Course Name
Congress and Cybersecurity
LGAF 6263.LH
3 Credits

Mondays and Wednesdays, 6pm – 8pm

Mondays and Wednesdays, 6-8pm
Class Location: **Hall of States, 444 North Capitol Street, NW, Washington, DC 20001**
(check at front desk for class room number each night).

BASIC INFORMATION AND RESOURCES

Instructor
Sean M. Farrell

Contact Information
Phone Number: (301) 437-5437
Email Address: farrell274@hotmail.com

Communication
Email is the best way to maintain contact, and students may expect a response the same day if the message is received prior to 6pm, or by the next morning if the message is received after 6pm. Students may also schedule an appointment – availability will depend on schedule, but Fridays provide greatest flexibility during working hours.

Blackboard Site
A Blackboard course site has been set. Each student is expected to check the site throughout the semester. Students can access the course site at https://blackboard.gwu.edu. Support for Blackboard is available at 202-994-4948, or helpdesk.gwu.edu.

Academic Integrity
All members of the university community are expected to exhibit honesty and competence in their academic work. Students have a special responsibility to acquaint themselves with, and make use of, all proper procedures for doing research, writing papers, and taking exams. Members of the community will be presumed to be familiar with the proper academic procedures and will be held responsible for applying them. Deliberate failure to act in accordance with such procedures will be considered academic dishonesty. Academic dishonesty is defined as "cheating of any kind, including misrepresenting one's own work, taking credit for the work of others without crediting them and without appropriate authorization, and the fabrication of information." Acts of academic dishonesty are a legal, moral, and intellectual offense against the community and will be prosecuted through the proper university channels. The University Code of Academic Integrity can be found at http://studentconduct.gwu.edu/code-academic-integrity.

University Policy on Observance of Religious Holidays

- Students should notify faculty during the first week of the semester of their intention to be absent from class on their day(s) of religious observance.
- Faculty should extend to these students the courtesy of absence without penalty on such occasions, including permission to make up examinations.
- Faculty who intend to observe a religious holiday should arrange at the beginning of the semester to reschedule missed classes or to make other provisions for their course-related activities

Support for Students with Disabilities
GW's Disability Support Services (DSS) provides and coordinates accommodations and other services for students with a wide variety of disabilities, as well as those temporarily disabled by injury or illness. Accommodations are available through DSS to facilitate academic access for students with disabilities. Please notify your instructor if you require accommodations. Additional information is available at http://disabilitysupport.gwu.edu/.

Title IX: Confidentiality and Responsible Employee Statement
The George Washington University (GWU) and its faculty are committed to helping create a safe and open learning environment for all students. If you (or someone you know) have experienced any form of sexual misconduct, including sexual assault, dating or domestic violence, or stalking, know that help and support are available. GWU strongly encourages all members of the community to take action, seek support and report incidents of sexual misconduct to the Title IX Office. Please be aware that under Title IX of the Education Amendments of 1972, faculty members are required to disclose information about such misconduct to the Title IX Office.

If you wish to speak to a confidential employee who does not have this reporting responsibility, you can contact Mental Health Services through Colonial Health (counselors are available 24/7 at 202-994-5300 or you can make an appointment to see a counselor in person.). For more information about reporting options and resources at GWU and the community, please visit https://haven.gwu.edu/.

In the Event of an Emergency or Crisis during Class
If we experience an emergency during class time, we will try to stay at this location until we hear that we can move about safely. If we have to evacuate, we will meet at **the Lower Senate Park (across the street and up one block from the Hall of States) at the intersection of D Street, NE, and Delaware Avenue, NE,** in order to account for everyone and to make certain that everyone is safe. Please refer to Campus Advisories for the latest information on the University's operating status: http://www.campusadvisories.gwu.edu/.

Attendance Policy
Attendance is mandatory and will be taken every day at the start of class, 6pm Mondays and Wednesdays from May 16 – June 22, 2022. Tardiness and unexcused absences will impact a student's participation grade, which accounts for **25 percent** of the course evaluation. Absences will be excused only in verified circumstances of family emergencies, work issues, or medical emergencies if notice is provided in advance.

Out-of-Class/Independent Learning Expectation
Over the course of the semester, students will spend at least 4 hours (240 minutes) per week in class. Required reading for the class meetings, written assignments, and presentation preparation are expected to take up, on average, 8 hours (480 minutes) per week. Over the course of the semester, students will spend 20 hours in instructional time and 40 hours preparing for class.

Course Evaluation
At the end of the semester, students will be given the opportunity to evaluate the course through GW's online course evaluation system. It is very important that you take the time to complete an evaluation. Students are also encouraged to provide feedback throughout the course of the semester by contacting any/all of the following:

Dr. Casey Burgat
Director, Legislative Affairs Program
cburgat@gwu.edu | 202-994-6000

Suzanne Farrand
Assistant Dean of Students, GSPM
sfarrand@gwu.edu | 202-994-9309

THE COURSE

Legislative Affairs Program Objectives

Upon completion of the Master's degree in Legislative Affairs, students will:

1. Gain both theoretical and practical knowledge related to the United States Congress, general issues in the legislative arena, and how to effectively advance legislation;
2. Hone their oral and written communication skills in both theoretical and technical aspects of legislative affairs;
3. Be able to conduct cutting-edge research and engage in effective problem solving by learning critical thinking skills; and
4. Learn how to work effectively with others, the value of collaborative work, and will understand ethical issues involved in the legislative arena.

Graduate School Expectations

Students enrolled in a graduate program should take their academic responsibilities seriously and be prepared to meet the following expectations:

1. Utilize effective time management skills so as to complete and submit their assignments on their required due dates and times.
2. Have attained a mastery of written communication skills including proper sentence structure, grammar, spelling, and word usage.
3. Understand how to properly format in-text citations and references for resources and information integrated into their written assignments.

Course Description and Overview

Advancements in information and communications technology have formed an online world of networked computers colloquially referred to as "cyberspace." The advancements that enable cyberspace provide enormous efficiencies and opportunities for continued innovation across all sectors of the economy, and government. Reliance on this technology also presents grave challenges as varied actors exploit vulnerabilities in the underlying cyber infrastructure to steal information and money, disrupt essential services, or augment military capabilities. Ensuring the security of cyberspace is a critical and growing challenge, and one of the most hotly debated areas of public policy. This course will present students with key concepts behind the evolution of United States cybersecurity law and policy, and equip students to think strategically about cybersecurity as new opportunities and challenges emerge.

Course Learning Objectives

This course will contribute to students' ability to be effective participants in the development, implementation, and assessment of sound public policy. The skills acquired will be applicable to work in the private, non-profit, government, or multilateral sectors.

