The Graduate School of Political Management

THE GEORGE WASHINGTON UNIVERSITY

M.P.S. in Legislative Affairs
Semester
May 18, 2020 – June 26, 2020

Course Name
LGAF 6270.LH1
3 Credits

Mondays and Wednesdays, 6pm – 8pm

Class Location:
Hall of States, 444 North Capitol Street, NW
Washington, DC 20001
(*check with front desk for class room number each night as the room may vary*)

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 for time during work hours.

Blackboard Site
A Blackboard course site has been set up for this course. Each student is expected to check the site throughout the semester, as Blackboard will be the primary venue for outside classroom communications between the instructors and the students. 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 some form of 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 leave here, 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 by having students sign a sheet of paper or by electronic means if class is conducted online. 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, 9 hours (540 minutes) per week. Over the course of the semester, students will spend 22 hours in instructional time and 54 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

Dr. Jack Prostko
Associate Dean for Learning and Faculty Development
College of Professional Studies
jackp@gwu.edu | 202-994-3592

Suzanne Farrand
Director of Academic Administration, 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 U.S. 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;
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, sophisticated 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 readings into succinct professional memoranda; and to make presentations to the class on assigned topics and engage with their fellow students.

Course Requirements
Students are encouraged to keep up with all readings, but are responsible, on an alternating basis, for only one readings per class. 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. Students should highlight three or four top line bullet points to guide their colleagues through the presentation.

Evaluation and Grading

Assignment	Learning Objective(s) Addressed	Due Date	Weight
Assignment 1: Hearing Proposal Memo	**Memo Due at Start of Class** You work for the chairman of a House or Senate committee with jurisdiction over some aspect of cybersecurity during the 116th Congress (may include Agriculture, Armed Services, Banking, Commerce, Finance, Homeland Security, Intelligence, Judiciary, Small Business, etc.). Your chairman wants to hold a hearing on an aspect of cybersecurity under the committee's jurisdiction, and wants a hearing proposal from you. You must provide your chairman with a hearing proposal memo (*3-5 pages, 1-inch margins, Times New Roman font, 1.5 spacing*). The memo should outline a topic to be considered, a summary of the committee's accomplishments – or lack of accomplishment – regarding the topic, a list of proposed witnesses, and several questions for the chairman to ask witnesses. Lastly, the memo must state the <u>objective you are trying to achieve with this hearing</u>.	Wed. 6/3/20	25%

Assignment 2 Vote Recommendation Memo	**Memo Due at Start of Class** It is August 1, 2012, the day before a cloture vote in the United States Senate on S.3414, the Cybersecurity Act of 2012. You are the cybersecurity policy advisor for a United States Senator that does not sit on a relevant committee of jurisdiction and has not been following the broader debate over S.3414. For days, other senators – from both sides of the aisle, and both sides of the issue – have been trying to convince your senator how to vote. You must provide your senator a briefing memo (*One page only*) analyzing the merits of S.3414, and make a recommendation to your senator to vote "YEA" or "NAY" on the cloture motion. *NOTE*: As a policy advisor, you are strictly evaluating the merits of S.3414 in a cybersecurity context – the political party and political considerations of your fictional senator are irrelevant.	Wed. 6/10/20	15%
Assignment 3 Op-Ed for Member of Congress	**Final Paper Due at Start of Class** You are the cybersecurity policy advisor for a House or Senate member who wants to publish an op-ed in a major paper or a periodical that explores the question: what does it mean to think strategically about cybersecurity?	Wed. 6/24/20	35%

	Students must draft this op-ed for their member (5-*7 pages, 1-inch margins, Times New Roman font, 1.5 spacing*). The point is to effectively synthesize the readings on cybersecurity with concepts on strategic thinking, and to present the synthesis in an analytical, logically coherent manner.		
Attendance and Participation	Every student will be required to make a presentation (*no less than 2 minutes; no more than 5 minutes*) of a course reading to the class on a rotating basis. Presentations should not be "book reports," but rather analyses of the readings. Students should highlight three or four top line bullet points to guide colleagues through their presentations. As such, participation and attendance counts for one quarter of the final grade!		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, 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 networks and computer forensics, as well as concepts relevant to the scientific method. 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 clear, concise, and grammatically correct. Strunk & White should be utilized by students to achieve clear prose, and it can kept as a reference for good writing for students 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

Class 1, Monday, May 18, 2020
Course Introduction and Overview: What is "Cyber?"

