The Graduate School
of Political Management

THE GEORGE WASHINGTON UNIVERSITY

M.P.S. in Legislative Affairs
Semester
May 20, 2019 – June 26, 2019

Course Name
Congress and Cybersecurity
LGAF 6270.LH1
3 Credits

Mondays and Wednesdays, 6-8pm

Class Location:
Hall of States
444 North Capitol, 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 request to 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. Tardiness and unexcused absences will impact a student's participation grade, which accounts for 10 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 and written response papers or projects 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. Steven Billet
Director, Legislative Affairs Program
sbillet@gwu.edu | 202-994-1149

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, 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:

1. Effectively communicate cybersecurity's evolution and key concepts, as well as the contemporary public policy debates that surround it;
2. Think critically about cybersecurity and analyze it from the political, economic, social, scientific, and strategic perspectives; and
3. Acquire the skills to evaluate and represent different sides of cyber public policy questions, and to distill complex readings into succinct professional memoranda and presentations.

Course Requirements

Students are responsible for keeping up with all required readings and participate constructively in class discussions. Students are encouraged to keep up with "optional" readings that supplement the required readings. In addition, students must choose at least one optional reading that is highlighted in yellow on a scientific or strategic concept (choices will be granted on a first-come-first-serve basis) to make a 15-

minute presentation to the class. The presentation should not be a "book report," but rather an analysis of the reading and its relationship to cybersecurity.

Evaluation and Grading

Assignment	**Learning Objective(s) Addressed**	**Due Date**	**Weight**
Assignment 1	**First 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. You must provide your senator a briefing memo (*3-5 pages, 1-inch margins, Times New Roman font, 1.5 spacing*) 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 policy context – political considerations are irrelevant.	June 5th	20%
Assignment 2	**Second Memo Due at Start of Class** It is the 116th Congress, and you work for the Chairman of a House/Senate committee with jurisdiction over some aspect of cybersecurity (may include	June 17th	20%

	Intelligence, Commerce, Armed Services, Homeland Security, Judiciary, etc.). Prospectively, the Chairman wants to hold a hearing on some aspect of cybersecurity under the committee's jurisdiction, and wants a hearing proposal. You must provide your Chairman with a hearing proposal memo (*3-5 pages, 1-inch margins, Times New Roman font, 1.5 spacing*) that outlines a topic to be considered, as well as what cyber-related hearings the committee held since the beginning of the 116th Congress, what relevant cyber legislation was reported out of the committee since the beginning of the 116th Congress (and whether any such legislation was signed into law), a list of witnesses you want to invite, and the objective you are trying to achieve with this hearing.		
Assignment 3	**Final Paper Due at Start of Class** Students must write a short paper (5-*7 pages, 1-inch margins, Times New Roman font, 1.5 spacing*) that answers a simple	June 26th	35%

	question: What is Cybersecurity, and what does it mean to think strategically about it? Students should approach this paper as if it were a long op-ed in a major newspaper or an article in a periodical. The point is to effectively synthesize the required readings on cybersecurity with concepts from the optional readings on strategic thinking, and to present the synthesis in an analytical, logically coherent manner.		
Assignment 4	**Presentation of an Optional Reading:** By the end of the first week of class (no later than close of business on Friday, May 24th) each student must choose an optional reading (highlighted in yellow in the syllabus) and make a presentation to the class that conveys the concepts from the reading, and relates those concepts to an aspect of cybersecurity. Reading choices will be granted on a first-come-first-serve basis, and there are choices available as early as Class 2. The presentation should be approximately 15 minutes,	Will depend on which optional reading is selected/assigned	15%

	including time for questions and answers from classmates. The presentation should not be a “book report,” but an analysis of the reading and its relationship to cybersecurity. Students will give their presentation on the evening for which the optional reading was assigned, and these presentations will be given at the beginning of class.		
Attendance and Participation	Students are expected to attend every class on time, participate constructively, and be respectful of other students in class debates.	N/A	10%
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

Readings for the class – both required and optional – are listed below for each class during the semester. Most readings will be available on Blackboard, but students are encouraged to purchase 4 texts for this class, as they constitute the majority of the required reading and contain the essential concepts to understanding cybersecurity:

- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed*., O'Reilly Media (2012).
- Shane Harris, *@ War: The Rise of the Military-Internet Complex,* First Mariner Books (2014).
- Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of the Computer Espionage*, Pocket Books, a division of Simon & Schuster (1989, 1990).
- Andrew Blum, *Tubes: A Journey to the Center of the Internet*, Harper Collins (2012).