Students are not expected to be cybersecurity subject matter experts or have a background in computer programming. The objective is for students, upon completion of the course, to have sufficient knowledge to effectively communicate cybersecurity's evolution and key concepts, as well as the contemporary public policy debates that surround it.

To accomplish this, students will be provided at the outset of class with a glossary of the technical terminology they will encounter in course materials. The true value of this seminar, however, is to supplement technical information and relevant statutory language with their real-world implications. To achieve this, students will need to think critically about cybersecurity and analyze it from the political, economic, social, scientific, and strategic perspectives.

Students will acquire the skills to evaluate and represent different sides of cyber public policy questions; to understand the larger dynamics driving the cyber debate; to develop the ability to analyze course readings – including theoretical literature – and articulate their central elements; to distill complex matters into succinct professional memoranda; and to make presentations to the class on assigned topics and engage with their fellow students.

Course Readings

Students may keep up with all readings, but are **ONLY** responsible for **one or two readings per class**, on an alternating basis (assigned alphabetically by surname). Specifically, students will be required to present (*no more than five minutes*) a summary of their assigned readings to the class and the reading's relation to cybersecurity. Presentations should not be "book reports", but rather analyses of the readings. The Professor will upload a spreadsheet to Blackboard of assigned readings for the course (*NOTE*: you may need to scroll down the spreadsheet to find your assigned reading).

Evaluation and Grading

Assignment	Parameters	Due Date	Weight
Assignment #1: Congressional Hearing Summary Relevant to Cybersecurity	**Students must select a congressional hearing:** After Class 1, held on Monday, May 16, 2022 – NOT BEFORE – students must select a congressional hearing (House or Senate) on some aspect of cybersecurity held from the 112th Congress onward (effectively, the last 10 years), and write up a memo summarizing the hearing. **Selections must be finalized by COB Friday, May 27, 2022**. The hearing summary must include: • Which committee; • Date/time/location of the hearing; • Which representatives/senators attended; • Witnesses; • A summary of witness testimony;	Assignment #1 due at start of class Wednesday, **6/1/22**	35%

	• A summary of the chairman/ranking member's opening statement; • A summary of questions asked by each representative/senator in attendance, and witness answers to such questions; • Any closing statements by chairman/ranking member; and • Any links to online information used. [*Students **may** include questions for the record (QFRs), answers to QFRs, and any other material submitted for the record*] Students' selection of a hearing (not a markup) granted on a **first come, first serve basis – no two students may do the same hearing.** This assignment is an exercise in straight reporting – no editorializing!!! This paper should be no more than 5 pages (2,200 words maximum) with 1-inch margins, Times-New Roman font, using 1.5 spacing. <u>Please put your name and email at the end of the paper.</u>		
Op-Ed for a Member of the Senate	**Students may select one of the two options, (a) or (b), below for Assignment #2:** (a) You are the cybersecurity policy advisor for a United States Senator that was not a member of the Senate when it held a vote to invoke cloture on S.3414, the Cybersecurity Act introduced by Senators Joseph Lieberman (I-CT) and Susan Collins (R-ME). The hotly debated cloture vote occurred on August 2, 2012. This was a real debate, about a real bill, with real world implications, but your senator is fictional. Almost ten years have passed since that vote, and your senator wants to lay out a leadership position on whether the federal government should have a stronger role in mandating cybersecurity standards for private companies. You must write a long op-ed for your	Assignment due at start of class Wednesday, **6/23/22**	40%

	fictional senator that succinctly explains the context of the debate that occurred in 2012, and the position – for or against – your senator is taking now regarding government-mandated standards. Specifically, what are the pros and cons of federally mandated cybersecurity standards? What are the pros and cons of voluntary information sharing of cyber threats? How did Congress resolve these questions, and what is the position of your fictional senator today? (b) You are the cybersecurity policy advisor for a United States Senator that is interested in the ambiguities that make deterrence so challenging in cyberspace. Considering recent legislation, such as the fiscal year 2019 National Defense Authorization Act (Sec.1636, Sec.1652) and the recent Cyberspace Solarium Commission report, you must write a long op-ed for your fictional senator that examines the pros and cons of offensive cyber operations, or "defense-forward," and how this strategy relates to deterrence. Specifically, is it possible to have an effective deterrent without the threat of retaliation, and how does one retaliate given the difficulties of attribution, predictable response, and counterforce options in cyberspace? This is a real, challenging, and ongoing policy debate, but your senator is fictional. ***NOTE***: regardless of your choice between (a) or (b), an op-ed should appeal to a broad audience (i.e. be easy to read), and be no more than 5 pages (2,200 words maximum) with 1-inch margins, Times-New Roman font, using 1.5 spacing. Please put your name and email at the end of the paper.		

Attendance and Participation	Every student will be required to make presentations (*no more than 5 minutes*) of course readings to the class on an alphabetically (surname) rotating basis. The number of readings per class never exceed 20, and the number of pages per reading varies from several pages to +100 pages; average around 20-30 pages per reading. The professor will upload a spreadsheet to Blackboard of student reading assignments. *NOTE*: Given time constraints, not every student will necessarily give a presentation, but all students should be prepared to give a presentation. Presentations should not be "book reports," but rather analyses of the readings. As such, participation and attendance counts for **one quarter of the final grade!**	The professor will select **randomly** from the course readings of a given class – **BE PREPARED!**	25%
Total			**100%**

Following is the grade scale for all GSPM classes:

Grade*		**Grading Standard**
A	94-100	Your work is outstanding and ready for submission in a professional environment. Your material, effort, research, and writing demonstrate superior work.
A-	90-93	Represents solid work with minor errors. Overall, excellent work.
B+	87-89	Very good. Represents well-written material, research, and presentation, but needs some minor work.
B	83-86	Satisfactory work, but needs reworking and more effort. Note that although not a failing grade, at the graduate level, anything below a "B" is viewed as unacceptable.
B-	80-82	You've completed the assignment, but you are not meeting all of the requirements.
C+	77-79	Needs improvement in content and in effort. Shows some motivation and concern.
C	73-76	Needs reworking, improved effort, and additional research. Shows minimal motivation and concern.
C-	70-72 (lowest grade to pass)	Poor performance. Major errors, too many misspellings, problems with accuracy, etc.
F	Below 70	Unacceptable performance, or inability to submit the assignment.

*Please note that you may be penalized for late submission of assignment(s).

Required Text and Learning Materials
Most readings will be available on Blackboard or via a link in the syllaubs, but students will be encouraged to purchase two books for this class:

- Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, a division of Simon & Schuster (1989, 1990).

  NOTE: This book remains relevant because it covers so many aspects of cybersecurity, from computer protection and adversary tracing to global network architectures and computer forensics, as well as concepts relevant to the scientific method. While technology improved in the 30 years since the book's publication, the concepts remain relevant. Students are expected to read this throughout the course of the semester and draw on it for class discussions.

