PLCY388C, Spring 2018

Cybersecurity Policy: Practical Hacking for Policy Makers

PFH 1111; Tu & Th, 9:30-10:45

Course Instructor
Professor Charles Harry
charry@umd.edu
School of Public Policy, University of Maryland

INTRODUCTION

This course explores the key issues facing policy makers attempting to manage the problem of cybersecurity from its technical foundations to the domestic and international policy considerations surrounding governance, privacy, risk management, and applications for achieving national goals. The course is designed for students with little to no background in information technology, and will provide the principles to understand the current debates shaping a rapidly evolving security landscape.

Learning Objectives:

1) Gain a high-level understanding of the technical structures and protocols of modern telecommunications.
2) Understand and assess the cybersecurity threat landscape including motivations, tactics and tradecraft used by individuals and organizations
3) Become familiar with the US governance structures, organizations related to cybersecurity threats
4) Understand how risk is assessed for corporations and critical infrastructure.
5) Understand the security and legal questions countries struggle to solve with respect to cybersecurity
6) Understand international efforts to promote responsible behavior among nations in cybersecurity.

The course is broken up into sections with each focused on a specific set of issues germane to communications technology, the identification and tracking of cyber intrusion methods, and the domestic and international policy efforts focused on responding to events and promoting resiliency in critical infrastructure and systemically important institutions.

REQUIREMENTS

This course is designed to help students develop the broad knowledge and analytical capabilities needed to understand complex policy issues surrounding cybersecurity, as well as the oral, written, and interpersonal skills needed to participate effectively in policy debates. Students will maintain the highest standards of professional behavior and will adhere to the University of Maryland's Code of Academic Integrity (https://www.president.umd.edu/administration/policies/section-v-student-affairs/v-100b) at all times.

Participation (20% of Final Grade)

To prepare students to be effective participants in security policy debates, class participation counts for 20% of the grade. Students are expected to prepare thoroughly, attend consistently, and engage actively in class discussions. Please e-mail me in advance if you must miss class for any reason.

Students are also encouraged to use the on-line forum to continue discussions begun in class; to share relevant news, articles, and event announcements; and to pose questions about readings that they want to discuss during the next class.

Mid-Term Exam (30% of Final Grade)

A mid term exam will be given to test student's mastery of the high level technical underpinnings of the global telecommunications environment, the current set of threat actors, internet governance structures, and the general types of cyber incidents found today.

Group Exercise (20% of Final Grade)

A group exercise will be administered to highlight the challenges policy makers face in allocating scare resources in defending critical services and organizations. Students will be grouped into teams and provided instructions prior to the activity. Grades will be determined based on the thoroughness of their approach to addressing the problem.

Final Memo (30% of Final Grade)

A final policy memo question will be provided to students. While the question will focus on a topic germane to areas we discuss in the second half of the course. A thoughtful response would leverage much of the material covered throughout the term.

READINGS AND RESOURCES

Required Texts:

National Research Council. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. Washington, DC: The National Academies Press, 2014. Free download: http://www.nap.edu/openbook.php?record_id=18749

Libicki, M "Cyberspace in Peace and War", Naval Institute Press, Annapolis Md, 2016

"Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"

Additional Readings:

In addition to the required texts, there are supplemental readings identified on a weekly basis. Students are expected to review the materials prior to the course lecture to maximize the value obtained from in class discussions.

SCHEDULE

Week 1 (1/25): Technical Revolutions, Economic Interdependence, and the Cyber Problem

Required Readings:

- Libicki pp 32-57
- Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics*, April 19, 1965 https://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf

Week 2 (1/30, 2/1): The Internet and Evolving Threat Landscape

Required Readings:

- Leiner, Cerf, et. al., A Brief History of the Internet – pp. 1-9, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.2474&rep=rep1&type=pdf
- National Research Council, "At the Nexus of Cybersecurity and Public Policy", Chapters 1 & 2 , http://docs.house.gov/meetings/IF/IF02/20150303/103079/HHRG-114-IF02-20150303-SD006.pdf
- James R. Clapper, Worldwide Threat Assessment of the US Intelligence Community (Feb. 2015) – pp. 1-4, https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf
- Larry Clinton, "The Evolving Cyberthreat and an Architecture for Addressing it," *NTDA,* pp. 37-42.
- Lewis, James Andrew, 2013. "Significant Cyber Incidents Since 2006." Center for Strategic and International Studies (skim). https://www.csis.org/programs/technology-policy-program/cybersecurity-and-warfare/other-projects-cybersecurity-0

Week 3 (2/6, 2/8): The Global Telecommunications Architecture and Governance

Required Readings:

- Tallin Manual 2.0 pp 284-298
- Andreas Schmidt, "At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker," Telecommunications Policy 36, 3 (July 2012) 451-461
- Joseph S. Nye, Jr. The Regime Complex for Managing Global Cyber Activities, https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf
- Chin, "Facebook and Microsoft's big undersea cable is finally finished", Sept 22nd 2017, Masahable.com, http://mashable.com/2017/09/22/microsoft-facebook-marea-cable/?utm_cid=mash-com-fb-main-link#F9FfPB3nxkq3

Week 4 (2/13, 2/15): Actors and Motivations

Required Readings:

- Pages 2-5 of Cybersecurity Threats Impacting the Nation, Testimony of Gregory C. Wilshusen Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, Tuesday, April 24, 2012 http://www.gao.gov/assets/600/590367.pdf
- Libicki pp 100-113, pp 196-208
- Fire Eye, "APT28 Cybergroup Activity", https://www.securitycasestudy.pl/wp-content/uploads/2015/05/SCS14%E2%80%93MOstrowski.TPietrzyk.pdf
- Knafo "Anonymous and the War Over the Internet", Huffington Post 2012, https://www.huffingtonpost.com/2012/01/30/anonymous-internet-war_n_1233977.html
- Symantec, "Internet Security Threat Report", April 2016 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
- Singer and Friedman, pp. 77 -114. (Cyberterrorists)

Week 5 (2/20, 2/22): Breaking Down a Hack: Exploits, Tools, Infrastructure, and Attribution

Required Readings:

- Libicki pp 238-248
- Tallinn Manual 2.0 pp 87-111
- Lockheed Martin Cyber Kill chain https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- Boebert, W. Earl, "A Survey of Challenges in Attribution," in National Research Council, Proceedings of a Workshop on Deterring Cyberattacks, 2010, pp. 41-52. https://www.nap.edu/read/12997/chapter/5#43
- Neil Ungerleider, How Spies, Hackers, And the Government Bolster A Booming Software Exploit Market. Fast Company May 1, 2013. http://www.fastcompany.com/3009156/the-code-war/how-spies-hackers-and-thegovernment-bolster-a-booming-software-exploit-market Supplemental Material

Week 6 (2/27, 2/29): Primary Effects and Secondary Effects of Cyber Attacks-Exploitation and Disruption

Required Readings

- Libicki pp 59-63, 129-131
- Michael Sentonas, "The Economic Impact of Cybercrime and Cyber Espionage," Security Solutions (Australia) 11 March 2014 http://www.securitysolutionsmagazine.biz/2014/03/11/the-economic-impact-of-cybercrime-and-cyber-espionage/ Accessed – 3 November 2017
- The Economic Impact of Cybercrime and Cyber Espionage (Washington DC: CSIS, 2013)

https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4.pdf Accessed - 3 November 2017

- John Gelinne, J. Donald Fancher, and Emily Mossburg "The Hidden Costs of an IP Breach: Cyber Theft and the Loss of Intellectual Property", Deloitte Insights 25 July 2016.
- https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html Accessed – 3 November 2017
- Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress " The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation", pp 5-10 (executive summary), and 15-23 (Timeline of key events), https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf
- https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
- Weinburg, "Maersk Says June Cyberattack will Cost it up to $300 Million", Bloomberg Business, August 16th 2017, https://www-bloomberg-com.cdn.ampproject.org/c/s/www.bloomberg.com/amp/news/articles/2017-08-16/maersk-misses-estimates-as-cyberattack-set-to-hurt-third-quarter
- Lillian Ablon, Martin C. Libicki, Andrea A. Golay, Markets for cybercrime tools and stolen data, RAND Corporation http://www.rand.org/pubs/research_reports/RR610.html