Learning Objective(s) Addressed:
Professor will review the structure of the course, guidelines, due dates, grading, and issues studied in the course.

A glossary of the technical terminology students will encounter in course materials.

A glossary of relevant statutes including: Electronic Communications Privacy Act (ECPA), Foreign Intelligence Surveillance Act (FISA), Computer Fraud and Abuse Act (CFAA), Cybersecurity Information Sharing Act (CISA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic Clinical Health (HITECH), Federal Information Security Management Act (FISMA), Federal Trade Commission (FTC) Unfair and Deceptive Acts and Practices (UDAP) authorities.

> *NOTE*: Students **not expected to memorize** the glossary or the relevant statutes; the purpose is for quick reference when encountering terms & statutes in the class readings.

Required Readings:
- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed.*, Chapters 1.
- Michael Riordan and Lillian Hoddeson, *Crystal Fire: The Birth of the Information Age*, Preface.
- Norbert Wiener, *Cybernetics or Control and Communications in the Animal and the Machine*, Introduction, pages 7-39.
- Judges, Chapters 6 – 7, Colloquially "Gideon's Night Attack," *The New American Bible*, Saint Joseph Edition (1986).
- Alfred Price, *Instruments of Darkness: The History of Electronic Warfare 1939 – 1945*, Greenhill Books (1977, 2017), Chapter 11.
- Eliot Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War*, Free Press, New York (1990), Chapter 4.
- Multiple news articles that bear on cyber matters relevant to course discussion.

Optional Readings:
- Glossary of Relevant Statutes
- Glossary of Cybersecurity Terminology, National Initiative for Cybersecurity Careers and Studies (NICCS), Official website of Cybersecurity and Infrastructure Security Agency (CISA), https://niccs.us-cert.gov/about-niccs/glossary.

Thought Exercises for Class Discussion:
- What is "Cyber?"
- Were the Allies' D-Day diversions a "cyber-attack"?
- Was Gideon's Night Attack a "cyber-attack"?
- What cyber implications are there in regards to American anti-submarine warfare in 1942?
- When did the "cyber age" begin?

Class 2, Wednesday, May 20, 2020
Cybernetic Perspectives

Learning Objective(s) Addressed:

This class will explore human history from a cybernetic perspective, looking at flows of information, how information is organized and processed, as well as how it dissipates.

Required Readings:

- Parunak and Bruechar, "Engineering Swarming Systems," *Altarum Institute* (2003).
- JFC Fuller, *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.), Ch. 1.
- Herbert Simon, "Rational Choice and the Structure of the Environment," *Psychological Review*, Vol.63, No.2 (1956).
- Sean Lynn-Jones, "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).
- Jared Diamond, *Guns, Germs, and Steel*, W.W. Norton & Company (1997), Ch. 10.
- Guy Deutscher, *The Unfolding of Language: An Evolutionary Tour of Mankind's Greatest Invention*, Picador (2005), Introduction.
- Robert O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression*, Oxford University Press, Oxford & New York (1989), Ch. 1.
- James Roche and Barry Watts, "Choosing Analytical Measures," *Journal of Strategic Studies*, June 1991, Vol.14, No.2, pp. 165-209.
- Martin Van Crevald, *Technology and War: From 2000 B.C. to the Present*, Excerpted Chapters.
- Multiple news articles that bear on cyber matters relevant to course discussion.

