Reading Group:
Cybersecurity Technology and Policy

January 13, 2019

Time and Place

This reading group will meet Tuesdays 1-2:15pm in room 325, Sterling Law Building.

Attendance Policy

This reading group will meet 13 times per semester, with sessions of 75 minutes each. To receive credit, students have to attend at least 10 sessions, or 750 minutes.

Week 1 — Infrastructure

What does the internet and our computers run on?
What happens if they fail?

Required Reading

Anderson, Ross (2008) Security Engineering *What Is Security Engineering?* `https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c01.pdf`

DeNardis, Laura (2015) *The Internet Design Tension between Surveillance and Security* IEEE Annals of the History of Computing 37, no. 2 (April 2015): 72–83.

Further Reading

David Clark, Thomas Berson, and Herbert S. Lin (2014) *The Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*
https://docs.house.gov/meetings/IF/IF02/20150303/103079/HHRG-114-IF02-20150303-SD006.pdf

Clark, David and Marjory Blumenthal (2000) *Rethinking the Design of the Internet: The End to End Arguments vs. the Brave New World*
http://dspace.mit.edu/bitstream/handle/1721.1/1519/TPRC_Clark_Blumenthal.pdf

Partridge, Derek (2011) *The Seductive Computer. Why IT Systems Always Fail*

Week 2 — History and Hacking Culture

How does the history of computing shape the field of security today?
How is that history relevant to culture and understandings among security specialists?

Required Reading

Warner, Michael (2012) *Cybersecurity: A Pre-history*, Intelligence and National Security, 27:5, 781-799
http://www.tandfonline.com/doi/full/10.1080/02684527.2012.708530

Levy, Steven (1984) *Hackers: Heroes of the Computer Revolution*
Chapter I.2. The Hacker Ethic

Leiner, Barry et al (2009) *A Brief History of the Internet*, ACM SIGCOMM Computer Communication Review, 39:5 (2009)22-31

Further Reading

Maurer, Tim (2017) *Cyber Mercenaires: The State, Hackers, and Power*, Cambridge University Press.

Lipner, Steven B. (2015) *The Birth and Death of the Orange Book.* IEEE Annals of the History of Computing 37, no. 2 (April 2015): 19–31. *doi:10.1109/MAHC.2015.27.*

Rid, T. (2016) *Rise of the Machines: A Cybernetic History* New York: W.W. Norton.

Time Magazine (1993) *Cyberpunk*, Time Magazine (8 February 1993)

Week 3 — Security economics and security provision

Attacker versus defender economics: how does the investment of time, resources, and technologies play a role in security?
Attribution and Deterrence, why do they matter?

Required Reading

Anderson, Ross (2008) Security Engineering *Economics*
`https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c07.pdf`

Anderson, Ross (2001) *Why Information Security is Hard: An Economic Perspective*, 17th Annual Computer Security Applications Conference, Dec 2001. `https://www.acsac.org/2001/papers/110.pdf`

Lindh, Andreas *Defender Economics*
`https://www.youtube.com/watch?v=mAP38Xy52X0`

Further Reading

Ronald J. Deibert & Rafal Rohozinski (2010) *Risking Security: Policies and Paradoxes of Cyberspace Security*
`https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1749-5687.2009.00088.x`

Network Associates *An Introduction to Cryptography* pp. 11–38.
`ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf`

Week 4 — Cybercrime

What is cybercrime, how do we defend against criminals?
What processes and technologies are used?
Can we solve issues with insurance?

Required Reading

Lusthaus, Jonathan (2018) *Industry of Anonymity.* Chapter Three.

Hetu, David, Paquet-Clouston, Masarah, Weissinger, Laurin (2019) *Trust in Cryptomarkets.* Journal of Cybersecurity (forthcoming)

Further Reading

Moore, Tyler Richard Clayton, and Ross Anderson (2009). *The Economics of Online Crime* Journal of Economic Perspectives. 23.3 (2009): 3-20.

Riley, Michael, Ben Elgin, Duen Lawrence, and Carol Matlack (2014) *Missed Alarms and 40 Million Stolen Credit Cards: How Target Blew It* in Bloomberg Businessweek
`http://www.businessweek.com/articles/2014---03---13/target---missed---alarms---in---epic---hack---of---credit---card---data`

Koops, Bert-Jaap (2011) *The Internet and its Opportunities for Cybercrime* Tilburg Law School Legal Studies Research Paper Series No. 09/2011
`http://ssrn.com/abstract=1738223.`

Ablon, L, Libicki, MC, Golay, AA. (2014) *Markets for Cybercrime Tools and Stolen Data* Santa Monica: RAND: 14 March 2014

Week 5 — Always On... Ubiquitous Computing, Critical Infrastructures, IoT, and Industry 4.0

What is IoT or I4.0, what are the devices and technologies underpinning them?
Do these developments change the security environment, if so how?

