

Syllabus – “Information and Cyber Power”

SAASS 667

David C. Benson (Course Director)
Nathan Huston

21 March 2019 – 05 April 2019

Approved: _____

Col. Shawn T. Cochran, PhD.
Commandant, SAASS

This Page Intentionally Left Blank

1 Overview and Evaluation

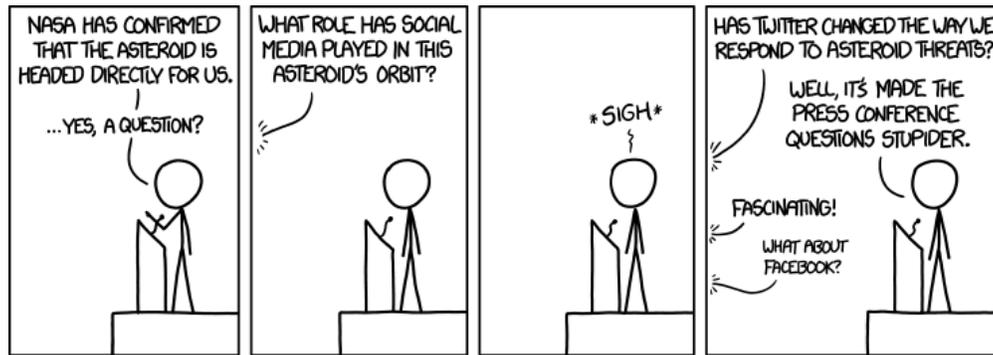


Figure 1: “Cyber” doesn’t naturally make you smarter.

Everyone in the modern world interacts with the internet, and yet few create cyberstrategy. SAASS 667 will introduce you to topics necessary to integrate the changing information and online environment into your strategies. When SAASS 667 concludes, you should understand the role information plays in political and military operations.

Evaluation



Figure 2: The more things change, the more they stay the same. Also... no.

Your final project is 60% of your grade, with the remaining 40% being participation. Please direct specific questions to your instructor, or as provided in the SAASS Operating Instructions.

Final Project

For your final project, propose a question empirically, theoretically or methodologically related to topics covered in SAASS 667. The question should also relate to strategy, broadly

defined. The best projects will engage all themes incorporated in SAASS 667 and demonstrate subject mastery where appropriate.

Students determine the project's format, but the format *can be neither slides nor verbal presentation*. Common formats include “requests for information (RFIs)” or “research proposals,” but students are encouraged to be innovative, if they would like. Regardless of format, all projects should include the following information:

1. A description of the problem the question is addressing
2. Any background information necessary to understand the question itself
3. Any important related questions that already have answers
4. A conceptual description of how to answer the question
5. An explanation of how the answer to the question will integrate into strategy

Students should not attempt to answer the question in the project. The question should be plausibly answerable in the real world given reasonable assumptions about investigative capabilities available to answer the question. Students themselves need not have access to, or be able to explicitly name the capabilities, so long as the student can describe the plausibly extant capabilities. For example, it is plausible that some entity could scrape all Twitter feeds for words related to terrorism, but it is not plausible that some entity could read all Twitter users' minds.

The Final Project is due at 1700 on 04 April 2019, the last day of class.