Week 7 (3/6, 3/8): Cyber Warfare and Espionage

Required Readings

- Libicki, pp. 129-195.
- "Demystifying the Title 10-Title 50 Debate", Harvard National Security Journal , 2012 http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Wall.pdf (Skim)
- Ryseff, "The Maliciously Formed Packets of August: Cyberwarfare and the Offense-Defense Balance", CSIS, September 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/170907_Ryseff_Cyberwarfare_And_the_Offense_Defense_Balance.pdf?wmiLQuqdILwMEO5YnxfQJY1IA4Ytbp_2
- Langner, Ralph, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," (Arlington VA: The Langner Group), Nov. 2013. Pp. 3-23
- Lewis, "The Likelihood of North Korean Cyber Attacks", CSIS, September 2017, https://www.csis.org/analysis/likelihood-north-korean-cyber-attacks
- Ars Technica, "Justice Department goes nuclear on Google in search warrant fight", September 2017, https://arstechnica.com/tech-policy/2017/09/justice-department-goes-nuclear-on-google-in-search-warrant-fight/

Week 8 (3/13, 3/15): Review and MIDTERM EXAM

****Spring Break** 3/20-3/22**

Week 9 (3/27, 3/29): When does a Cyber threat move from a Private Problem to a Public Concern?

Required Readings:

- PPD-41, "Presidential Policy Directive 41 : United States Cyber Incident Coordination, White House 2016 https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
- NIST, "Framework for Improving Critical Infrastructure Cybersecurity", pp 3-6 https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
- Harry, C "A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact", CISSM Working Paper 2015 (Skim)

Week 10 (4/3, 4/5): Team Exercise – Protecting Organizations and Critical Infrastructure

Week 11 (4/10, 4/12): Assessing Cybersecurity Risk for Organizations and Protecting Critical Infrastructure

Required Readings:

- Libicki, pp. 114-128
- EO 13618: Assignment of National Security and Emergency Preparedness Functions (2012) https://obamawhitehouse.archives.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-
- EO 13636: Improving Critical Infrastructure Cybersecurity (2015) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- PPD-21: Critical Infrastructure Security and Resilience (2015) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- Presidential Decision Directive 63: Critical Infrastructure Protection https://fas.org/irp/offdocs/pdd/pdd-63.htm
- NIST, "Framework for Improving Critical Infrastructure Cybersecurity" https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf **(Skim)**
- "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", White House, May 2017 https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

Week 12 (4/17, 4/19): Defending Critical Systems: Government Structures in Dealing with Cybersecurity Incidents (Guest Lecture)

Required Readings:

- Bayuk et al, "Cyber Security Policy Guidebook" Chapter 7, pp 211-233, http://pdf.th7.cn/down/files/1312/Cyber%20Security%20Policy%20Guidebook.pdf
- Eric A. Fischer, Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions, Congressional Research Service, R42114, June 20, 2013, http://www.fas.org/sgp/crs/natsec/R42114.pdf
- GAO Testimony Before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space, and Technology, House of Representatives "Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies", July 2015 http://www.gao.gov/assets/680/671253.pdf
- Public Law 113-283 Federal Information Security Modernization Act (FISMA), Skim
- Larry Jones. "Establishing the Structure, Authority, and Process to Create an Effective Program." *NTDA,* pp. 91-101

Week 13 (4/24, 4/26): International Law and Armed Conflict in Cyberspace (Guest Lecture)

