PUAF 688C, Spring 2018
Cybersecurity Policy: Problems, Actors and Prospects
Schedule, Tuesdays – 4:15 - 6:45 pm; Room: Dean's Conference Room

Professor David Mussington
2101 Van Munching Hall
bmussing@umd.edu
301.405.4794
Office Hours: By Appointment

Course Objectives

This course is designed to introduce students to the complexities of cybersecurity policy. Most popular literature treats cybersecurity risks as a technical problem, with threats and vulnerabilities appearing often seemingly at random. This course will refocus student's attention on the interplay of technical, economic and political factors that create demand for cybersecurity policies, and influence the deployment of solutions – both in the public and private sectors.

The undoubted prominence of cybersecurity in media and political debates in recent years has not produced widespread public understanding of the risks and opportunities involved of cyberspace. While individual products (e.g., Smart Phones) and digital services (delivered via the Internet) are adopted – with market fashion and trends influencing global technology development, vulnerabilities and their exploitation by hackers, criminals or agencies of nation-states are often treated as hidden factors – potentially unknowable and of little interest to customers.

There is an unavoidable US–centric aspect to this course. The literature on cybersecurity policy is dominated by US scholars and approaches, current and former government officials and industry technology suppliers and business – oriented commentators. Important contributions, however, are made by scholars and researchers from elsewhere in the world. An effort is made to integrate some of this work in selected readings that expand the core reading list presented below. These added resources are signified by the addition of an asterisk (*) adjacent to the reference item. It is of course the case that many countries have begun to develop national approaches to cybersecurity policy and strategy. Later in the course we examine some of these approaches from the vantage point of a better understanding of US approaches over the last 2 decades. This provides a basic baseline for comparison, and an added appreciation of the unique factors in different national security and economic circumstances that impact the approaches adopted by both nation states and private sector organizations.

This course will provide students with a conceptual framework for understanding the emergence of the cybersecurity policy issue set, with parallel economic, technical, and political factors influencing the policy setting. Equipped with a better grounding in policy supply and demand, students will then be exposed to the challenges involved in reconciling sometimes competing policy goals such as privacy protection, national security, economic growth, and open access to information and education.

Syllabus Version: 4

Required Readings and Additional Support Materials

The primary texts for this course are: Martin Libicki, Cyberspace in Peace and War (Annapolis, MD: US Naval Institute Press, 2016); and Thomas Rid, Rise of the Machines: A Cybernetic History (New York: W.W. Norton, 2016) These books are mandatory for the course, but are supplemented by selected

sections in additional sources. The following books will provide chapters addressing issues that will be raised in course lectures and for class readings (in addition to being useful background material for student assignments).

Secondary Texts

Kim Zetter, Countdown to Zero Day: STUXNET and the Launch of the World's First Digital Weapon (New York: Crown Publishers, 2014).

Adam Segal, The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age (New York: Council on Foreign Relations, 2016)

Fred Kaplan, Dark Territory: The Secret History of Cyber War (New York: Simon and Schuyler, 2016).

Jason Healey (Ed.) A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Washington DC: Cyber Conflict Studies Association (CCSA)/Atlantic Council, 2013)

Nigel Inkster China's Cyber Power (London: IISS, 2016)

Adam Segal and Hannah Pitts (Eds.) Cyber Conflict After STUXNET: Essays from the Other Bank of the Rubicon (Vienna, VA: CCSA, 2016)

Derek Reveron (Ed.) Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World (Washington DC: Georgetown University Press, 2012)

Richard A. Clarke and Robert K. Knake Cyber War: The Next Threat to National Security and What to Do About It (New York: Harper Collins (Ecco), 2010)

Ed Finn What Algorithms Want: Imagination In the Age of Computing (Cambridge, MA: MIT Press, 2017)

Samuel Charap and Timothy J. Colton Everyone Loses: The Ukraine Crisis and the Ruinous Contest for Post-Soviet Eurasia (London: IISS, 2017)

(*) Evolution of the Cyber Domain: The Implications for National and Global Security (London: International Institute for Strategic Studies, 2015)

Lastly, a number of government reports, policy and strategy documents from the Government Accountability Office, the Congressional Research Service, DHS, National Intelligence Council (NIC), and Federally Funded Research and Development Centers (FFRDCs) will be used, alongside analyses produced by university research institutions and private sector commercial enterprises - in order to round out the vulnerability and cyber risk picture presented. This list will be augmented as I find additional sources during the semester.