2 The World We Live In

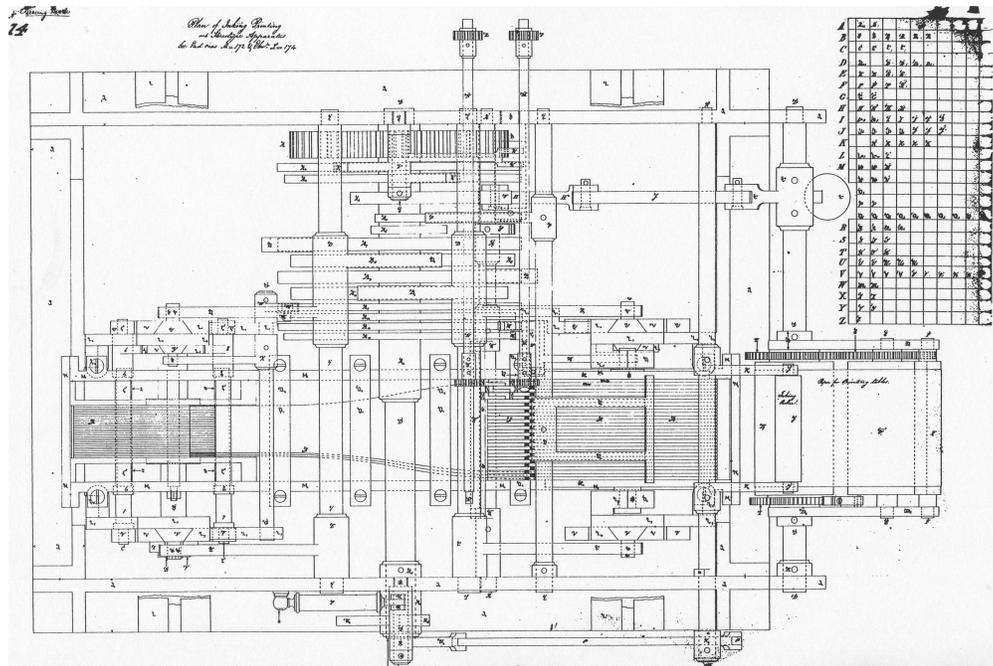


Figure 3: A Diagram of Charles Babbage's “Difference Machine” (one of the first computers)

Many students are surprised at how much we discuss issues unrelated to computers in an “*Information and Cyber Power*” course. Computers are a part of information, but infor-

mation was a part of warfare and strategy long before Babbage first imagined his machine. Information appears directly and indirectly in many of the readings in previous classes, but this course will make explicit some mechanisms and terms discussed previously. Specifying information's role in strategy generally will help us discuss how information technologies like computers have changed strategy.

We start a class on information and cyberpower by answering two simple questions without respect to computers at all. First, how do people get and share information? Second, how do groups of people do things? These questions are precursors for all future discussion in SAASS 667.

Day 1: How is Society Structured

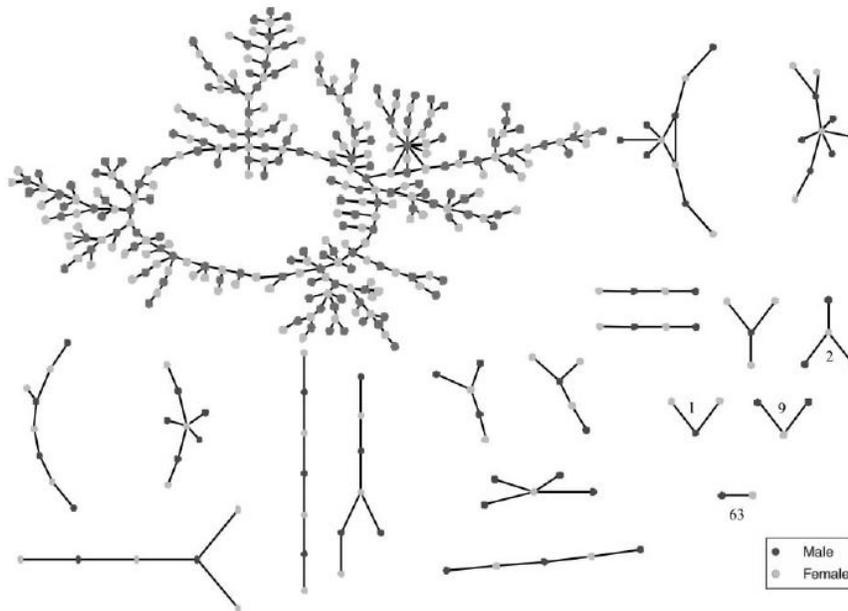


FIG. 2.—The direct relationship structure at Jefferson High

Figure 4: Network of Sexual and Romantic Networks of Teens in a US High School

We can describe groups of people and groups of computers as networks, but we start with social networks in SAASS 667. Human communication starts by using real world networks, and online communication frequently reveals those real world networks. Communications online are not necessarily the same as communications offline, and offline groups sometimes behave materially differently from online groups. Qualitative differences between online and offline communications create strategic opportunities that require in depth understanding of the differences, which implies an understanding of both types of communications. Mathematically, network analysis math is the same whether examining computers or people, as is the vocabulary. Human social networks are more salient, and easier to relate to than computer networks, so we start there.