- William Strunk, Jr., and E.B. White, *The Elements of Style*, 4th Ed., Pearson Education, Inc. (1979, 2000).

  NOTE: Good writing is paramount in a professional environment. Good writing should be concise and grammatically correct. Strunk & White should be utilized by students to achieve clear prose, and it may be kept as a reference for good writing as careers progress.

Tentative Course Calendar*

*The instructor reserves the right to alter course content and/or adjust the pace to accommodate class progress. Students are responsible for keeping up with all adjustments to the course calendar.

Week 1

***NOTE*: The professor will upload a spreadsheet to Blackboard of student reading assignments.**

Class 1, Monday, May 16, 2022
Course Introduction and Overview: What is "Cyber"?

This class will introduce students to the course, including the syllabus, class readings and assignments, as well as publicly available class resources. Questions students should consider as they do these readings include: What are the pros and cons theory and practice? What are the pros and cons of specialists and generalists? What role does Congress play in setting federal policy in regard to cybersecurity? Is cybersecurity a partisan issue? What are the pros and cons of liberalism and conservatism? And, finally, a fundamental question for a course entitled "Congress and Cybersecurity":

What is "cyber"?

_____

- Carr, Jeffrey, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed.*, O'Reilly Media, Inc., Chapters 1: Assessing the Problem.
- Constitution of the United States, https://www.senate.gov/civics/constitution_item/constitution.htm.
- CSIS Significant Cyber Incidents Since 2006: some of the broader trends regarding challenges in cyberspace, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents. This timeline records significant cyber incidents since 2006. It focuses on cyber-attacks on government agencies, defense and high tech companies, or economic crime with losses of more than a million dollars.
- Deutscher, Guy, *The Unfolding of Language: An Evolutionary Tour of Mankind's Greatest Invention*, Picador (2005), Introduction.
- Diamond, Jared, *Guns, Germs, and Steel*, W.W. Norton & Company (1997), Chapter 10, Spacious Skies and Tilted Axes.
- Fuller, JFC, *Armament & History: The Influence of Armament on History from the Dawn of Classical Warfare to the End of the Cold War*, Da Capo Press, New York (1945, 1998 ed.), excerpts.
- Gleick, James, *The Information: A History, A Theory, A Flood*, Vintage Books, a division of Random House (2011), Prologue.

- Glossary of Cybersecurity Terminology, National Initiative for Cybersecurity Careers and Studies (NICCS), Official website of Cybersecurity and Infrastructure Security Agency (CISA), https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.
- https://library.gwu.edu/, the George Washington University Library.
- https://uscode.house.gov/, The United States Code is a consolidation and codification by subject matter of the general laws of the United States. It is prepared by the Office of the Law Revision Counsel of the United States House of Representatives.
- https://www.congress.gov/, presented by the Library of Congress, congress.gov is the official website for US federal legislative information.
- https://www.govinfo.gov/app/collection/cfr, The Code of Federal Regulations (CFR) annual edition is the codification of the general and permanent rules published in the Federal Register by departments and agencies of the Federal Government. It is divided into 50 titles that represent broad areas subject to Federal regulation.
- Judges, Chapters 6 – 7, Colloquially "Gideon's Night Attack," *The New American Bible*, Saint Joseph Edition (1986).
- Libicki, Martin, "The Convergence of Information Warfare," *Strategic Studies Quarterly*, Vol.11, No.1 (Spring 2017).
- Mukherjee, Siddhartha, *The Gene: An Intimate History,* Scribner, an Imprint of Simon & Schuster, Inc. (2016), Excerpts.
- Ong, Walter, "Look Upon my Works," *Lapham's Quarterly*, Vol. XIV, No.1 (Winter 2021), excerpted from *Orality and Literacy: The Technologizing of the World* (1982).
- *The Associated Press Stylebook*, 55th ed., Hachette Book Group (2020), Excerpts.
- *The Chicago Manual of Style* Online, https://www.chicagomanualofstyle.org/home.html
- The US Government Publishing Office Style Manual, https://www.govinfo.gov/collection/gpo-style-manual.
- Wiener, Norbert, *Cybernetics or Control and Communications in the Animal and the Machine*, The Massachusetts Institute of Technology (1948), Introduction, pages 7-39.

***NOTE*: Upon conclusion of class, students may begin submitting requests for a congressional hearing they want to summarize for assignment #1.**

Hearing selections granted on a first come, first serve basis – no two students may cover the same hearing.

Students have until COB Friday, May 27, 2022, to finalize their selection.

Class 2, Wednesday, May 18, 2022
Telecom 101: The Foundations of Contemporary Information and Communications Technology, and Their Weaknesses

This class will focus on the foundations of modern information and communications technology, including some of the history, technical literature, and regulatory governance, as well as inherent vulnerabilities. Questions students should consider as they do these readings include: Does the reading address the transmission of information, how information is transmitted and received? Does the reading address the storage or processing of information?

- Black, Jr., William, "Thinking Out Loud About Cyberspace," *Cryptolog* (U) (Spring 1997).
- Blum, Andrew, *Tubes: A Journey to the Center of the Internet*, Excerpts.
- Bruning, Deonne, "The Telecommunications Act of 1996: The Challenge of Competition," *Creighton Law Review*, Vol.30 (1997).
- Gertner, Jon, *The Idea Factory: Bell Labs and the Great Age of American Innovation*, Penguin Books (2012), Chapters 1 and 2.
- Gertner, Jon, *The Idea Factory: Bell Labs and the Great Age of American Innovation*, Penguin Books (2012), Chapter 3: System.
- Gleick, James, *The Information: A History, A Theory, A Flood*, Vintage Books, a division of Random House (2011), Chapter 7: Information Theory.
- Kingsbury, N.C., Vice President, American Telephone and Telegraph Company, Letter to the Attorney General, a.k.a. the Kingsbury Commitment (1913); and Brian Fung, "This 100-year-old deal birthed the modern phone system. And it's all about to end," the *Washington Post* (December 19, 2013).
- Kippenhahn, Rudolf, *Code Breaking: A History and Exploration,* Overlook Duckworth, Peter Mayer Publishers, Inc., New York and London (2012), Chapter 2: Hidden Messages and Code Books.
- Martin, James, *Telecommunications and the Computer, 3rd ed.*, Prentice-Hall, a division of Simon & Schuster, Englewood Cliffs, NJ (1976, 1990), Chapter 16: Digital Revolution.
- Martin, James, *Telecommunications and the Computer, 3rd ed.*, Prentice-Hall, a division of Simon & Schuster, Englewood Cliffs, NJ (1976, 1990), Chatper 11: Transmission Media.
- Mitnick, Kevin, with Simon, William, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Little Brown & Company (2011), Excerpted Chapters vI.
- Mitnick, Kevin, with Simon, William, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Little Brown & Company (2011), Excerpted Chapters vII.
- Moritz, Michael, "Origin Story," *Lapham's Quarterly*, Vol. XIV, No.1 (Winter 2021), excerpted from *The Little Kingdom: The Private Story of Apple Computer* (1984).
- National Security Decision Directive (NSDD-145), *National Policy on Telecommunications and Automated Information System* (U), Washington, DC (September 17, 1984).
- Nuechterlein, Jonathan, and Weiser, Philp, *Digital Crossroads: Telecommunications Law and Policy in the Internet Age*, 2nd ed., MIT Press, Cambridge (2013), Preface, Introduction, Chapter 1: The Big Picture.

