INST408V/PLCY388C, Spring 2019
Cybersecurity Policy: Practical Hacking for Policy Makers
PHY 4221; Tu & Th, 3:30-4:45pm

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, response, critical infrastructure risk management, and privacy. 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 security and legal questions countries struggle to solve with respect to cybersecurity including abuse of networks and resources and violations of privacy
6) Understand international efforts to promote responsible behavior among nations in cybersecurity.

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 (15% of Final Grade)

To prepare students to be effective participants in security policy debates, class participation counts for 10% 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. The expectation is that each student will at a minimum post at least one article of interest over the course of the semester, and *lead* a class discussion surrounding its relevance to any topic we are covering in the course.

Mid-Term Exam (35% 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 (15% 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 (35% of Final Grade)

A final exam will be given to test mastery of the course's content.

READINGS AND RESOURCES

Required Texts:

Required

Richard Harrison Cyber Insecurity, Published by Rowman and Littlefield, 2016

ISBN 978-1-7284-2

Optional

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

Additional Readings:

In addition to the required texts, there are often 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 (1/29, 1/31): What do we Mean by Cybersecurity and Should We Care?

Required Readings:

- 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
- 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 (2/5,2/7): The Development of the Internet and Evolving Threat Landscape

Required Readings:

- SANS 2017 Threat Landscape Survey https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910
- 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

Optional:

- 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 (2/12, 2/14): The Global Telecommunications Architecture and Governance

Required Readings:

- Vangie Beal "The 7 layers of the OSI Model", Webopedia https://www.webopedia.com/quick_ref/OSI_Layers.asp
- Harrison, Chapter 11 Pgs 173-190
- Joseph S. Nye, Jr. "The Regime Complex for Managing Global Cyber Activities", Global Commission on Internet Governance" 2014 https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf

Optional:

- Tallin Manual 2.0 pp 284-298
- 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 (2/19, 2/21): Expanding Attack Surfaces: The Opportunities and Concerns Surrounding IoT and Cloud Computing and their use in Smart City Infrastructure

Required Readings:

• Harrison Chapter 4 pgs 47-68

• 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

•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

Optional:

• "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

• 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/

• 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.

Week 5 (2/26, 2/28): Threat Actors and Motivations

Required Readings:

- Harrison, Chapter 6 Pgs 89-101
- 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
- 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

Optional Readings

- 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
- 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 6 (3/5, 3/7): Breaking Down a Hack: Exploits, Tools, Infrastructure, and Attribution

Required Readings:

- Harrison, Chapter 15 pgs 241-255
- 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

Week 7 (3/12, 3/14): Primary Effects and Secondary Effects of Cyber Attacks-Exploitation and Disruption

Required Readings

- Charles Harry, "A Proposed Hierarchical Taxonomy for Assessing the Primary Effects of Cyber Events: A Sector Analysis 2014-2016" CISSM Working Paper http://www.cissm.umd.edu/sites/default/files/Cyber-Taxonomy-022818.pdf
- 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

Optional Readings

- 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

- 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

Week 8 (3/19, 3/21)

****** Spring Break******

Week 9 (3/26, 3/28)

******Review and Midterm******

Week 10 (4/2, 4/4): When does a Cyber threat move from a Private Problem to a Public Concern?

**** UMD Cyber Security Summit (4/4-4/5)****

Required Readings:

- 2018 US Cybersecurity Strategy https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

- 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

Week 11 (4/9, 4/12): Team Exercise – Protecting Organizations and Critical Infrastructure

Week 12 (4/16, 4/18): Assessing Cybersecurity Risk for Organizations and Protecting Critical Infrastructure

Required Readings:

- Harrison Chapter 3 Pgs 31-45
- EO 13636: Improving Critical Infrastructure Cybersecurity (2015) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- NIST, "Framework for Improving Critical Infrastructure Cybersecurity" https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf **(Skim)**

Optional Readings

- "EO 13800: Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", White House, May 2017
- 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-
- 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

Week 13 (4/23, 4/25): Cyber Warfare, Espionage, and the Title 10/50 Debate

Required Readings

- Harrison, Chapter 16 Pgs 259-276
- "Demystifying the Title 10-Title 50 Debate", Harvard National Security Journal , 2012

http://harvardnsj.org/wp-content/uploads/2012/01/Vol-3-Wall.pdf

Optional Reading

- (Skim) Department of Defense Strategy for Operating in Cyberspace, http://www.defense.gov/news/d20110714cyber.pdf , Pages 1 through 11
- 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)
- 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 https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Week 14 (4/30, 5/2): National Response to Cyberattack

Required Readings:

- Harrison Chapter 2 pgs 19-30 & Chapter 5 pgs 69-85
- Executive Order 13757 " Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" of December 28, 2016
- Botting, Alexander "The Road Ahead for Transatlantic Cybersecurity Cooperation" https://www.uschamber.com/above-the-fold/the-road-ahead-transatlantic-cybersecurity-cooperation

Optional Readings:

- Steinbrunner, John, "Prospects for Global Restraint on Cyberattack," Arms Control Today, 2011, pp. 21-26.
- Tallinn Manual pp 79-153 (skim)
- 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

Week 15 (5/7, 5/9): International Law and Armed Conflict in Cyberspace

** Revise Lecture**

Required Readings

- Gerstein, "Define Acceptable Cyberspace Behavior", Rand, 2015. https://www.rand.org/blog/2015/09/define-acceptable-cyberspace-behavior.html
- 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)

Week 16 (5/14, 11/29): Criminal Abuse and Privacy

Required Readings

- Harrison Chapters 8, 9, and 20
- Susan Mcgregor and Hugo Zylberberg "Understanding the General Data Protection Regulation: A Primer for Global Publishers" Columbia Journalism Review https://www.cjr.org/tow_center_reports/understanding-general-data-protection-regulation.php/
- California Assembly Bill No. 375 https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375