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 20, 2019
Course Introduction and Overview:

Learning Objective(s) Addressed:

Professor will review the structure of the course, guidelines, due dates, grading, practical skills to be gained, and issues to be studied in the course.

Students will be provided a glossary of the technical terminology they will encounter in course materials, as well as 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 will not be expected to memorize the glossary; its purpose is for quick reference when encountering terms, statutes, and acronyms in the readings.

Required Readings:

- Shane Harris, *@ War: The Rise of the Military-Internet Complex*, Prologue.
- Adam Shostack and Andrew Stewart, *The New School of Information Security*, Chapters 4 and 6.
- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed*., Chapters 1 and 2.
- Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of the Computer Espionage*, Chapters 2, 15, 32, 53, and Epilogue.

- Several contemporary news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:

- Norbert Wiener, Cybernetics or Control and Communications in the Animal and the Machine, Excerpted Chapters.*
- Lillian Hoddeson and Micahel Riordan, *Crystal Fire: The Birth of the Information Age*, Preface.

**NOTE: A student who selects this reading from Norbert Wiener will not be required to present it until Class 2.*

Class 2, Wednesday, May 22, 2019
Science, Technology, and Analytical Methods

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.

Students will be introduced to concepts in the scientific method that parallel concepts in strategic thinking, i.e. grappling with uncertainty by employing empirical data and brutal honesty in questioning long held underlying assumptions, as well as critical, independent thinking that may clash with normative beliefs.

Required Readings:

- Jon Gertner, *The Idea Factory: Bell Labs and the Great Age of American Innovation*, Introduction, and Chapter 3.
- Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of the Computer Espionage*, Chapter 16.
- Adam Shostack and Andrew Stewart, *The New School of Information Security*, Chapter 3.
- Lillian Hoddeson and Micahel Riordan, *Crystal Fire: The Birth of the Information Age*, Excerpted Chapters.
- James Roche and Barry Watts, "Choosing Analytical Measures," *Journal of Strategic Studies*, June 1991, Vol. 14, No. 2, pp. 165-209.
- Several contemporary news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:

- Karl Popper, *The Logic of Scientific Discovery*, Excerpted Chapters.
- Lee Smolin, *The Trouble with Physics: The Rise of String Theory, the Fall of Science, and What Comes Next,* Excerpted Chapters.

- John Kotter, "Leading Change: Why Transformation Efforts Fail," *Harvard Business Review*, Mar-April 1995.

Week 2:

Monday, May 27, 2019

NO CLASS – MEMORIAL DAY

Class 3, Wednesday, May 29, 2019
Global Communications Architecture and Radio Frequency Spectrum

Learning Objective(s) Addressed:
Class will focus on the development and evolution of global telecommunications networks from analog to digital communications, as well as network architecture, and different technologies involved, i.e. copper wire pairs, coaxial cable, fiber optics, wireless, satellites, and undersea cable networks. We will also explore the rise of Silicon Valley, and data centers that are linked by communications networks.

The relationship between communications networks and their national security implications will also be explored.

Required Readings:

- Jon Gertner, *The Idea Factory: Bell Labs and the Great Age of American Innovation*, Excerpted Chapters.
- Andrew Blum, *Tubes: A Journey to the Center of the Internet*.
- Lillian Hoddeson and Micahel Riordan, *Crystal Fire: The Birth of the Information Age*, Chapter 11, "California Dreaming."
- 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), https://www.acq.osd.mil/dsb/reports/2010s/DSB_SS13--EW_Study.pdf.
- James Lewis, "Spectrum Management for Economic Growth and National Security," Center for Strategic and International Studies (April 2017), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170404_Lewis_SpectrumManagement_Web_Rev.pdf?XIjFJ0kHnStbN_UM2Jzn9fIJW_HLTuFK.
- Several contemporary news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:

- Ludwig von Bertalanffy, *General Systems Theory: Foundation, Development, and Applications*, Excerpted Chapters.
- Murray Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex*, Excerpted Chapters.