Thought Exercises for Class Discussion:

- What is "Cyber?"
- How should we analyze cyber?
- Can one perceive language and ancient civilizations from a cybernetic perspective?
- Is J.F.C. Fuller's "Constant Tactical Factor" relevant to the current debate on cybersecurity?
- Is there a link between AI development in the Parunak/Breucher study and human society, civilization, and language?
- Are there other examples from history that underscore the role of information flows?

Week 2

Monday, May 25, 2020

NO CLASS – MEMORIAL DAY

Class 3, Wednesday, May 27, 2020
Cyber, Technology, and the Role of Science

Learning Objective(s) Addressed:
This class will examine some of the history around basic scientific research that had momentous implications for technological advancements in the early- and mid-20th Century. It was this time period that laid the ground work for modern information-technology systems.

Required Readings:

- Jon Gertner, *The Idea Factory: Bell Labs and the Great Age of American Innovation*, Introduction, and Chapter 3.
- Karl Popper, *The Logic of Scientific Discovery*, Excerpted Chapters.
- Robert Buderi, *The Invention that Changed the World: How a Small Group of Radar Pioneer Won the Second World War and Launched a Technical Revolution*, Simon & Schuster (1996), Excerpted Chapters.
- Stephen Van Evera, *Guide to Methods for Students of Political Science*, Cornell University Press (1997), Excerpts from Chapter 1.
- Lillian Hoddeson and Michael Riordan, *Crystal Fire: The Birth of the Information Age*, Excerpted Chapters.
- Peter Woit, *Not Even Wrong: The Failure of String Theory and the Search for Unity in Physical Law*, Basic Books (2006), Excerpted Chapters.
- Adam Shostack and Andrew Stewart, *The New School of Information Security*, Chapter 3.
- Guy Deutscher, *The Unfolding of Language: An Evolutionary Tour of Mankind's Greatest Invention*, Picador (2005), Appendix E.
- Lee Smolin, *The Trouble with Physics: The Rise of String Theory, the Fall of Science, and What Comes Next,* Excerpted Chapters.
- Multiple news articles that bear on cyber matters relevant to course discussion.

Thought Exercises for Class Discussion:

- What is cyber?
- What is science?
- What differentiates science from non-science?
- What is the role of basic research in scientific discovery?
- What role does scientific discovery play in technological development?
- Scientific specialization v. interdisciplinary studies, which is preferable?
- Is "science" always consistent with Popper's concept of the Scientific Method?

Week 3

Class 4, Monday, June 1, 2020
Telecommunications 101

Learning Objective(s) Addressed:
Class will focus on the development and evolution of networks from analog to digital communications, as well as among people, and the law and policy that developed as technologies matured.

Required Readings:

- Jon Gertner, *The Idea Factory: Bell Labs and the Great Age of American Innovation*, Excerpted Chapters.
- Lillian Hoddeson and Michael Riordan, *Crystal Fire: The Birth of the Information Age*, Chapter 11, "California Dreaming."
- Sam Halabi with Danny McPherson, *Internet Routing Architectures*, 2nd ed., Cisco Press (2000), Chapter 1.
- Ludwig von Bertalanffy, *General Systems Theory: Foundation, Development, and Applications*, Excerpted Chapters.
- Andrew Blum, *Tubes: A Journey to the Center of the Internet*, Excerpted Chapters.
- Sam Sarkesian, John Allen Williams, and Stephen Cimbala, *US National Security: Policymakers, Processes & Politics, 4th ed*., Lynn Rienner Publishers (2008), Chapter 11.
- Jeff Kosseff, *The Twenty-Six Words that Created the Internet*, Cornell University Press (2019), Introduction.
- Murray Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex*, Excerpted Chapters.
- Jonathan Nuechterlein and Philp Weiser, *Digital Crossroads: Telecommunications Law and Policy in the Internet Age*, 2nd ed., MIT Press, Cambridge (2013), Excerpts.
- Committee on Review of Switching, Synchronization and Network Control in National Security Telecommunications, "Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness," Washington, DC (1989), Excerpts.
- Duncan Watts, *Six Degrees: The Science of a Connected Age*, WW Norton Co. (2002), Excerpts.
- Jonah Berger, *Contagious: Why Things Catch On*, Simon & Schuster (2013), Introduction.
- Multiple news articles that bear on cyber matters relevant to course discussion.