- Nuechterlein, Jonathan, and Weiser, Philp, *Digital Crossroads: Telecommunications Law and Policy in the Internet Age*, 2nd ed., MIT Press, Cambridge (2013), Preface, Introduction, Chapter 3: The Spectrum.
- Robert Buderi, *The Invention that Changed the World: How a Small Group of Radar Pioneers Won the Second World War and Launched a Technical Revolution,* Simon & Schuster (1996), Chapters 1 & 2.
- Rosenbaum, Ron, "Secrets of the Little Blue Box," *Esquire* (1971), reprinted with permission from the author: http://www.slate.com/articles/technology/the_spectator/2011/10/the_article_that_inspired_steve_jobs_secrets_of_the_little_blue_.html.
- Sarkesian ,Sam, Williams, John Allen, and Cimbala, Stephen, *US National Security: Policymakers, Processes & Politics, 4th ed*., Lynn Rienner Publishers (2008), Chapter 11: Empowering the People.
- Van Crevald, Martin, *Technology and War: From 2000 B.C. to the Present*, Excerpts.

Week 2

Class 3, Monday, May 23, 2022
What is "Science"?

This class will focus on understanding the meaning of science. On Capitol Hill, in the media, and among private groups, many will invoke the word "science" in support of their arguments. Questions students should consider as they do these readings include: What is science? How does one demarcate science from non-science? Is the differentiation between science and non-science an example of information processing? What is information processing? Does science have anything to do with cybersecurity? How has science contributed to modern technology? Is science analogous to strategy, why or why not?

- Cohen, Eliot and Gooch, John, *Military Misfortunes: The Anatomy of Failure in War*, Free Press, a Division of Simon & Schuster, Inc. (1990), Chapter 4: Failure to Learn: American Antisubmarine Warfare in 1942.
- Deutscher, Guy, *The Unfolding of Language: An Evolutionary Tour of Mankind's Greatest Invention*, Picador (2005), Appendix E.
- Gell-Mann, Murray, *The Quark and the Jaguar: Adventures in the Simple and the Complex*, Henry Hold and Company, LLC (1994), Chapter 3: Information and Crude Complexity.
- Gertner, Jon, *The Idea Factory: Bell Labs and the Great Age of American Innovation* Penguin Books (2012), Chapter 5: Solid State.
- Harari, Yuval Noah, *Sapiens: A Brief History of Humankind*, HarperCollins Publishers (2015), Chapter 14: The Discovery of Ignorance.

- Hastings, Max, *The Korean War*, Simon & Schuster Paperbacks (1987), Chapter 13: The Intelligence War.
- Hoddeson, Lillian, and Riordan, Michael, *Crystal Fire: The Birth of the Information Age*, W.W. Norton & Company (1997), Excerpts.
- Karl Popper, Stanford Encyclopedia of Philosophy, https://plato.stanford.edu/entries/popper/.
- Kay, John, and King, Mervin, *Radical Uncertainty: Decision-Making Beyond the Numbers*, W.W. Norton & Company (2020), Preface & Chapter 1: The Unknowable Future.
- Lynn-Jones, Sean, "Preface," *Rational Choice and Security Studies: Stephen Walt and His Critics*, Michael E. Brown, Owen Coté, Jr., Sean Lynn-Jones, and Steven Miller, editors, MIT Press, Cambridge (1999).
- Popper, Karl, *The Logic of Scientific Discovery*, Routledge Classics (1959, 2002), Excerpts.
- Price, Alfred, *Instruments of Darkness: The History of Electronic Warfare 1939 – 1945*, Greenhill Books (1977, 2017), Chapter 11: In Support of the Invasion.
- Price, Alfred, *Instruments of Darkness: The History of Electronic Warfare 1939 – 1945*, Greenhill Books (1977, 2017), Chapter 3: Discovery.
- Roche, James, and Watts, Barry, "Choosing Analytical Measures," *Journal of Strategic Studies*, June 1991, Vol.14, No.2, pp. 165-209.
- Seth, Anil, "Our Inner Universes: Reality is Constructed by the Brain, and No Two Brains are Exactly Alike," *Scientific American* (Fall 2020).
- Simon, Herbert, "Rational Choice and the Structure of the Environment," *Psychological Review*, Vol.63, No.2 (1956).
- Smolin, Lee, *The Trouble with Physics: The Rise of String Theory, the Fall of Science, and What Comes Next,* First Mariner Books (2007), Excerpts.
- Van Evera, Stephen, *Guide to Methods for Students of Political Science*, Cornell University Press (1997), Excerpts from Chapter 1.
- Warner, Edward, "Douhet, Mitchell, Seversky: Theories of Air Warfare," from *Makers of Modern Strategy: Military Thoughts from Machiavelli to Hitler*, Edward Mead Earle, editor, Princeton University Press (1943, 1971).
- Westwick, Peter, *Stealth: The Secret Contest to Invent Invisible Aircraft*, Oxford University Press (2020), Chapter 4: Tin Shed in a Hurricane.

Class 4, Wednesday, May 25, 2022
Telecom 202: Information Technology and the Revolution in Military Affairs

This class will focus on the evolution and application of information technologies to warfare, described by some analysts as revolutionary. What are the advantages and disadvantages of applying information technologies to military force? Is the revolution in military affairs nascent, ongoing, complete, or even attainable? What are revolutions? What are the catalysts and impediments to organizational changes that permit or resist revolutions? How does Thomas Kuhn's view of scientific revolutions contrast with that of Karl Popper? What is science, and what does it have to do with technological applications to military force? How is information applied to military activities? Are science and strategy analogous to one another?