- 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.

Week 3

Class 4, Monday, June 3, 2019
Scope of Cybersecurity Challenges

Learning Objective(s) Addressed:
We will outline some of the broader trends regarding challenges in cyberspace (including data breaches and data breach notification, Internet of Things (IoT), privacy, wiretap authorities, artificial intelligence, "big data" analytics, geolocation, quantum computing, industrial espionage, threats to critical infrastructure, virtual reality, autonomous systems, encryption and the "going dark" debate, tax return fraud, and genetic hacking).

Lastly, supply students with context of the major actors threatening cyberspace in an ascending list of severity: (1) hacktivists and script kiddies; (2) criminal networks; and (3) nation-states. The boundaries between these groups, as we will learn throughout the semester, are not always distinct.

Required Readings:

- 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
- Tom Larsen, "The Growing Problem of Cybersecurity," Presentation (June 7, 2013).
- "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).
- What Every CEO Needs to Know About Cybersecurity, AT&T Cybersecurity Insights, Vol. 1., available at: https://www.business.att.com/cybersecurity/docs/decodingtheadversary.pdf
- 2017 Cost of Cybercrime Study, Ponemon Institute (2017), available at:
- https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50
- Several contemporary news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:

- Martin Van Crevald, *Technology and War: From 2000 B.C. to the Present*, Excerpted Chapters.
- U.S. Department of Homeland Security, National Cybersecurity & Communications Integration Center, "Heartbleed" OpenSSL Vulnerability (4/10/17).
- CRS IN FOCUS: "Cybersecurity Issues and Challenges," (11/6/14)

- CSIS Significant Cyber Incidents Since 2006: https://csis-prod.s3.amazonaws.com/s3fs-public/170519_Significant_Cyber_Events_List.pdf?HJ4k1Bt7x.zleLsdr9m6SQbkWHtuNJ39
- James March and Herbert Simon, Organizations, 2nd Ed., (1993), Excerpted Chapters.

Class 5, Wednesday, June 5, 2019
Congressional and Executive Approaches to Cybersecurity Solutions:

Assignment Due Today:

!! First Memo 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 (*3-5 pages, Times New Roman font, 1.5 spacing*) 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 evolution of approaches to addressing cybersecurity concerns. At the Congressional level, we will focus on the evolution of legislation, including: the introduction of the Cyber Intelligence Sharing and Protection Act (CISPA) in the 112th Congress, which authorized information sharing between the government and private sector; the Senate debate during the 113th Congress over the Lieberman-Collins Cybersecurity Act, which would have created minimum mandatory cybersecurity requirements for owners and operators of critical infrastructure; the introduction and final passage of the Cybersecurity Information Sharing Act (CISA) in the 114th Congress.

Class will also explore separate developments in the Executive Branch that culminated in the issuing of Executive Order 13636: "Improving Critical Infrastructure Cybersecurity," that led to the development of the National Institute of Standards and Technology (NIST) Framework of voluntary cybersecurity best practices, and challenges with the Framework's implementation.

Required Readings:

- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed.*, Chapter 17.
- Shane Harris, *@ War: The Rise of the Military-Internet Complex*, Chapters 3, 8, 10, and 12.
- Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of the Computer Espionage*, Chapter 45.
- Lieberman-Collins Dear Colleague Letter
- Summary of S. 3414 & Section-by-section summary of S. 3414
- U.S. Chamber of Commerce Analysis of Revised S. 3414
- Statement of Administration Policy on S. 3414
- *The Hill/Roll Call* Articles on SECURE IT Perspective
- Executive Order 13636, Improving Critical Infrastructure Cybersecurity (2/12/13)

- NIST Framework
- U.S. Chamber of Commerce Letter to NIST on International Standardization (9/24/15).
- Multi-Industry Letter to European Commission on P3 (March 11, 2016).
- 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).
- Several news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:
- Horst Rittel and Melvin Webber, "Dilemmas is a General Theory of Planning," Policy Sciences 4 (1973).
- Alan Beyerchen, "Clausewitz, Nonlinearity and the Unpredicatbility of War, International Security, 17:3 (Winter, 1992).
- Richard Cyert and James March, A Behavioral Theory of the Firm, Chapters Preface, Introduction, 7.
- "From Awareness to Action," A Cybersecurity Agenda for the 45th President," Center for Strategic and International Studies, Cyber Policy Task Force (January 2017), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf.