Thought Exercises for Class Discussion:

- What is cyber?
- What role does government play in the flow of information?
- How has the communications landscape in the United States changed over the last century?
- Do communications architectures and technology constitute a complex adaptive system?
- Are countries with more robust communications economically, politically, and militarily stronger than those without?
- Are there down sides to connectivity?

Class 5, Wednesday, June 3, 2020
From World War II, Through the Cold War, and Into the Modern Era of Warfare and Technology

!!FIRST ASSIGNMENT DUE AT START OF CLASS!!

Memo Parameters:

You work for a Senate/House committee with jurisdiction over some aspect of cybersecurity. The chairman wants a hearing proposal from you on a cyber-topic within jurisdiction.

You must provide your chairman with a hearing proposal that outlines a topic to be considered, and the ultimate objective you are trying to achieve with this hearing.

Learning Objective(s) Addressed: This class will cover both the increased lethality and vulnerabilities of the US Armed Forces' dependence on, and integration of, information and communications technology.

Required Readings:

- Andrew Marshall, *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.
- National Security Decision Directive (NSDD-145), *National Policy on Telecommunications and Automated Information System* (U), Washington, DC (September 17, 1984).
- Richard Van Atta, 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).
- Alfred Price, *War in the Fourth Dimension: US Electronic Warfare, from the Vietnam War to the Present*, Greenhill Books, London (2001), Chapter 20.
- Andrew Marshall, "Some Thoughts on Military Revolutions – Second Version," OSD/NA memorandum for the record, August 23, 1993.
- 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).
- Elihu Zimet, with Robert Armstrong, Donald Daniel, and Joseph Mait, "Technology, Transformation, and New Operational Concepts, Defense Horizons (Sept 2003).
- Thomas Mahnken, *Technology and the American Way of War Since 1945*, Chapters 4, 5, and Conclusion.
- Michael Schrage, "Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency," MIT SSP, May 2003.
- John Stillion and Bryan Clark, "What it Takes to Win: Succeeding in 21st Century Battle Network Competitions," Center for Strategic and Budgetary Assessments (July 10, 2015).
- Thomas Kuhn, *Structure of Scientific Revolutions*, University of Chicago Press (1962), Excerpted Chapters.
- Multiple news articles that bear on cyber matters relevant to course discussion.

Thought Exercises for Class Discussion:

- What are the pros and cons of the "revolution in military affairs" (RMA)?
- How does Kuhn's conception of science contrast with Popper's, and how does it relate to RMA?

Week 4

Class 6, Monday, June 8, 2020
Scope of Cybersecurity Challenges 101

Learning Objective(s) Addressed:
The class will outline some of the broader trends regarding challenges in cyberspace.

Required Readings:

- CSIS Significant Cyber Incidents Since 2006: some of the broader trends regarding challenges in cyberspace.
- Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, Excerpted Chapters.
- Adam Shostack and Andrew Stewart, *The New School of Information Security*, Chapters 4 and 6.
- Kevin Mitnick with William Simon, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Little Brown & Company (2011), Excerpted Chapters_1.
- Kevin Mitnick with William Simon, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Little Brown & Company (2011), Excerpted Chapters_2.
- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed.*, Chapters 6 and 10.
- The National Strategy to Secure Cyberspace, President George W. Bush, Washington, DC (February 2003).
- "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).
- Steve Kroft, "The Data Brokers: Selling Your Personal Information," *60 Minutes* (August 24, 2014); and Anderson Cooper, "Bitcoin's Wild Ride," *60 Minutes* (May 19, 2019).
- 2019 Data Breach Investigations Report, Verizon (May 2019).
- Kevin Mitnick with Robert Vamosi, *The Art of Invisibility*, Hachette Book Group (2019), Ch. 1-2.
- John Kotter, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review*, Mar-April 1995.
- Multiple news articles that bear on cyber matters relevant to course discussion.