(*) Anna-Maria Osula and Henry Roigas (Eds.) International Cyber Norms: Legal, Policy and Industry Perspectives Tallinn: NATO Cooperative Cyber Defence Center of Excellence (CCDCOE), 2016)

David Kim and Michael G. Solomon Fundamentals of Information Systems Security (Third Edition), (Burlington, MA: Jones and Bartlett, 2018)

Roger C. Molander, Peter A. Wilson, David A. Mussington, Richard F. Mesic Strategic Information Warfare Rising (Washington DC: RAND, 1998)

Assignments

- Policy Briefs – 3 pages, double spaced. Briefs should explain a key dimension or aspect of a cybersecurity topic based on the interplay of economic, technical and political factors. Three of these briefs will be required during the semester.
- One Op-Ed or Opinion Paper. This should be submitted in a format ready to be sent to a media outlet. This assignment is due at the mid-Semester break. It can be submitted earlier.
- Working as a team (3-4 students), an analysis of a non - US cyber strategy, or a comparative analysis of US cybersecurity strategies with at least 2 (two) foreign strategies, must be prepared. The focus here is on the priorities articulated in the strategy or policy, the resources allocated to strategy implementation, and the time-frame envisioned for shaping outcomes. Each group will do a 1-hour presentation to the class, and submit a brief paper (not exceeding 10 pages (not incl. references) summarizing the presentation, one week after the presentation due date.
- US Cybersecurity Policy (Individual) Presentation – addressing one or more issues raised in the national and international cybersecurity policy debate since the Year 2000. The selection of issues here is potentially vast, ranging from: national and homeland security, industry concerns with theft of intellectual property, economic competition and digital services, reconciling individual privacy with the power of big data and data-enabled surveillance, etc. I am willing to consider a broad range of topics.

Summary of Assignments	Per Cent of Grade
Policy Briefs	30 Per Cent
Op-Ed or Opinion Paper	10 Per Cent
Foreign Cybersecurity Strategy Analysis (Group)	30 Per Cent
US Cybersecurity Policy Presentation	20 Per Cent
Class Participation	10 Per Cent
	100 Per Cent

Schedule of Lectures and Readings

Session (0) Introductions and Course Overview

- Basic assumptions
- Definitions: what is cyberspace?
- Sources
- Technical and Policy Constraints and Challenges
- Research and Participation Expectations
- Assignments

Weeks 1 and 2 (1/25/2018 – 1/30/2018) - Risk Identification and Policy Frameworks for Cybersecurity – Basic Concepts

Discussion Issues / Part 1:

- What is important, and how is it counted?
- Networks and Data in Economy and Government
- The Emergence of Digital Services

David Kim and Michael G. Solomon, Fundamentals of Information System Security (Burlington, MA: Jones and Bartlett, 2018), Chapters 1 and 2. "The Need for Information Security," and "The Internet of Things is Changing How We Live," pp. 1-71.

Peter Sommer and Ian Brown, Reducing Systemic Cybersecurity Risk (January 14, 2011). Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3. Available at https://ssrn.com/abstract=1743384 (chapters on: critical infrastructures: cyber elements, risk analysis and the broader context, and specific systemic threats), Accessed – 30 January 2018

Aaron Kleiner, Paul Nicholas and Kevin Sullivan Linking Cybersecurity Policy and Performance (Redmond, WA: Microsoft Trustworthy Computing, 2013). http://www.ilsole24ore.com/pdf2010/SoleOnLine5/_Oggetti_Correlati/Documenti/Tecnologie/2013/02/SIR-Special-Edition-Security-Atlas-whitepaper.pdf Accessed - 3 November 2017

Discussion Issues / Part 2:

- Defining Cybersecurity and Critical Infrastructure
    - Foundational Policies and Risk Appreciations
    - How many, are they truly critical?

- PDD-63 and Y2K as Framing Events
    - Public Sector Views
    - Private Sector Views

Libicki, Cyberspace in Peace and War, Chapter 2. "Some Basic Principles," pp. 19-31.