Week 4

Class 6, Monday, June 10, 2019
Social Engineering, Cyber Hygiene, and Insider Threats – How Most Hackers Gain Access

Learning Objective(s) Addressed:
It is estimated by experts that roughly 90 percent of network penetrations are due to social engineering (such as spear phishing), lack of cyber hygiene (insecure passwords and failure to update software patches), and insider threats (such as Edward Snowden).

All the technical sophistication to secure systems and networks is irrelevant if there is not adequate training, personal responsibility, vigilance, and internal controls to prevent breaches.

Additionally, this class will also examine some of the long-term repercussions of the Snowden breach, including its impact on cyber training and recruitment.

The problem is compounded by ubiquitous social media platforms wherein individuals from corporate CEOs to human resources administrative support employees post vast amount of personal information about themselves. This information can be exploited by hackers to pose as a trusted person to gain access to systems.

Required Readings:

- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed*., Chapters 6 and 10.
- Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of the Computer Espionage*, Chapters 3, 4, 5, 7, 8, 9, 10, 11, 12, 20, 25, 29, 30, 31, 34, 35, 38, 40, 50, and 55.
- Kevin Mitnick, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*, Excerpted Chapters.
- Several contemporary news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:

- Edward Lorenz, *The Essence of Chaos*, Excerpted Chapters.
- Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, Excerpted Chapters.
- Benoit Mandelbrot and Richard Hudson, *The (Mis)Behavior of Markets: A Fractal View of Financial Turbulence*, Chapters Excerpted.

Class 7, Wednesday, June 12, 2019
Revolution in Military Affairs (RMA)

Learning Objective(s) Addressed:
Students will learn about the United States military's use of, and dependence on, electronics and information networks.

As the Cold War came to a close, the United States leveraged its comparative advantage in technology of sensors, precision munitions, and networked information systems to overcome vastly superior numbers of Soviet military equipment and personnel.

Russian military strategists wrote about these nascent developments, and noted the centrality of fast, accurate information on the battlefield to enable what became known as the "Revolution in Military Affairs" (RMA)

Today, United States military forces are ever more dependent on the battle networks enabled by electronic communications systems, which are potentially vulnerable to hacking. Moreover, the proliferation of technologies that enabled the RMA are increasingly available to adversaries at lower costs.

Required Readings:

- Thomas Mahnken, *Technology and the American Way of War Since 1945*, Chapters 4, 5, and Conclusion.
- Andrew Marshall, "Some Thoughts on Military Revolutions – Second Version," OSD/NA memorandum for the record, August 23, 1993.
- James FitzSimonds and Jan van Tol, "Revolutions in Military Affairs," Joint Force Quarterly, Spring 1994.
- Andrew Marshall, "Revolutions in Military Affairs," Statement Prepared for the Subcommittee on Acquisition and Technology, Senate Armed Services Committee, May 5, 1995.

- Elihu Zimet, with Robert Armstrong, Donald Daniel, and Joseph Mait, "Technology, Transformation, and New Operational Concepts, Defense Horizons (Sept 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), available at: http://csbaonline.org/uploads/documents/What-it-Takes-to-Win.pdf
- Several contemporary news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:

- Thomas Kuhn, Structure of Scientific Revolutions, Excerpted Chapters.
- Michael Schrage, "Perfect Information and Perverse Incentives: Costs and Consequences of Transformation and Transparency," MIT SSP, May 2003.

Week 5

Class 8, Monday, June 17, 2019
Strategic Thinking

Assignment Due Today:

!! Second Memo due at Start of Class!!

Memo Parameters:
You work for the Chairman of a Senate/House committee with jurisdiction over some aspect of cybersecurity (such as the committees on Intelligence, Commerce, Armed Services, Homeland Security, or Judiciary).
The Chairman wants to hold a hearing on some aspect of cybersecurity, and wants a hearing proposal from you.