Thought Exercises for Class Discussion:

- Are cyber challenges and data breaches growing or slowing?
- How do network intrusions occur?
- What are "black swan" events, and can data breaches be "black swans?"
- Why isn't security built into cyber systems at the outset?
- Why are organizations resistant to securing their cyber systems?
- What are other examples of organizations being resistant to change?
- What can the federal government do about data breaches – should this be left to state and local governments to figure out?
- Do individuals have an expectation of privacy in the 21st Century?

Class 7, Wednesday, June 10, 2020
Congressional and Administrative Responses to Cyber Challenges

!!SECOND ASSIGNMENT DUE AT START OF CLASS!!

Memo Parameters:

It is August 1, 2012, the day before a cloture vote on S. 3414. You are the cybersecurity policy advisor for a United States Senator that does not sit on a relevant committee of jurisdiction and has not been following the broader debate on S. 3414.

You must provide your senator a briefing memo (*One page, Times New Roman font*) analyzing the merits of S. 3414 in the context of the broader debate and make a recommendation to your senator to vote **"YEA"** or **"NAY"** on cloture.

Learning Objective(s) Addressed: Class will focus on the challenges of crafting cyber policy, and go over the merits of S.3414, its evolution, and subsequent congressional and administrative actions.

Required Readings:

- Carl Von Clausewitz, *On War*, Michael Howard and Peter Paret, eds., Princeton University Press (1976), Excerpts.
- Shane Harris, *@ War: The Rise of the Military-Internet Complex*, First Mariner Books (2015), Excerpted Chapters.
- Tom Larsen, "The Growing Problem of Cybersecurity," Presentation (June 7, 2013).
- 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).
- 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).
- 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).
- 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).
- Lieberman-Collins Dear Colleague Letter
- Lieberman-Collins_SECURE IT Side-by-Side
- Statement of Administration Policy on S. 3414
- Executive Order 13636, Improving Critical Infrastructure Cybersecurity (2/12/13)
- U.S. Chamber of Commerce Letter to NIST on Framework (2/9/16).
- U.S. Chamber of Commerce Letter to NIST on Cyber (9/9/16).
- Horst Rittel and Melvin Webber, "Dilemmas is a General Theory of Planning," Policy Sciences 4 (1973).
- Multiple news articles that bear on cyber matters relevant to course discussion.

Thought Exercises for Class Discussion:

- Which is preferable when it comes to cybersecurity: regulation or information sharing?

Week 5

Class 8, Monday, June 15, 2020
Scope of Cybersecurity Challenges 202

Learning Objective(s) Addressed:
This class will explore more recent shifts in trends regarding challenges in cyberspace.

Required Readings:

- Eric Fischer, Cybersecurity Issues and Challenges: In Brief, Congressional Research Service, Washington, DC (August 12, 2016).
- What Every CEO Needs to Know About Cybersecurity, AT&T Cybersecurity Insights, Vol. 1, AT&T (2015).
- 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).
- Report of the Defense Science Board, "21st Century Military Operations in a complex Electromagnetic Environment," Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics (July 2015).
- "The Internet of Things (IoT): A New Era of Third-Party Risk," Ponemon Institute, LLC, Sponsored by Shared Assessments (May 2017).
- "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.
- Seth Lloyd, "Quantum-Mechanical Computers: Quantum-Mechanical Computers, if they can be constructed, will do things no ordinary computer can," *Scientific American* (October 1995).
- Sam Sacks, Testimony before the House Energy and Commerce Subcommittee on Communications and Technology Hearing, "Telecommunications, Global Competitiveness, and National Security," (May 16, 2018).
- Benoit Mandelbrot and Richard Hudson, *The (Mis)Behavior of Markets: A Fractal View of Financial Turbulence*, Chapters Excerpted
- The Hon. Eric Rosenbach, Testimony before the Senate Commerce Committee Hearing, "China: Challenges to US Commerce," (March 7, 2019).
- Diane Souvaine, Testimony before the Senate Commerce Committee Hearing, "Research & Innovation: Ensuring America's Economic and Strategic Leadership," (October 22, 2019).
- Edward Lorenz, *The Essence of Chaos*, Excerpted Chapters.
- Multiple news articles that bear on cyber matters relevant to course discussion.