Required Reading

Schneier, Bruce (2017) *Click Here to Kill Everybody: Security and the Internet of Things* New York Magazine, Jan 2017.
`http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html`

Koval, Nikolay in Kenneth Geers, ed (2015) *Cyber War in Perspective: Russian Aggression Against Ukraine*, NATO CCD COE Publications, Tallinn 2015, pp.55-58. (Ch.6)

Barno, David and Nora Bensahel (2015) *Defending the Cyber Nation: lesson from Civil Defense* War on the Rocks, (2015)
`https://warontherocks.com/2015/06/defending-the-cyber-nation-lessons-from-civil-defense/`

Further Reading

National Institutes for Standards and Technology (2014) *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 2014)

Bate, Laura (2017) *The Cyber workforce Gap: A national security liability?* War on the Rocks
https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/

Burton, Joe (2013) *Small states and cyber security: the case of New Zealand.* Political Science, 2013, 65: 216

Week 6 — State and Non-State Actors

How does cooperation work between state and private actors?
What procedures and technological solutions are used?

Required Reading

Van Eeten et al (2010) ***The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data***
https://www.econinfosec.org/archive/weis2010/papers/session4/weis2010_vaneeten.pdf

Eichensehr, Kristen (2018) ***Digital Switzerlands***
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205368

Network Security (2011) ***Big boost in cyber-security spending.*** **Vol.2011(12), pp. 20-20**

Further Reading

Harris, Shane (2014) *The NSA's Cyber-King Goes Corporate: Here's why Keith Alexander thinks he's worth a million dollars a month* Foreign Policy, (2014, July 29)
www.foreignpolicy.com/2014/07/29/the-nsas-cyber-king-goes-corporate

Yadron, Danny (2015) *Ex-NSA Chief's Cybersecurity Startup Draws Funding* The Wall Street Journal, (2015, October 25)
www.wsj.com/articles/ex-nsa-chiefs-cybersecurity-startup-draws-funding-1445819345

Maurer, Tim (2015) *Hackers for hire: Cyber-mercenary industry grows worldwide* IHS Jane's Intelligence Review

Week 7 — Mass Surveillance, Back-doors, and Encryption

How does mass surveillance work?
Is there a difference between state and private surveillance?
How are people tracked by different actors?

Required Reading

Deibert, Ronald (2003) ***Black Code: Censorship, Surveillance, and Militarization of Cyberspace*** **Millennium, Vol. 32, No. 2, pp. 501–530**

Abelson et al (2015) ***Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications***
`https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8`

Popa, Raluca and Zeldovich, Nikolai (2015) ***How to Compute With Data You Can't See***
`https://spectrum.ieee.org/computing/software/how-to-compute-with-data-you-cant-see`

Further Reading

Adam I. Klein (2016) *Decryption Mandates and Global Internet Freedom*
`https://www.hoover.org/sites/default/files/research/docs/klein_webreadypdf.pdf`

Anderson, Ross (2008) Security Engineering *Terror, Justice and Freedom*
`https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c24.pdf`

Week 8 — Cyberwar

What is and is not cyberwar; on a technical level, what would cyberwar constitute?

What is a cyberweapon, politically and technologically; can the term be defined at all?

Required Reading

Thomas Rid (2011) ***Cyber War Will Not Take Place***
`https://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939`

CLTC (2018) ***Cyber Operations Conflict Lessons: Analytic Wargames***
https://cltc.berkeley.edu/2018/04/16/cyber-operations-conflict-lessons-analytic-wargames/

Further Reading

Anderson, Ross (2008) Security Engineering *Electronic and Information Warfare*
https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c19.pdf

Rosenzweig, Paul (2010) Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Chapter: *The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence*
https://www.nap.edu/read/12997/chapter/18

Lin, Herbert (2016) *Attribution of Malicious Cyber Incidents* From Soup to Nuts
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2835719

Week 9 — Cyber Terrorism, Cyber-Operations, and Subversion

What types of cyber espionage do exist and who are the players?
How is that different from mass surveillance?