- Government Accountability Office, Testimony Before the Permanent Subcommittee on Investigations, Committee on Governmental Affairs, US Senate, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risk," (May 22, 1996).
- Halabi, Sam, with McPherson, Danny, *Internet Routing Architectures*, 2nd ed., Cisco Press (2000), Chapter 1.
- Harris, Shane, *@ War: The Rise of the Military-Internet Complex*, First Mariner Books (2015), Prologue & Chapter 1: The First Cyber War.
- Johnson, Chalmers, *Revolutionary Change, 2nd Edition*, Stanford University Press (1982), Excerpts from Chapters 3 & 4.
- Kaplan, Fred, *Dark Terriroty: The Secret History of Cyber War*, Simon & Schuster (2016), Chapter 7: Deny, Exploit, Corrupt, Destroy.
- Kaplan, Fred, *Dark Terriroty: The Secret History of Cyber War*, Simon & Schuster (2016), Chapter 4: Eligible Receiver.
- Kotter, John, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review*, Mar-April 1995.
- Krepinevich, Andrew, and Watts, Barry, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy,* Basic Books, New York (2015), Chapter 8: The Military Revolution 1991-2000.
- Kuhn, Thomas, *Structure of Scientific Revolutions*, University of Chicago Press (1962), Excerpts.
- Mahnken, Thomas, *Technology and the American Way of War Since 1945*, Columbia University Press (2008), Chapter 3: Technology and the War in Vietnam.
- Mahnken, Thomas, *Technology and the American Way of War Since 1945*, Chapters 4, 5, and Conclusion.
- Marshall, Andrew, "Some Thoughts on Military Revolutions – Second Version," OSD/NA memorandum for the record, August 23, 1993.
- Martin, James, *Telecommunications and the Computer, 3rd ed.*, Prentice-Hall, a division of Simon & Schuster, Englewood Cliffs, NJ (1976, 1990), Chapter 4: Systems that Use Data Transmission.
- Pollack, Kenneth, *The Threatening Storm: The Case for Invading Iraq*, Random House (2002), Excerpts from Chapter 10: The Risks of the Afghan Approach.
- Price, Alfred, *War in the Fourth Dimension: US Electronic Warfare, from the Vietnam War to the Present*, Greenhill Books, London (2001), Chapter 20: Information Warfare.

- Price, Alfred, *War in the Fourth Dimension: US Electronic Warfare, from the Vietnam War to the Present*, Greenhill Books, London (2001), Chapter 21: Kosovo.
- Schrage, Michael, "Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency," MIT SSP, May 2003.
- Van Atta, Richard, et al, Transformations and Transitions: DARPA's Role in Fostering an Emerging Revolution in Military Affairs, Volume 1 – Overall Assessment , Alexandria, VA: Institute for Defense Analysis (April 2003).
- Westwick, Peter, *Stealth: The Secret Contest to Invent Invisible Aircraft*, Oxford University Press (2020), Chapters 7 & 9.
- Zimet, Elihu, with Armstrong, Robert, and Daniel, Donald, and Mait, Joseph, "Technology, Transformation, and New Operational Concepts, *Defense Horizons* (Sept 2003).

Week 3

Monday, May 30, 2022

NO CLASS – MEMORIAL DAY

Class 5, Wednesday, June 1, 2022
Telecom 303: The Internet: Globalized Information and Vulnerabilities

***NOTE*: Assignment #1, Committee Memo, Due at START OF CLASS!!!**

This class will highlight more recent developments in the cyber domain, especially in regards to internet usage, its vulnerabilities, and policy debates surrounding both. The class will focus particularly on the debate that evolved from the pitched legislative battle between, on the one hand, Senators Joseph Lieberman (D-CT) and Susan Collins (R-ME) who sponsored the Cybersecurity Act (S.2105), and, on the other hand, a group of Ranking Republican Senators led by John McCain (R-AZ) who sponsored the SECURE IT Act (S.2151). This fight was multifaceted but centered on the question of how best to achieve cybersecurity outcomes in the private sector: government-mandated standards to mitigate vulnerabilities, or voluntary information sharing to mitigate vulnerabilities.

What are the pros and cons of both mandated standards and voluntary information sharing?

Additionally, as Congress debated cybersecurity during this time, the Federal Communications Commission (FCC) was taking contradictory positions on the internet and whether it should classified as an information service under Title I of the Communications Act of 1934, or as a common carrier service under Title II of the Communications Act of 1934.

What are the pros and cons of these contradictory actions by the FCC, and do they have implications from a cyber perspective?

- "The Federal Government's Track Record on Cybersecurity and Critical Infrastructure," a report prepared by the Minority Staff of the Homeland Security and Government Affairs Committee (2014).
- "The Internet of Things (IoT): A New Era of Third-Party Risk," Ponemon Institute, LLC, Sponsored by Shared Assessments (May 2017).
- Berinato, Scott, "Inside Facebook's AI Workshop," *Harvard Business Review Special Issue* (Winter 2021).
- Chertoff, Michael, *Exploding Data: Reclaiming our Cyber Security in the Digital Age*, Grove Press (2018), Chapters 1 & 2.
- Clarke, Richard and Knake, Robert, *Cyber War: The Next Threat to National Security and What to do About It*, HarperCollins Publishers (2010), Introduction, Chapters 1 and 8.
- Kosseff, Jeff, *The Twenty-Six Words that Created the Internet*, Cornell University Press (2019), Introduction.
- Mitnick, Kevin, with Vamosi, Robert, *The Art of Invisibility*, Hachette Book Group (2019), Ch. 1-2.
- Sageman, Marc, *Understanding Terror Networks*, University of Pennsylvania Press (2004), Chapter 5: Social Networks and the Jihad.
- Schneider, Jacquelyn, "A World Without Trust: The Insidious Cyberthreat," *Foreign Affairs* (January/February 2022).
- Secretary Janet Napolitano, US Department of Homeland Security, Statement for the Record, Committee on Homeland Security and Government Affairs Hearing: "Securing America's Future: The Cybersecurity Act of 2012," (February 16, 2012).
- Senator John McCain, Opening Statement, Committee on Homeland Security and Government Affairs Hearing: "Securing America's Future: The Cybersecurity Act of 2012," (February 16, 2012).
- Senator Joseph Lieberman, Chairman, Senate Committee on Homeland Security and Government, Opening Statement, Hearing, "Securing America's Future: The Cybersecurity Act of 2012," (February 16, 2012).
- Shostack, Adam and Stewart, Andrew, *The New School of Information Security*, Pearson Education, Inc. (2008), Chapters 4 and 6.
- The Hon. Thomas Ridge, Chairman, National Security Task Force, US Chamber of Commerce, Statement for the Record, Committee on Homeland Security and Government Affairs Hearing: "Securing America's Future: The Cybersecurity Act of 2012," (February 16, 2012).
- United States Government Accountability Office, Report to Congressional Requesters, "Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation," (March 2021), https://www.gao.gov/assets/720/712946.pdf.
- United States Senate Select Committee on Intelligence Report to Accompany S.754, a bill to Improve Cybersecurity in the United States Through Enhanced Sharing of Information About Cybersecurity Threats, the "Cybersecurity Information Sharing Act," S.Rept.114-32 (4/15/15).
- Various Articles I
- Various Articles II
- Watts, Duncan, *Six Degrees: The Science of a Connected Age*, WW Norton Co. (2002), Preface, Chapter 1, The Connected Age.