Thought Exercises for Class Discussion:

- How has the cyber threat landscape evolved since the 2012 cyber debate?
- What new technologies emerged, and where does the US stand in relation to competitors regarding these new technologies?
- The US led technological development in the 20th Century, has that changed in the 21st Century?
- Is the answer to innovation to be found with the private sector, government, or both?

Class 9, Wednesday, June 17, 2020
The Need to Think Strategically about Cyber

Learning Objective(s) Addressed:
This class will examine the role of strategic thinking, compare/contrast cyber weapons with nuclear weapons, and examine

Required Readings:

- Andrew Krepinevich and Barry Watts, Regaining Strategic Competence, Center for Strategic and Budgetary Assessments (2009).
- United States of America, Cyberspace Solarium Commission, Washington, DC, (March 2020), Executive Summary: https://www.solarium.gov/
- Konrad Lorenz, *On Aggression*, Chapters Introduction, 13.
- Andrew Krepinevich, Cyber Warfare: A "Nuclear Option," Center for Strategic and Budgetary Assessments (2012), available at: http://csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf
- Bryan Clark and Mark Gunzinger, "Winning the Airwaves: Regaining America's Dominance in the Electromagnetic Spectrum," (2017), http://csbaonline.org/research/publications/winning-the-airwaves-sustaining-americas-advantage-in-the-electronic-spectr/publication.
- Richard Rumelt, *Good Strategy Bad Strategy: The Difference and Why it Matters*, Excerpted Chapters.
- Bernard Brodie, "The Development of Nuclear Strategy," *International Security*, Vol. 2, No. 4, Spring 1978, pp 65-83.
- David Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Crown Publishing Group (2018), Excerpts.
- Alan Beyerchen, "Clausewitz, Nonlinearity and the Unpredicatbility of War, *International Security*, 17:3 (Winter, 1992).
- William Black, Jr., "Thinking Out Loud About Cyberspace," *Cryptolog* (U) (Spring 1997).
- Shane Harris, *@ War: The Rise of the Military-Internet Complex*, First Mariner Books (2015), Chapter 13.
- Paul Feyerabend, *Against Method*, 4th Ed., Excerpted Chapters.
- Multiple news articles that bear on cyber matters relevant to course discussion.

Thought Exercises for Class Discussion:

- What does it mean to think strategically?
- Does cybersecurity require strategic thinking?
- How does the US Cyberspace Solarium Commission compare and contrast with the Solarium exercise of the Eisenhower administration?
- How do cyber weapons compare and contrast against with nuclear weapons?
- Is cyber "deterrence" possible?
- How does one compare and contrast strategy with operations, and with tactics?
- How does Feyerabend's conception of science contrast with those of Kuhn and Popper?
- Are science and strategy analogous to one another?

Week 6

Class 10, Monday, June 22, 2020
Russia and China

Learning Objective(s) Addressed: Class will evaluate Russia and China in relation to the United States.