Required Reading

Fireeye Inc. (n.d.) ***APT1: Exposing One of China's Cyber Espionage Units***
https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Zelin, Aaron Y. (2013) ***The State of Global Jihad Online*** **New America Foundation, January 2013.** https://www.newamerica.org/international-security/the-state-of-global-jihad-online

Further Reading

Bartles, Charles K. (2016) *Getting Gerasimov Right*
https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf

Rid, Thomas (2017) *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*
https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf

The Grugq (2017) *A Last Minute Influence Op by Data DDoS*
https://medium.com/@thegrugq/a-list-minute-influence-op-by-data-ddos-3698906d8836

The Grugq (2017) *American Snoper*
https://medium.com/@thegrugq/american-snoper-6d28e833b377 The Grugq (2017) *Opening Cyber Salvo in the French Elections*
https://medium.com/@thegrugq/opening-cyber-salvo-in-the-french-elections-e677447b91dc

Week 10 — Regulation

Who regulates IT-Security and what are the ways in which security is audited and regulated?
How is regulation turned into technical and procedural solutions?

Required Reading

Weissinger, Laurin (2019) *Working Paper: Assessing Regulation Regimes – A practitioner-focussed study.*

Anderson, Ross (2008) Security Engineering *System Evaluation and Assurance*
https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c26.pdf

Further Reading

Purser, Steve (2014) *Standards for Cyber Security*
https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security

Hathaway, Oona and Rebecca Crootof (2012) *The Law of Cyber Attack* Yale Law School Faculty Scholarship Series (Jan. 2012)

Koh, Harold (2012) *International Law in Cyberspace*" USCYBERCOM Inter-Agency Legal Conference. Sept. 18, 2012

Lessing, Lawrence (1998) *The Laws of Cyberspace*
https://cyber.law.harvard.edu/works/lessig/laws_cyberspace.pdf

Week 11 — What does the future hold? AI, quantum computing, algorithms, and blockchain...

Do these developments change cybersecurity, and if so, how?
Will the field transform when these technologies mature?

Required Reading

CLTC Berkeley (2017) ***Cybersecurity Futures 2020***
`https://cltc.berkeley.edu/wp-content/uploads/2016/04/cltcReport_04-27-04a_pages.pdf` Choose one Scenario.

Anderson, Ross (2008) Security Engineering *The Bleeding Edge* (This is from 2008!)
`https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c23.pdf`

Further Reading

Arquilla, John, and David Ronfeldt (2001) *Networks and Netwars: The Future of Terror, Crime, and Militancy.* 1st ed. Rand Corporation

Schneier, B. (2015) *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* New York: W.W. Norton.

Galič, M et al (2016) *Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation* Philosophy and Technology.
`http://link.springer.com/article/10.1007/s13347-016-0219-1`

Week 12 — Governance and National Strategies

What do governments do in the "cyber realm"? What are the implications?
How are strategies defined and put into action?
Do they actually have an effect on how practitioners act?

Required Reading

Shackelford, Scott J. and Russell, Scott (2016) ***Operationalizing Cybersecurity Due Diligence: A Transatlantic Comparative Case Study*** **South Carolina Law Review.**
`https://ssrn.com/abstract=2714529`

Zittrain, Jonathan *No Barack Obama Isn't Handing Control of the Internet Over to China* New Republic, March 24, 2014, http://www.newrepublic.com/article/117093/us-withdraws-icann-why-its-no-big-deal

GPDR Regulation (2017) https://eugdpr.org/
Read around the issue, the official home page provides a good starting point.

Further Reading

Obama Administration (2015) *New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts*
https://obamawhitehouse.archives.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat

Commission on Enhancing National Cybersecurity (2016) *Report on Securing and Growing the Digital Economy*
https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

Barlow, J.P. (1996) *A declaration of the independence of cyberspace* 8 February, https://www.eff.org/cyberspace-independence

Week 13 — Governance and *Governance Lenses* versus Technology

Do governance, regulation, strategies matter?
Technology versus policy, who wins?

Required Reading

Nye, Joseph (2011) *Nuclear Lessons for Cyber Security?* Strategic Studies Quarterly 5(4): 18-38. https://dash.harvard.edu/handle/1/8052146

Schneier, Bruce (2000) *Secrets and Lies: Digital Security in a Networked World* Wiley, 2000, pp. 85–119 (Chapters 6 & 7).

Further Reading

Mulligan, Deirdre K. and Schneider, Fred B. *Doctrine for Cybersecurity*
https://www.mitpressjournals.org/doi/pdf/10.1162/DAED_a_00116

Barrett, Edward T. (2013) *Warfare in a New Domain: The Ethics of Military Cyberoperations* Journal of Military Ethics 12.1 (2013): 4–17.

Kahler, M., ed. (2009). *Networked Politics: Agency, Power, and Governance* Ithaca: Cornell University Press

Benkler, Y. (2001) *The battle over the institutional ecosystem in the digital environment.* Commun. ACM,vol. 44, no. 2, 84—90.