Clarke and Knake, Cyber War, Chapter 3. "The Battlespace," pp. 69-99.

Scott Ackerman, "How Y2K Changed the Field of Cybersecurity," Security Magazine 24 October 2014, (https://www.securitymagazine.com/articles/85866-how-y2k-changed-the-field-of-cybersecurity-technology); Accessed – 3 November 2017

Earl D. Mathews, "Incoming: The Lessons of Y2K for Cybersecurity," AFCEA Signal 1 June 2017. (https://www.afcea.org/content/Article-incoming-lessons-y2k-cybersecurity); Accessed – 3 November 2017

David Mussington, Concepts for Critical Infrastructure Protection: Relating Y2K to CIP Research and Development (Santa Monica: RAND/Science and Technology Policy Institute, 2002) (https://www.rand.org/pubs/monograph_reports/MR1259.readonline.html); Accessed - 3 November 2017

Week 3 (2/6/2018) - Conceptualizing Military Cybersecurity

Libicki, Cyberspace in Peace and War, Chapter 14. "Is Cyberspace a Warfighting Domain," pp. 158-168; and Chapter 17. "Strategic Cyberwar", pp. 187-195.

Jarno Limnell, "The Cyber Arms Race is Accelerating – What are the Consequences?", Journal of Cyber Policy, Vol. 1, Issue 1 (February 2016).

Segal, The Hacked World Order, Chapter 2. "The Anatomy of Cyber Power," pp.31-56.

Clarke and Knake, Cyber War, Chapter 5. "Toward a Defensive Strategy," pp. 151-178; and Chapter 6. "How Offensive?" pp. 179-218.

Zetter, Countdown to Zero Day, Chapter 16. "Olympic Games," pp. 308-335.

Kaplan, Dark Territory, Chapter 9. "Cyber Wars," pp. 145-169.

Discussion Issues:
- Defining Military Cyber Capabilities
- Offense and Defense in Cyberspace Operations
- Defense and Deterrence in Cyberspace

Week 4 (2/15/2018) - Conceptualizing Civilian/Commercial Cybersecurity

Libicki, Cyberspace in Peace and War, Chapter 6. "What the Government Can and Cannot do," pp. 70-88.

Department of Homeland Security Office of Infrastructure Protection, Commercial Facilities Sector Cybersecurity Framework: Implementation Guidance 2015/ https://www.dhs.gov/sites/default/files/publications/commercial-facilities-cybersecurity-framework-implementation-guide-2015-508.pdf Accessed - 3 November 2017

Information Technology Industry Council, The IT Industry's Cybersecurity Principles for Industry and Government (Washington DC: ITIC, 2011) v.3.0 https://www.itic.org/dotAsset/31bcabf8-514e-498e-a0af-7ed37e3a92ef.pdf Accessed - 3 November 2017

Commercial/Civil Cybersecurity Snapshot, (Obama Whitehouse Archives) https://obamawhitehouse.archives.gov/files/documents/cyber/Comm-Civil_CyberSnapshotPoster.pdf Accessed - 30 January 2018

Accenture High Performance Security Report 2016 – Public Service, Rebooting Public Sector Cybersecurity https://www.accenture.com/t20170227T025533Z__w__/us-en/_acnmedia/PDF-41/Accenture-FY17-AFS-Rebooting-Public-Sector-Cybersecurity-Research.pdf Accessed - 30 January 2018

Discussion Issues:
- Priorities
- Decision making and Incentives for Cybersecurity Actions
- Regulation and Cyber Risk Management

(Potential Policy Brief Due Date (#1))

Week 5 – (2/20/2018) - Critical Infrastructure Priorities and Dependencies

Libicki, Cyberspace in Peace and War, Chapter 9. "Return to Vendor", pp. 114-119; and Chapter 10. "Cybersecurity Futures," pp. 120-128.

Argonne National Laboratory, Risk and Infrastructure Science Center – Global Security Sciences Division - "Analysis of Critical Infrastructure Dependencies and Interdependencies", (2015)

http://www.ipd.anl.gov/anlpubs/2015/06/111906.pdf Accessed - 3 November 2017.