Required Reading:

- Charles Kadushin, *Understanding Social Networks: Theories, Concepts, and Findings* (Oxford, U.K.: Oxford University Press, 2011)

Recommended Reading:

- Zeev Maoz, *Networks of Nations: The Evolution, Structure, and Impact of International Networks, 1816-2001* (Cambridge, U.K.: Cambridge University Press, 2011)
- John Frederick Padgett and Walter W. Powell, *The Emergence of Organizations and Markets* (Princeton, NJ: Princeton University Press, 2012)
- Roger Dale Petersen, *Resistance and Rebellion: Lessons from Eastern Europe* (Cambridge, England; New York, NY: Cambridge University Press, 2001)

3 Information Into Action

Day 2: How Do People Do Things Together?



Figure 5: Mobilizing means different things to different people

Strategic operations involve multiple people, usually on both sides. The bulk of today's reading comes from Mancur Olson. His explanation still serves as the basis for how social scientists and strategists think about group action. We also read a possible theoretical update, which argues that Olson's logics may no longer hold, thanks to the internet.

Required Reading:

- Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge, MA: Harvard University Press, 1971)
- W. Lance Bennett and Alexandra Segerberg, "The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics," *Information, Communication & Society* 15, no. 5 (5 2012): 739–68

Recommend Reading:

- Robert Axelrod and Robert O. Keohane, “Achieving Cooperation under Anarchy: Strategies and Institutions,” *World Politics* 38, no. 1 (1 1985): 226–254
- Russell Hardin, *Collective Action* (Baltimore: Johns Hopkins University Press, 1982)
- Robert Jervis, “Cooperation under the Security Dilemma,” *World Politics* 30, no. 2 (2 1978): 167–214
- Paul R. Milgrom, Douglass C. North, and Barry R. Weingast, “The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs,” *Economics & Politics* 2, no. 1 (1 1990): 1–23
- Elinor Ostrom, “Collective Action and the Evolution of Social Norms,” *The Journal of Economic Perspectives* 6, no. 4 (2000): 235–252
- Kenneth Oye, “Explaining Cooperation under Anarchy: Hypotheses and Strategies,” *World Politics* 38, no. 1 (1 1985): 1–24
- Duncan Snidal, “Relative Gains and the Pattern of International Cooperation,” *American Political Science Review* 85, no. 3 (1991): 701–726

Day 3: Social Mobilization



Figure 6: Not all social mobilization is online, or desirable.

From its beginning, scholars believed the internet would affect social mobilization. Social mobilization differs from collective action conceptually, even when seeking the same outcomes. Today's readings explain social mobilization, with some directly applying to online social mobilization. Students should note the conceptually different mechanisms for social mobilization than from Olson-style collective action.

Required Reading:

- Roger V. Gould, "Multiple Networks and Mobilization in the Paris Commune, 1871," *American Sociological Review* 56, no. 6 (6 1991): 716–29
- Timur Kuran, "Now Out of Never: The Element of Surprise in the East European Revolution of 1989," *World Politics* 44, no. 01 (01 1991): 7–48
- Doug McAdam, "Recruitment to High-risk Activism: The Case of Freedom Summer," *American Journal of Sociology* 92, no. 1 (1 1986): 64–90
- Clay Shirky, "The Political Power of Social Media," *Foreign Affairs* 90, no. 1 (1 2011): 28–41
- Gabriel Weimann, "Going Dark: Terrorism on the Dark Web," *Studies in Conflict & Terrorism* 39, no. 3 (2015): 195–206, doi:10.1080/1057610x.2015.1119546

Recommended Reading:

- George T. Crane, "Collective Identity, Symbolic Mobilization, and Student Protest in Nanjing, China, 1988-1989," *Comparative Politics* 26, no. 4 (1994): 395, doi:10.2307/422023
- William A. Gamson, *The Strategy of Social Protest* [in English] (Homewood, IL: Dorsey Press, 1975)
- Marshall Ganz, "Resources and Resourcefulness: Strategic Capacity in the Unionization of California Agriculture, 1959-1966," *American Journal of Sociology* 105, no. 4 (4 2000): 1003–62, doi:10.2307/3003887, JSTOR: 3003887
- J. Craig Jenkins, "Resource Mobilization Theory and the Study of Social Movements," *Annual Review of Sociology* 9, no. 1 (1 1983): 527–553, doi:10.1146/annurev.so.09.080183.002523
- Doug McAdam, Sidney G. Tarrow, and Charles Tilly, *Dynamics of Contention* (New York: Cambridge University Press, 2001)
- John D. McCarthy and Mayer N. Zald, "Resource Mobilization and Social Movements: A Partial Theory," *American Journal of Sociology*, 1977, 1212–1241
- Susan Olzak and Emily Ryo, "Organizational Diversity, Vitality and Outcomes in the Civil Rights Movement," *Social Forces* 85, no. 4 (4 2007): 1561–91, doi:10.2307/4494999, JSTOR: 4494999
- Karen Rasler, "Concessions, Repression, and Political Protest in the Iranian Revolution," *American Sociological Review* 61, no. 1 (1996): 132–152, accessed September 18, 2018, doi:10.2307/2096410, JSTOR: 2096410

- Idean Salehyan and Brandon Stewart, “Political Mobilization and Government Targeting: When Do Dissidents Challenge the State?,” *Comparative Political Studies*, 2016, doi:10.1177/0010414016655541, eprint: <http://cps.sagepub.com/content/early/2016/06/14/0010414016655541.full.pdf+html>, <http://cps.sagepub.com/content/early/2016/06/14/0010414016655541.abstract>
- Theda Skocpol, *Social Revolutions in the Modern World* (Cambridge, England ; New York, NY: Cambridge University Press, 1994)
- Mayer N. Zald and Michael A. Berger, “Social Movements in Organizations: Coup D’etat, Insurgency, and Mass Movements,” *American Journal of Sociology* 83, no. 4 (4 1978): 823–861, doi:10.2307/2777718, JSTOR: 2777718

Day 4: Counter-Mobilization (What Governments Do)



Figure 7: Who would you rather be?

Yesterday’s writings portrayed social movements as powerful, but governments control most of the globe. Why? Governments retain tools they can use to control their populations. Most importantly governments can use force, commonly called repression. SAASS primarily studies the use of force, and today’s readings focus on the using force to counter social movements and collective action.

Required Reading:

- Anita R. Gohdes, “Pulling the Plug: Network Disruptions and Violence in Civil Conflict,” *Journal of Peace Research*, 2015,
- Peter Lorentzen, “China’s Strategic Censorship,” *American Journal of Political Science* 58, no. 2 (2014): 402–414

- Gary King, Jennifer Pan, and Margaret E. Roberts, “How Censorship in China Allows Government Criticism but Silences Collective Expression,” *American Political Science Review* 107, no. 02 (02 2013): 326–43
- Ron Deibert, “Cyberspace under Siege,” *Journal of Democracy* 26, no. 3 (2015): 64–78
- Sheena Chestnut Greitens, “Authoritarianism Online: What Can We Learn from Internet Data in Nondemocracies?,” *PS: Political Science & Politics* 46, no. 02 (2013): 262–270

Recommended Reading:

- David C. Benson, “Why the Internet Is Not Increasing Terrorism,” *Security Studies* 23, no. 2 (2 2014): 293–328
- Carles Boix and Milan W. Svobik, “The Foundations of Limited Authoritarian Government: Institutions, Commitment, and Power-Sharing in Dictatorships,” *The Journal of Politics* 75 (02 2013): 300–316
- Christian Davenport, *Media Bias Perspective, and State Repression: The Black Panther Party* (New York, NY: Cambridge University Press, 2010)
- Donatella Della Porta, *Social Movements, Political Violence, and the State: A Comparative Analysis of Italy and Germany* (Cambridge, England: Cambridge University Press, 1995)
- Jennifer Earl, “Political Repression: Iron Fists, Velvet Gloves, and Diffuse Control,” *Annual Review of Sociology* 37, no. 1 (1 2011): 261–84
- Diana Fu, “Disguised Collective Action in China,” *Comparative Political Studies* 50, no. 4 (2017): 499–527
- Jennifer Gandhi, *Political Institutions under Dictatorship* (New York, NY: Cambridge University Press, 2008)
- Jennifer Gandhi and Adam Przeworski, “Cooperation, Cooptation, and Rebellion under Dictatorships,” *Economics & Politics* 18, no. 1 (2006): 1–26
- Jennifer Gandhi and Adam Przeworski, “Authoritarian Institutions and the Survival of Autocrats,” *Comparative Political Studies* 40, no. 11 (2007): 1279–1301
- Milan W Svobik, *The Politics of Authoritarian Rule* (New York, NY: Cambridge University Press, 2012)
- Sean L. Yom and III Gause F. Gregory, “Resilient Royals: How Arab Monarchies Hang On,” *Journal of Democracy* 23, no. 4 (2012): 74–88, accessed June 22, 2017, doi:10.1353/jod.2012.0062, <https://muse.jhu.edu/article/487784>