Required Readings

- Thomas Rid, "What is Cyberwar?" Chapter 1 of Cyberwar Will Not Take Place. 2013 Excerpts from Owens, Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack, ISBN 9780309138505 National Academies Press (2009)
- Tallinn Manual pp 79-153 (skim)
- Osula and Raoigas "International Cyber Norms: Legal, Policy, & Industry Perspectives" https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf
- Dunlap, Perspectives for Cyber Strategists on Law for Cyberwar (Strategic Studies Quarterly, Spring 2011)
- Department of Defense Strategy for Operating in Cyberspace, http://www.defense.gov/news/d20110714cyber.pdf , Pages 1 through 11
- Liff, Adam P., 2011. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," Journal of Strategic Studies, vol. 35, pp. 401-28
- Belk, Robert and Matthew Noyes, 2012. On the Use of Offensive Cyber Capabilities (JFK School of Government), pp. 75-110.
- Gerstein, "Define Acceptable Cyberspace Behavior", Rand, 2015. https://www.rand.org/blog/2015/09/define-acceptable-cyberspace-behavior.html

Week 14 (5/1, 5/3): Strengthening National Response to Cyberattack: Cooperation, Sanctions, and Deterrence

Required Readings:

- Libicki pp 196-237, 285
- Executive Order 13757 " Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" of December 28, 2016
- Farnsworth, Timothy, "China and Russia Submit Cyber Proposal," Arms Control Today, 2011, pp. 35-36.
- Botting, Alexander "The Road Ahead for Transatlantic Cybersecurity Cooperation" https://www.uschamber.com/above-the-fold/the-road-ahead-transatlantic-cybersecurity-cooperation
- Lewis "Sustaining Progress in International Negotiations on Cybersecurity", CSIS, July 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170725_Lewis_IntlNegotiationsCybersecurity_Web.pdf?zYqP8XAS14o4OU2Sqr7dn4WitgANhtck

Optional Readings:

- Steinbrunner, John, "Prospects for Global Restraint on Cyberattack," Arms Control Today, 2011, pp. 21-26.
- "Former officials buck White House adviser's comments about government hacking", September 8th 2017, Cyberscoop.com, https://www.cyberscoop.com/tom-bossert-government-hacking/

Week 15 (5/8, 5/10): Expanding Attack Surfaces: The Opportunities and Concerns Surrounding IoT and Cloud Computing

Required Readings:

- Executive Office of the President, International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World, (May 2011) https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf Accessed – 6 November 2017
- "Public Policy for the Cloud: How Policy Makers Can Enable Cloud Computing", Computer & Communications Industry Association, (2011) pp 9-12 , http://www.ccianet.org/wp-content/uploads/library/CCIA%20-%20Public%20Policy%20for%20the%20Cloud.pdf
- EU Commission Press Release "EU Commission and the United States agree on new framework for transatlantic data flows: The EU-US Privacy shield", 2016
- Fischer, "The Internet of Things: Frequently Asked Questions" Congressional Research Service, Oct 2015 https://fas.org/sgp/crs/misc/R44227.pdf
- Anderson et al "Autonomous Vehicle Technology" Rand Corp, https://www.rand.org/pubs/research_briefs/RB9755.html?utm_source=t.co&utm_medium=rand_social
- Greenburg, A "Securing Driverless Cars from Hackers is Hard. Ask the Uber Guy Who Protects Them" , Wired, 2017 https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/
- Assante & Bochman "IoT, Automation, Autonomy, and Megacities in 2025: A Dark Preview", Center for Strategic & International Studies, April 2017, https://csis-

prod.s3.amazonaws.com/s3fs-public/publication/170427_Assante_Megacities_Web.pdf?EyNZo5k6LSorErmOo_1_roQHCOQwGL6v

- Bekara, “Security Issues and Challenges for the IoT-based Smart Grid”, International Workshop on Communicating Objects and Machine to Machine for Mission Critical Applications, 2014.
- Harry, “IoT Cybersecurity Act of 2017: A Necessary but Insufficient Approach”, CISSM, August 2017, http://www.cissm.umd.edu/publications/iot-cybersecurity-act-2017-necessary-insufficient-approach