- National Security

Sidney M. White and Jim Halpert, "Cybersecurity Executive Order Escalates Cybersecurity to Greater Priority –Top Points About Critical Infrastructure", DLAPiper Cybersecurity Alert, 12 June 2017 https://www.dlapiper.com/en/us/insights/publications/2017/06/executive-order-escalates-cybersecurity-priority/ Accessed – 3 November 2017

(*) Lior Tabansky "Cybercrime: A National Security Issue?" Military and Strategic Affairs vol. 4, no. 3 (December 2012), pp. 117-136 https://i-hls.com/wp-content/uploads/2013/03/Cybercrime-A-National-Security-Issue.pdf Accessed - 3 November 2017

(*) Peter Grabosky, "Organized Crime and National Security", Korean Institute of Criminology Research Report Series 13-B-01 Information Society and Cybercrime: Challenges for Criminology and Criminal Justice., Seoul. pp.19-30 RegNet Research Paper No. 2014/40 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2464377 Accessed – 3 November 2017

Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," International Security, Vol 38, No. 2 (Fall 2013), pp. 7-40.

- Crime Control

Federal Bureau of Investigation – What we Investigate -- https://www.fbi.gov/investigate/cyber Accessed 3-November 2017

Ron Cheng, "US and China Department Heads Discuss Cybersecurity and Law Enforcement Cooperation" Forbes, 13 October 2017. https://www.forbes.com/sites/roncheng/2017/10/13/u-s-and-china-department-heads-discuss-cybersecurity-and-law-enforcement-cooperation/#69fc4b291afb Accessed – 3 November 2017

Steve Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019," Forbes, 17 January 2016 https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7e27f3143a91 Accessed – 3 November 2017

Brian Robinson (CyberEye), "The Equifax Breach is Teaching the Same Old Lessons," GCN v36, issue 6 (October/November 2017), p. 10. https://gcn.com/blogs/cybereye/2017/09/equifax-open-source-cybersecurity.aspx Accessed - 3 November 2017

- Economic Competitiveness

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

Potomac Institute for Policy Studies, Cyber Readiness Index Reports – Country Profiles
http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

Discussion Issues:
- National Security Criteria
  - Defense Policy Priorities
  - Intelligence Priorities
- Economic Competitiveness Criteria
  - Trade and Business
  - Legacy Effects
- Crime Control Criteria
  - Local and Global Impacts
  - Strategic Crime

(Mid Semester Assignment due)

Week 6 (2/27/2018) - Cybersecurity: Risk and Threat Trends – Peer and Non-Peer Actors

Libicki, Cyberspace in Peace and War, Chapter 23. "Attribution," pp. 238-250.

Jon R. Lindsay "The Impact of China on Cybersecurity: Fiction and Friction," International Security, Vol. 39, Issue 3 (Winter 2014/2015), pp. 7-47.

Department of Defense - Defense Science Board Task Force Report: Resilient Military Systems and the Advanced Cyber Threat (Washington DC: Department of Defense, October 2012) https://www.acq.osd.mil/dsb/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf Accessed - 3 November 2017

Discussion Issues:
- Long-term Trends
- State Practices and International Cybersecurity Challenges

(Potential Policy Brief Due Date (#2))

Week 7 (3/6/2018) - Cybersecurity and Technology: Vulnerabilities

Libicki, Cyberspace in Peace and War, Chapter 4. "The Search for Cybersecurity", pp. 41-58.

"Military Cyber Affairs", in Evolution of the Cyber Domain, pp. 159-189.

Thomas Rid "Chapter 8. "War", in Rise of the Machines, pp. 295-339.

Roderick Jones, "Wi-Fi Vulnerability Illustrates the Need for Better Cybersecurity," The Hill Newspaper, 18 October 2017, http://thehill.com/opinion/cybersecurity/356077-wi-fi-vulnerability-illustrates-the-need-for-better-cybersecurity Accessed - 3 November 2017

Discussion Issues:
- Trends in Vulnerability and Risk Management

- Public and Private Sector Perspectives
- Impediments to Progress

Week 8 (3/15/2018) - Cybersecurity and Technology Trends: Attacker Exploitation

Libicki, Cyberspace in Peace and War, Chapter 5. "Defending Against Attacks of High and Broad Consequence," pp. 59 – 69.