4 Information and Intelligence

Day 5: Big Data

Until recently, the “information problem” was getting maximum information from minimal data. Now data abounds, and computers can analyze as much data as exist. “Big Data”



Figure 8: It's not so far away if you aren't aware of your social media settings.

has positive and negative effects on strategy. Data can possibly illuminate previously hidden facts, but with attendant risk of misplaced confidence. Not everyone wants their data available creating an ethical conundrum.

Required Reading:

- Kenneth Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think About the World," *Foreign Affairs* 92, no. 3 (2013): 28–40, JSTOR: 23526834
- Hans Krause Hansen and Tony Porter, "What Do Big Data Do in Global Governance?," *Global Governance* 23, no. 1 (2017): 31–42, <https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=121231921&site=ehost-live&scope=site&custid=airuniv>
- Mél Hogan and Tamara Shepherd, "Information Ownership and Materiality in an Age of Big Data Surveillance," *Journal of Information Policy* 5 (2015): 6
- Salar Jahedi, Jennie Wenger, and Douglas Yeung, *Searching for Information Online: Using Big Data to Identify the Concerns of Potential Army Recruits*, technical report (Santa Monica, CA, 2016), doi:10.7249/rr1197
- Carter Jernigan and Behram F.T. Mistree, "Gaydar: Facebook Friendships Expose Sexual Orientation," *First Monday*, 2009, <http://firstmonday.org/ojs/index.php/fm/article/view/2611>
- William Marcellino et al., *Monitoring Social Media*, research report (RAND Corporation, 2017)

Recommended Reading:

- Christopher Eldridge, Christopher Hobbs, and Matthew Moran, "Fusing Algorithms and Analysts: open-source intelligence in the age of 'Big Data'," *Intelligence and National Security*, 2017, 1–16, doi:10.1080/02684527.2017.1406677
- Nathan Kallus, "Predicting Crowd Behavior with Big Public Data," in *International World Wide Web Conference* (Seoul, Korea: IW3C2, April 7, 2014)

- Atif Mian and Howard Rosenthal, "Introduction: Big Data in Political Economy," *RSF: The Russell Sage Foundation Journal of the Social Sciences* 2, no. 7 (2016): 1, doi:10.7758/rsf.2016.2.7.01
- Anthony Sistilli, *Twitter Data Mining: A Guide to Big Data Analytics Using Python*, technical report (Toptal, 2017), <https://www.toptal.com/python/twitter-data-mining-using-python>
- Anna Wilson et al., "Big Data and Learning Analytics: Singular or plural?," *First Monday* 22, no. 4 (2017)