Required Readings:

- "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).
- Mao Tse Tung, *On Guerrilla Warfare*, Excerpted Chapters.
- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed.*, Chapter 11.
- Daniel Rosen, Testimony before the Senate Commerce Committee Hearing, "China: Challenges for US Commerce," (March 7, 2019).
- Mandiant Report: "APT1: Expsoing One of China's Cyber Espinage Units," (2013), available at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
- Report on the Investigation Into Russian Interfernce 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.
- F.W. Walbank, Introduction, *Polybius: The Rise of the Roman Empire*, Penguin Books (1979).
- Crowdstrike Intelligence Report: "Putter Panda" (2015), available at: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf
- Andrei Tsygankov, *Russian Foreign Policy: Change and Continuity in National Identity*, 2nd ed. (2010).
- 2019 Report to Congress of the US-China Economic and Security Review Commission (November 2019), Executive Summary.
- "Military Doctrine of the Russian Federation," from Russian Foreign Policy in Transition: Concepts and Realities, Andrei Melville and Tatiana Shakleina, editors, CEU Press (2005).
- 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.
- You Ji, "Friends in need or Comrades in Arms: The Dilemma in the Sino-Russian Weapons Business."
- Multiple news articles that bear on cyber matters relevant to course discussion.

Thought Exercises for Class Discussion:

- How are Russia and China incorporating cyber into their tactics, operations, and broader strategies?
- Is there anything fundamentally different about Russia and China, and their relationships to each other and with the United States, today compared to the Cold War in regards to cyber?
- Is the United States political system strong enough to withstand Russian attempts to interfere to with our elections?
- What role does the media – both traditional and social – play in checking foreign adversaries, i.e. do they have a responsibility and who has oversight of such responsibility?
- Is the United States playing a reactive game in cyber with regards to Russia and China, or does the United States have potential opportunities for asymmetric advantages?

Class 11, Wednesday, June 24, 2020
Artificial Intelligence, Biotechnology, and Human Evolution

!!THIRD & FINAL ASSIGNMENT DUE AT START OF CLASS!!

Paper Parameters:

Students must write a short paper (5-*7 pages, Times New Roman font, 1.5 spacing*) that answers a simple question: What is cybersecurity, and what does it mean to think strategically about it? Students should approach this paper as if they are writing an op-ed for a member of Congress.

Required Readings:

- Edward Felton, Testimony before the Senate Commerce Committee hearing, "Digital Decision-Making: The Building Blocks of Machine Learning and Artificial Intelligence," (December 12, 2017).
- Executive Order 13859, "Maintaining American Leadership in Artificial Intelligence," Federal Register, Vol.84, No.31 (February 14, 2019).
- Robin Fox, Aggression: Then and Now," in Michael Robinson & Lionel Tiger (eds.), *Man & Beast Revisited*, pp. 81-93.
- US Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools, National Institute for Standards and Technology (NIST), US Department of Commerce, Prepared in Response to Executive Order 13859 (August 2019).
- The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update, A report by the Select Committee on Artificial Intelligence of the National Science & Technology Council, Executive Office of the President (June 2019).
- Malcolm Gladwell, *Blink: The Power of Thinking Without Thinking*, pp 72-98.
- Kelley Sayler, "Artificial Intelligence and National Security," Congressional Research Service, R45178 (November 21, 2019).
- Linxing Jiang, et al, "BrainNet: A Multi-Person Brain-to-Brain Interface for Direct Collaboration Between Brains," *Nature* (September 2018).
- Francis Fukuyama, *Our Post Human Future: Consequences of the Biotechnology Revolution*, Furrar, Straus, and Giroux, New York (2002), Excerpts.
- Michael Brown, Testimony before the Senate Armed Services Subcommittee on Emerging Threats Hearing, "Artificial Intelligence Initiatives within the Department of Defense (March 12, 2019).
- Phil Quade, editor, *The Digital Big Bang: The Hard Stuff, the Soft Stuff, and the Future of Cybersecurity*, John Wiley & Sons, Inc., Indianapolis (2019), Excerpts.
- Daniel Kahneman, "Maps of Bounded Rationality: A Perspective on Intuitive Judgment and Choice," Noble Prize Lecture, Dec. 8 2002.
- Multiple news articles that bear on cyber matters relevant to course discussion.