- Wheeler, Tom, Chairman, Federal Communications Commission, Statement Regarding Protecting and Promoting the Open Internet, GN Docket No.14-28 (March 12, 2015); and Pai, Ajit, Chairman, Federal Communications Commission, Statement Regarding Restoring Internet Freedom, WC Docket No.17-108 (December 14, 2017).

Week 4

Class 6, Monday, June 6, 2022
What is "Strategy"?

This class will focus on understanding the meaning of strategy. Strategy is as crucial on Capitol Hill as it is on the frontlines of cyber warfare, but strategy is often misunderstood, misapplied, not applied, or just plain wrong. Questions students should consider as they do these readings include: What is strategy? What is grand strategy? What are tactics? What are operations? What are the differences between these concepts? Are strategy and science analogous to one another? What is science? How does Feyerabend's view of science differ from Kuhn and Popper? Does the United States have a cyber-strategy? Is strategy applicable to the cyber domain, why or why not?

- Beyerchen, Alan, "Clausewitz, Nonlinearity and the Unpredictability of War, *International Security*, 17:3 (Winter, 1992).
- Bilalic, Merim, and McLeod, Peter, "Why Good Thoughts Block Better Ones," *Scientific American* (Fall 2020).
- Feyerabend, Paul, *Against Method*, 4th Ed., Verso Books (1975, 2010), Excerpted Chapters.
- Fischhoff, Baruch, "Tough Calls," *Scientific American* (Fall 2020).
- Iansiti, Marco, and Lakhani, Karim, "Competing in the Age of AI," *Harvard Business Review Special Issue* (Winter 2021).
- Krepinevich, Andrew and Watts, Barry, Regaining Strategic Competence, Center for Strategic and Budgetary Assessments (2009).
- Libicki, Martin, "Brandishing Cyberattack Capabilities," RAND Corporation Study (2013), available at: https://www.rand.org/pubs/research_reports/RR175.html
- Mandelbrot, Benoit, and Hudson, Richard, *The (Mis)Behavior of Markets: A Fractal View of Financial Turbulence*, Basic Books, A Member of Perseus Books Group (2004), Excerpts.
- Marshall, Andrew, *Long-Term Competition with the Soviets: A Framework for Strategic Analysis (U)* (Santa Monica, CA: RAND, April 1972), R-862-PR, redacted, pp. iii-52.
- Rittel, Horst, and Webber, Melvin, "Dilemmas is a General Theory of Planning," *Policy Sciences* 4 (1973).
- Lorenz, Edward, *The Essence of Chaos*, the University of Washington Press (1993), Excerpts.
- Rumelt, Richard, *Good Strategy Bad Strategy: The Difference and Why it Matters*, Crown Publishing Group, a division of Random House, Inc. (2011), Excerpts.
- Schelling, Thomas, *Arms and Influence*, Yale University Press (1966), Excerpts.

- Smolin, Lee, *The Trouble with Physics: The Rise of String Theory, the Fall of Science, and What Comes Next,* Chapter 17: What is Science?
- United States of America, Cyberspace Solarium Commission, Washington, DC, (March 2020), Executive Summary: https://www.solarium.gov/
- Von Clausewitz, Carl, *On War*, Michael Howard and Peter Paret, eds., Princeton University Press (1976), Excerpts.
- Wack, Pierre, "Scenarios: Unchartered Waters Ahead," *Harvard Business Review*, No.85516 (Sept/Oct 1985).
- X (George Kennan), "The Sources of Soviet Conduct," *Foreign Affairs* (July 1947), https://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=3&psid=3629
- Gordon, Sue, and Rosenbach, Eric, "America's Cyber-Reckoning: How to Fix a Failing Strategy," *Foreign Affairs* (January/February 2022).
- National Defense Authorization Act, Fiscal Year 2019 (P.L.115-232), Sections 889 and 1632, available at https://www.congress.gov/bill/115th-congress/house-bill/5515/text?q=%7B%22search%22%3A%22National+Defense+AUthorization%22%7D&r=32&s=1.

Class 7, Wednesday, June 8, 2022
Scope of Modern Cyber Threats & Policy Responses – PART I (Hacktivists, Thieves, Iran, N. Korea)

This class will focus broadly on multiple threats in the cyber domain from both state and non-state actors, as well as responses to such threats by the U.S. government. Questions students should consider as they do these readings include: What cyber threats do we face? How effective have policymakers been in mitigating cyber threats? Is there bipartisanship in cyber legislation? What are the prospects for further action?

- "Cost of Cyber Crime Study: Insights on the Security Investments that Make a Difference," Independently conducted by Ponemon Institute LLC and jointly developed by Accenture (2017).
- 2019 Data Breach Investigations Report, Verizon (May 2019).
- Caesar, Ed, "The Incredible Rise of North Korea's Hacking Army," The New Yorker (April 19, 2021), https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army.
- Carr, Jeffrey, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed*., O'Reilly Media, Inc., Chapters 2: Rise of the Nonstate Hacker.
- David Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Crown Publishing Group (2018), Excerpts.
- Eisenbach, Thomas, Kovner, Anna, and Lee, Michael, "Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis," *Federal Reserve Bank of New York Staff Reports*, No.909 (January 2020; revised May 2021).