Brandon I. Koerner "Inside the OPM Hack That Shocked the US Government," Wired Magazine 23 October 2016. https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ Accessed – 3 November 2017

Shaun Waterman "Latest Cyber 'Moon Shot' Idea is a National DDOS Defense System" Cyberscoop 3 November 2017. https://www.cyberscoop.com/cyber-moonshot-ddos-defense-phil-quade-fortinet/ Accessed – 3 November 2017

Phil Goldstein "NASA Faces Down New Cybersecurity Vulnerabilities," FedTech 31 March 2017 https://fedtechmagazine.com/article/2017/03/nasa-faces-down-new-cybersecurity-vulnerabilities Accessed - 3 November 2017.

Robert M. Lee et al., Analysis of the Cyber Attack on the Ukrainian Power Grid (Electricity Information Sharing and Analysis Center (E-ISAC), SANS Industrial Control Systems,18 March 2016 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf Accessed - 3 November 2017

John Leyden "BlackEnergy Power Plant Hackers Target Ukrainian Banks," The Register 15 December 2016. https://www.theregister.co.uk/2016/12/15/ukraine_banks_apt/ Accessed – 3 November 2016

Dean Beeby, "State-sponsored Cyber Attacks on Canada Successful About Once a Week," http://www.cbc.ca/news/politics/cyber-attacks-canada-cse-1.4378711 Accessed - 3 November 2017

Discussion Issues:
- Peer and Non-Peer Threats
- States and Markets for Malware
- Critical Infrastructure Targets

Week 9 (3/27/2018) - Cybersecurity and Technology: Proposed Solutions

David Mussington, Concepts for Critical Infrastructure Protection: Relating Y2K to CIP Research and Development (Santa Monica: RAND/Science and Technology Policy Institute, 2002) (https://www.rand.org/pubs/monograph_reports/MR1259.readonline.html); Accessed - 3 November 2017

Discussion Issues:
- Research and Development
- Operational and Best Practice Steps
- Standards and Regulation

Week 10 (4/3/2018) - International Cybersecurity Policy: Varying Approaches

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

US Department of State, Department of State International Cyber Policy Strategy, March 2016 [Required by Public Law 114-113, Division N, Title IV, Section 402)
https://www.state.gov/documents/organization/255732.pdf Accessed - 6 November 2017
Ministry of the Interior, Germany Cybersecurity Strategy for Germany (2011)
https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile Accessed – 6 November 2017

Her Majesty's Government (UK) National Cybersecurity Strategy, 2016-2021,
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf Accessed - 6 November 2017

Public Safety Canada, Canada's Cyber Security Strategy (2016)
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx Accessed - 6 November 2017

Discussion Issues:
- Militarized or Civilian Approaches
- Private Sector – Centric or Government Oversight Bias

Week 11 (4/10/2018) - National Cybersecurity Strategies

- Group Presentations (3-4 people)
- Analysis and Critique

Week 12 (4/17/2018) - May 1 -- International Cybersecurity Norms – Proposals and Agreements

Libicki, Cyberspace in Peace and War, Chapter 32. "Norms for Cyberspace", pp. 317-332.

Osula and Roigas, International Cyber Norms, Chapter 11. "Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms," pp. 221-242.

Melissa Hathaway, "Getting Beyond Norms When Violating the Agreement Becomes Customary Practice," CIGI Papers No. 27, (April 2017)
https://www.cigionline.org/sites/default/files/documents/Paper%20no.127.pdf
Accessed – 3 November 2017

Discussion Issues:
- History
- Problems and Prospects
- Strategic Objectives

Week 13 (4/24/2018) - May 8 -- Cybersecurity Strategy: What is Missing from Real-World Strategy and Policy Approaches -- and what impedes innovation?

Discussion Issues:
- Public and Private Sector Capabilities
- Dealing with Cybercrime, Intellectual Property Theft and Economic Competition
- Asymmetric Risk Management Requirements

(Potential Policy Brief due date (#3))

Week 13 (4/24/2018) – Advanced Topics / Guest Speaker (Peter Wilson, RAND Corporation (Invited)

Week 14 (5/1/2018) – Advanced Topics

Week 15 (5/18/2018) – Advanced Topics