You must provide your Chairman with a hearing proposal memo (*3-5 pages, 12 Times New Roman font, 1.5 spacing*) that outlines a topic to be considered, as well as what cyber-related hearings the committee held since the beginning of the 116th Congress, what relevant cyber legislation was reported out of the committee since the beginning of the 116th Congress (and whether any such legislation was signed into law), a list of witnesses you want to invite, questions you want your Chairman to ask, and the ultimate objective you are trying to achieve with this hearing.

Required Readings:

- George Pickett, James Roche, and Barry Watts, Net Assessment: A Historical Review" in Andrew Marshall, J.J. Martin, & Henry Rowen (eds.), *On Not Confusing Ourselves: Essays on National Security Strategy in Honor of Albert & Roberta Wohlstetter*, pp. 159-189.
- Stephen Peter Rosen, "Net Assessment as an Analytical Concept" in *On Not Confusing Ourselves: Essays on National Security Strategy in Honor of Albert & Roberta Wohlstetter*, pp. 283-301.

- Andrew Krepinevich and Barry Watts, Regaining Strategic Competence, Center for Strategic and Budgetary Assessments (2009), available at: http://csbaonline.org/uploads/documents/2009.09.01-Regaining-Strategic-Competence.pdf
- Henry Mintzberg, "The Fall and Rise of Strategic Planning," Harvard Business Review, Jan-Feb. 1994.
- Several contemporary news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:

- Paul Feyerabend, Against Method, 4th Ed., Excerpted Chapters.
- Richard Rumelt, *Good Strategy Bad Strategy: The Difference and Why it Matters*, Excerpted Chapters.

Class 9, Wednesday, June 19, 2019
Cyber Deterrence and Problems with Attribution

Learning Objective(s) Addressed:
This class will analyze Cold War-era writings on classical nuclear deterrence, and survey contemporary writings on the subject emanating from prominent think tanks, government institutions, and private sector companies.

One of the biggest debates percolating on cybersecurity policy is the concept of deterrence in cyberspace. Whereas Cold War-era nuclear deterrence was fairly straight forward (if the Soviets launched a nuclear first strike, mutually assured destruction was guaranteed in our counterstrike), it if often difficult – and sometimes impossible – to positively identify the perpetrator of a cyber-attack in real time.

Deterrence in cyberspace is made more difficult in that hackers often commandeer civilian systems to carry out their attacks – systems that, if counter-attacked – could result in a compromise of personal privacy, economic losses, or even loss of life.

Required Readings:

- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed*., Chapters 5, 7, and 9.
- Shane Harris, *@ War: The Rise of the Military-Internet Complex*, Chapters 5 and 6.
- Cliff Stoll, *The Cuckoo's Egg: Tracking a Spy Through the Maze of the Computer Espionage*, Chapter 46.
- Dr. Craig Fields, Chairman, Defense Science Board, and Dr. Jim Miller, Member, Defense Science Board, "Cyber Deterrence," Statement Before the Armed Services Committee, United States Senate (March 2, 2017), https://www.armed-services.senate.gov/imo/media/doc/Fields-Miller_03-02-17.pdf.
- Martin Libicki, "Cyberdeterrence and Cyberwar," RAND Corporation Study (2009), available at: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

- Martin Libicki, "Crisis and Escalation in Cyberspace," RAND Corporation Study (2012), available at: https://www.rand.org/pubs/monographs/MG1215.html
- Martin Libicki, "Brandishing Cyberattack Capabilities," RAND Corporation Study (2013), available at: https://www.rand.org/pubs/research_reports/RR175.html
- Several contemporary news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:

- Bernard Brodie, "The Development of Nuclear Strategy," *International Security*, Vol. 2, No. 4, Spring 1978, pp 65-83.
- Thomas Kuhn, *The Road Since Structure: Philosophical Essays* (2000), Excerpted Chapters.
- Herman Kahn, "Twelve Nonissues and Twelve Almost Nonissues," from *Thinking About the Unthinkable in the 1980s*.
- Thomas Schelling, *Arms and Influence*, Chapters Excerpted.