- Eric Fischer, Cybersecurity Issues and Challenges: In Brief, Congressional Research Service, Washington, DC (August 12, 2016).
- Executive Order 13636, Improving Critical Infrastructure Cybersecurity (2/12/13)
- Harris, Shane, *@ War: The Rise of the Military-Internet Complex*, First Mariner Books (2015), Excerpts.
- Hodgson, Quentin, Ma, Logan, Marcinek, Krystyana, and Schwindt, Karen, "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace," RAND Corporation (2019), Chapters 5 & 6, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2961/RAND_RR2961.pdf.
- Huddleston, Tom, "What is Anonymous? How the Infamous "Hacktivist" Group Went from 4chan Trolling to Launching Cyberattacks on Russia," *CNBC* (March 25, 2022), https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html.
- Majority Staff Report for Chairman Rockefeller, United States Senate Committee on Commerce, Science, and Transportation, "A 'Kill Chain' Analysis of the 2013 Target Data Breach (March 26, 2014).
- Perlroth, Nicole, "In Cyberattack on Saudi Firm, US Sees Iran Firing Back," *New York Times* (October 23, 2012).
- Perlroth, Nicole, and Hardy, Quentin, "Bank Hacking Was the Work of Iranians, Officials Say," New York Times (January 8, 2013).
- Richter, Chris, "Patching: A Growing Challenge and a Needed Discipline," from the *Digital Big Bang: The Hard Tuff, the Soft Stuff, and the Future of Cybersecurity*, Phil Quade, editor, John Wiley & Sons (2019).
- United States Senators Gary Peters (D-MI) and Robert Portman (R-OH), text of "Cyber Incident Reporting Act of 2021," available at: https://www.hsgac.senate.gov/media/majority-media/peters-and-portman-introduce-bipartisan-legislation-requiring-critical-infrastructure-entities-to-report-cyber-attacks.
- Tassi, Paul, "How ISIS Terrorists May Have Used Playstation 4 to Discuss and Plan Attacks [Updated], *Forbes* (November 14, 2015).
- United States Department of Justice, Indictment of Seven Iranians in Relation to an Extensive Campaign of over 176 days of Distributed Denial of Service (DDoS) attacks, available at: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.
- United States Department of Justice, Indictment of Three North Korean Military Hackers in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe, available at: https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.
- Zetter, Kim, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired* (November 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/,

Week 5

Class 8, Monday, June 13, 2022
Scope of Modern Cyber Threats & Policy Responses – PART II (Russia & China)

This class will continue the broad focus from the previous class on multiple threats in the cyber domain but with a particular focus on Russia and China, as well as responses to such threats by the U.S. government. Questions students should consider as they do these readings include: What cyber threats do we face? How effective have policymakers been in mitigating cyber threats? Is there bipartisanship in cyber legislation? What are the prospects for further action?

- "Russia at the Turn of the Millennium," Vladimir Putin, from Russian Foreign Policy in Transition: Concepts and Realities, Andrei Melville and Tatiana Shakleina, editors, CEU Press (2005).
- 2019 Report to Congress of the US-China Economic and Security Review Commission (November 2019), Executive Summary.
- Defense Science Board Study on 21st Century Military Operations in a Complex Electromagnetic Environment (July 2015), https://dsb.cto.mil/reports/2010s/DSB_SS13--EW_Study.pdf
- Gibney, Elizabeth, "Where is Russia's Cyberwar? Researchers Decipher its Strategy," *Nature* (March 17, 2022), https://www.nature.com/articles/d41586-022-00753-9.
- Hodgson, Quentin, Ma, Logan, Marcinek, Krystyana, and Schwindt, Karen, "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace," RAND Corporation (2019), Chapters 1, 2, 3, and 4, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2961/RAND_RR2961.pdf.
  https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
  https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.
- Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, A report by Chairman Mike Rogers and Ranking Member Dutch Ruppersberger of the Permanent Select Committee on Intelligence, US House of Representatives, 112th Congress (October 8, 2012).
- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed.*, Chapter 11.
- Johnson, Reuben, "Tennis Shoes and Stolen Toilets," *The Weekly Standard* (November 24, 2008).
- Kotkin, Stephen, "American Hustle: What Mueller Found – and Didn't Find – About Trump and Russia," *Foreign Affairs* (July/August 2019).
- Mandiant Report: "APT1: Expsoing One of China's Cyber Espinage Units," (2013), available at:
- Report on the Investigation Into Russian Interference in the 2016 Presidential Election, Volume I of II, Special Counsel Robert S. Mueller, III, Submitted Pursuant to 28 C.F.R. § 600.8(c), Washington, DC (March 2019), Pp 1 – 66.
- Ritchie, Rae, "Maersk: Springing back from a catastrophic cyberattack," *I Global Intelligence for Digital Leaders* (August 2019), https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack.

- Sanger, David, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Crown Publishing Group (2018), Chapter 7: Putin's Petri Dish
- Sanger, David, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Crown Publishing Group (2018), Chapter 5: The China Rules
- The Hon. Eric Rosenbach, Testimony before the Senate Commerce Committee Hearing, "China: Challenges to US Commerce," (March 7, 2019).
- Tse Tung, Mao, translated by Samuel Griffith II, *On Guerrilla Warfare*, University of Illinois Press (1961), Excerpts.
- United States Government Accountability Office, Blogpost, "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response," (April 2021), https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.
- US Chamber of Commerce, Made in China 2025: Global Ambitions Built on Local Protections (2017), https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.
- Zakhoarov, Andrei, and Napalkova, Anastasia, "Why Chinese Farmers Have Crossed Border Into Russia's Far East," *BBC Russian Service* (November 1, 2019), https://www.bbc.com/news/world-europe-50185006.
- Zetter, Kim, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired* (March 3, 2016).

Class 9, Wednesday, June 15, 2022
The United States of America

This class will examine the United States of America, including its history, pivotal documents, and some contemporary challenges in the cyber domain. Questions students should consider as they do these readings include: What are the ideals the United States was founded upon, and how have these ideals shaped the country and its people? Is the concept of American exceptionalism to be embraced or eschewed? Was the so-called "unipolar" moment real or imagined? What, if any, cyber implications exist regarding contemporary partisan politics?

- Charles Mahoney, "Corporate Hackers: Outsourcing US Cyber Capabilities," *Strategic Studies Quarterly*, Vol.15, No.1 (Spring 2021).
- Diane Souvaine, Testimony before the Senate Commerce Committee Hearing, "Research & Innovation: Ensuring America's Economic and Strategic Leadership," (October 22, 2019).
- George Washington, Farewell Address (1796), Randall Adkins, editor, *The Evolution of Political Parties, Campaigns, and Elections: Landmark Documents 1787-2007*, CQ Press (2008).
- Haslam, Bill, *Faithful Presence: The Promise and the Peril of Faith in the Public Square*, Nelson Books (2021), Prologue and Chapter 2: What is Happening Now?
- Jeff Kosseff, *The Twenty-Six Words that Created the Internet*, Cornell University Press (2019), Chapter 7: American Exceptionalism.