Week 6

Class 10, Monday, June 24, 2019
Cyber Challenges: China & Russia

Learning Objective(s) Addressed:
This class will critically examine Chinese and Russian government actions in cyberspace with a multidisciplinary focus on the social, economic, political, and strategic contexts in which they occur.

Required Readings:

- Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld, 2nd Ed.*, Chapters 15 and 16.
- Shane Harris, *@ War: The Rise of the Military-Internet Complex*, Chapter 3, pp. 63-66, and Chapter 12, pp. 191-192.
- Federal Communications Commission Notice of Proposed Rulemaking, "Protecting National Security Through FCC Programs," (March 27, 2018), https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0327/DOC-349937A1.pdf.
- "Assessing Russian Activities and Intentions in Recent U.S. Elections," Senate Select Committee on Intelligence Report (January 6, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.
- Mandiant Report: "APT1: Expsoing One of China's Cyber Espinage Units," available at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
- Crowdstrike Intelligence Report: "Putter Panda" (2015), available at: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

Optional Readings:

- Mao Tse Tung, *On Guerrilla Warfare*, Excerpted Chapters.
- Andrei Tsygankov, *Russian Foreign Policy: Change and Continuity in National Identity*, 2nd ed. (2010).
- "Foreign Policy Conception of the Russian Federation," Approved by the President of the Russian Federation, V.V. Putin on June 28, 2000, from Russian Foreign Policy in Transition: Concepts and Realities, Andrei Melville and Tatiana Shakleina, editors, CEU Press (2005).
- "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).
- "Military Doctrine of the Russian Federation," from Russian Foreign Policy in Transition: Concepts and Realities, Andrei Melville and Tatiana Shakleina, editors, CEU Press (2005).
- You Ji, "Friends in need or Comrades in Arms: The Dilemma in the Sino-Russian Weapons Business."

Class 11, Wednesday, June 26, 2019
Artificial Intelligence, Robotics, and Human Evolution

Assignment Due Today:

!! FINAL PAPER 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 it were a long op-ed in a major newspaper or an article in periodical.

The point is to effectively synthesize the required readings on cybersecurity with concepts from the optional readings on strategic thinking, and to present the synthesis in an analytical, logically coherent manner.

Learning Objective(s) Addressed:
In the last class of the semester, students will survey the state-of-the-art in artificial intelligence and robotics and their implications in a cyber context for both civilian and military uses. Students will be challenged to consider these developments in the context of human evolution by exploring topics in human history, biology, and anthropology.

Required Readings:

- "Eyes on the Eyes," *Economist*, April 4, 2007.
- Ray Kurzweil, "The Coming Merging of Mind and Machine," Scientific American (2008).
- Hans Moravec, "Rise of the Robots," Scientific American (1999).
- Malcolm Gladwell, *Blink: The Power of Thinking Without Thinking*, pp 72-98.
- Parunak and Bruechar, "Engineering Swarming Systems," Altarum Institute (2003).

- William Carter, “The Plan to Build the Jobs of the Future is Loosing Us the AI Race,” Center for Strategic and International Studies (November 20, 2017), https://www.csis.org/analysis/plan-build-jobs-future-losing-us-ai-race.
- Several contemporary news articles (Washington Post, Wall Street Journal, New York Times, Wired, Scientific American, etc.) that bear on cyber matters relevant to course discussion – these will be uploaded to Blackboard at least 1-week prior to class.

Optional Readings:

- Daniel Kahneman, “Maps of Bounded Rationality: A Perspective on Intuitive Judgment and Choice,” Noble Prize Lecture, Dec. 8 2002.
- Robin Fox, Aggression: Then and Now,” in Michael Robinson & Lionel Tiger (eds.), *Man & Beast Revisited*, pp. 81-93.
- Steven Pinker, *The Blank Slate*, excerpted chapters.
- Konrad Lorenz, *On Aggression*, Chapters Introduction, 13.

Copyright Statement

Unless explicitly allowed by the instructor, course materials, class discussions, and examinations are created for and expected to be used by class participants only. The recording and rebroadcasting of such material, by any means, is forbidden.