- Jefferson, Thomas, as well as Adams, John, Franklin, Benjamin, Livingston, Robert, and Sherman, Roger, Declaration of Independence: A Transcription, available at the National Archives (July 4, 1776), https://www.archives.gov/founding-docs/declaration-transcript.
- John Aldrich, *Why Parties: The Origins and Transformation of Political Parties in America*, University of Chicago Press (1995), Chapter 4.
- King, Martin Luther, Jr., transcript of the "I Have a Dream" Speech" (August, 28, 1963), available from National Public Radio, https://www.npr.org/2010/01/18/122701268/i-have-a-dream-speech-in-its-entirety#:~:text=sisters%20and%20brothers.-,I%20have%20a%20dream%20today.,flesh%20shall%20see%20it%20together..
- Krauthammer, Charles, "The Unipolar Moment," The Washington Post (July 20, 1990), https://www.washingtonpost.com/archive/opinions/1990/07/20/the-unipolar-moment/62867add-2fe9-493f-a0c9-4bfba1ec23bd/.
- Leffler, Melvin, and Jeffrey Legro, *To Lead the World: American Strategy After the Bush Doctrine*, Oxford University Press (2008), Introduction and Chapter 11: Dilemmas of Strategy.
- Maier, Pauline, *Ratification: The People Debate the Constitution 1787-1788*, Simon & Schuster (2010), Introduction & Prologue.
- National Security Council Report, NSC 68, 'United States Objectives and Programs for National Security," April 14, 1950, History and Public Policy Program Digital Archive, US National Archives, Wilson Center Digital Archive: International History Declassified, https://digitalarchive.wilsoncenter.org/document/116191.pdf?v=2699956db534c1821edefa61b8c13ffe.
- Publius (Hamilton & Madison, respectively), The Federalist Papers No.9, "The Union as a Safeguard Against Domestic Faction and Insurrection," and No.10, "The Same Subject Continued," Clinton Rossiter, editor, *The Federalist Papers*, Penguin Group (USA), Inc. (1961, 1999; originally published in 1787).
- Remini, Robert, *A Short History of the United States*, HarperCollins Publishers (2008), Excerpts from Chapter 7: Manifest Destiny, Progressivism, War, and the Roaring Twenties.
- Roitblat, Herbert, *Algorithms Are Not Enough: Creating General Artificial Intelligence*, The MIT Press (2020), Chapters 5: Neural Networks Approach to Artificial Intelligence.
- Sam Sacks, Testimony before the House Energy and Commerce Subcommittee on Communications and Technology Hearing, "Telecommunications, Global Competitiveness, and National Security," (May 16, 2018).
- Shane Harris, *@ War: The Rise of the Military-Internet Complex*, First Mariner Books (2015), Chapter 13.
- Shostack, Adam, and Stewart, Andrew, *The New School of Information Security*, Pearson Education, Inc. (2008), Chapter 3: On Evidence.
- Steve Kroft, "The Data Brokers: Selling Your Personal Information," *60 Minutes* (August 24, 2014).
- Walbank, F.W., Introduction, *Polybius: The Rise of the Roman Empire*, Penguin Books (1979).

Week 6

Monday, June 20, 2022

NO CLASS – Juneteenth DAY

Class 10, Wednesday, June 22, 2022
Artificial Intelligence, Biotechnology, Quantum Technology, and Human Evolution

NOTE: Assignment #2, Op-Ed, Due at START OF CLASS!!!

Humans have been leveraging information and applying technology to assist them since our species evolved – a number of scientific studies illustrate other animals learn techniques and pass along tools and knowledge as well. Questions students should consider as they do these readings include: Are we on the precipice of a new era ushered in by emerging technologies like artificial intelligence, biotechnology, and quantum computing? Are these emerging technologies nothing more than an iterative improvement in tools that can be traced back to the earliest days of humanity? What is the role of the United States Congress in answering these questions?

- Babic, Boris, Cohen, I. Glenn, Evgeniou, Theodoros, and Gerke, Sara, "When Machine Learning Goes Off the Rails," *Harvard Business Review Special Issue* (Winter 2021).
- Copeland, Jack, and Proudfoot, Diane, "Our Posthuman Future," *The Philosophers' Magazine*, Issue 57 (2nd Quarter 2012).
- Giles, Martin, "Explainer: What is Quantum Communication?" MIT Technology Review (February 14, 2019), https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/.
- Harari, Yuval Noah, *Sapiens: A Brief History of Humankind*, HarperCollins Publishers (2015), Timeline of Human History and Chapters 2 & 3.
- Howard, Heidi, van El, Carla, Forzano, Francesca, Radojkovic, Dragica, Rial-Sebbag, Emmanuelle, de Wert, Guido, Borry, Pascal, and Cornel, Martina, on behalf of the Public and Professional Policy Committee of the European Society of Human Genetics, "One Small Edit for Humans, One Giant Edit for Humankind? Points and Questions to Consider for a responsible way forward for Gene Editing in Humans," *European Journal of Human Genetics* (November 30, 2017).
- Jiang, Linxing, et al, "BrainNet: A Multi-Person Brain-to-Brain Interface for Direct Collaboration Between Brains," *Nature* (September 2018).
- Kahneman, Daniel, "Maps of Bounded Rationality: A Perspective on Intuitive Judgment and Choice," Noble Prize Lecture, Dec. 8 2002.
- Lindsay, Jon, "Surviving the Quantum Cryptocalypse," *Strategic Studies Quarterly* (Summer 2020).
- Lloyd, Seth, "Quantum-Mechanical Computers: Quantum-Mechanical Computers, if they can be constructed, will do things no ordinary computer can," *Scientific American* (October 1995).
- Lorenz, Konrad, *On Aggression*, Introduction and Chapter 13.

- Metzl, Jamie, *Hacking Darwin: Genetic Engineering and the Future of Humanity*, Sourcebooks (2019), Excerpts.
- Mukherjee, Siddhartha, *The Gene: An Intimate History,* Scribner, an Imprint of Simon & Schuster, Inc. (2016), Excerpts.
- O'Connell, Robert, *Of Arms and Men: A History of War, Weapons, and Aggression*, Oxford University Press, Oxford & New York (1989), Chapter 1: Mechanisms.
- Parker, Edward, "Commercial and Military Applications and Timelines for Quantum Technology," RAND Corporation Study (2021), available at: file:///D:/GW/LGAF6270%20(2022)/Blackboard/Class%2010_AI_Biotech_Quantum_Humans/Parker_Quantum%20Applications_RAND_RRA1482-4.pdf
- Parunak, H. Van Dyke, and Bruechar, Sven, "Engineering Swarming Systems," *Altarum Institute* (2003).
- Robin Fox, "Aggression: Then and Now," in Michael Robinson & Lionel Tiger (eds.), *Man & Beast Revisited*, pp. 81-93.
- Roitblat, Herbert, *Algorithms Are Not Enough: Creating General Artificial Intelligence*, The MIT Press (2020), Chapters 6.
- Sanker, Pamela, and Cho, Mildred, "Engineering Values into Genetic Engineering: A Proposed Analytic Framework for Scientific Social Responsibility," *American Journal of Bioethics* (September 13, 2016).
- Smith, Brad, President of Microsoft Corporation, Testimony before the Senate Committee on Armed Services (February 23, 2021).
- Susskind, Daniel, "Invention," *Lapham's Quarterly*, Vol. XIV, No.1 (Winter 2021), excerpted from *A World Without Work: Technology, Automation, and How We Should Respond* (2020).