Day 6: Information Integration

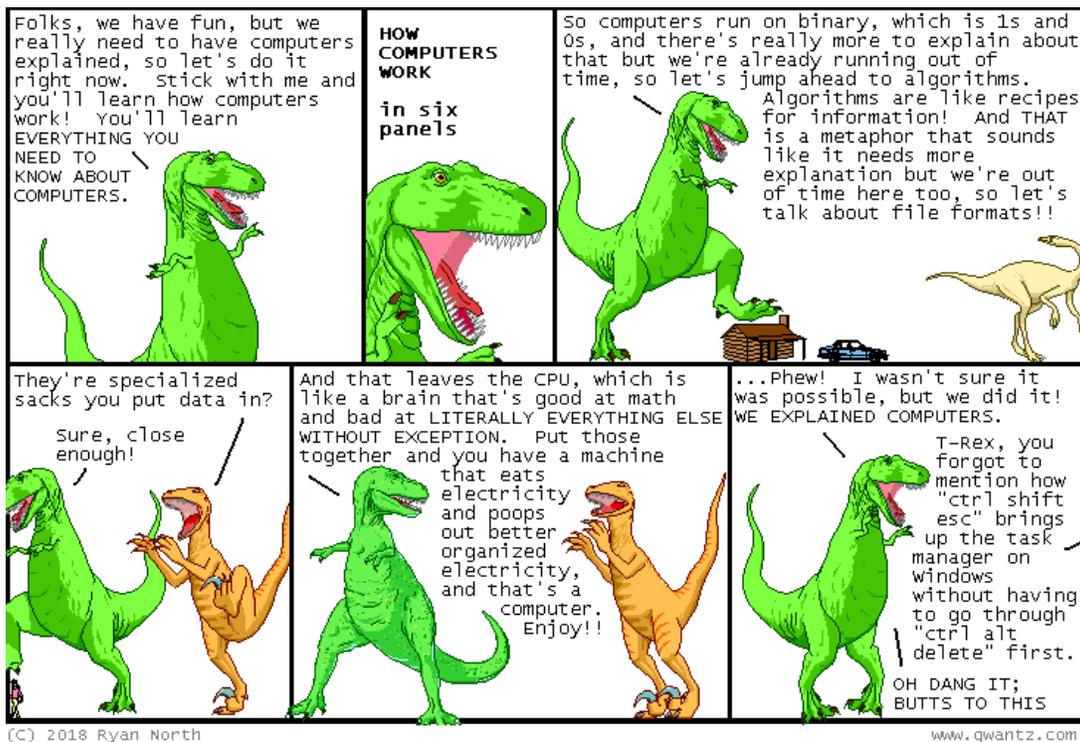


Figure 9: Information use has real consequences for everyone in this room

All the information in the world avails strategists nothing if they cannot incorporate it into strategy. Big data may be getting close to providing all the information in the world, but people are still responsible for strategy, and people must figure out ways to use the information available. In the military, information usually means intelligence and today's reading examines "intelligence failures." The Iranian Revolution and Operation Iraqi Freedom are still relevant, and illustrate how information, even when available, may not properly be incorporated into strategy. Spare yourself, and skim chapter 2.

Required Reading:

- Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2010)

Recommended Reading:

- Richard K Betts, “Analysis, War, and Decision: Why Intelligence Failures Are Inevitable,” *World Politics* 31, no. 1 (1978): 61–89
 - Richard K Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (Columbia University Press, 2009)
 - Sherman Kent, *Strategic Intelligence for American World Policy*, vol. 2377 (Princeton University Press, December 8, 2015)
 - Amos Kovacs, “Using Intelligence,” *Intelligence and National Security* 12, no. 4 (1997): 145–164
 - Stephen Marrin and Jonathan D. Clemente, “Improving Intelligence Analysis by Looking to the Medical Profession,” *International Journal of Intelligence and CounterIntelligence* 18, no. 4 (2005): 707–729, doi:10.1080/08850600590945434
 - Office of the Director of National Intelligence, *Iran: Nuclear Intentions and Capabilities*, technical report (National Intelligence Council, November 2007)
 - David H. Petraeus and James F. Amos, *FM 3-24 Counterinsurgency*, technical report (Washington D.C.: Government Publications Office, 2006)
- Appendix B.
- Christopher A Preble, “‘Who Ever Believed in the ‘Missile Gap’?: John F. Kennedy and the Politics of National Security,” *Presidential Studies Quarterly* 33, no. 4 (2003): 801–826
 - David Robarge, “Getting It Right: CIA Analysis of the 1967 Arab-Israeli War,” *Studies in Intelligence*, 2005, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no1/html_files/arab_israeli_war_1.html
 - Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Cornell University Press, 2011)
 - Richard L Russell, “CIA’s Strategic Intelligence in Iraq,” *Political Science Quarterly* 117, no. 2 (2002): 191–207
 - Richard L Russell, *Sharpening Strategic Intelligence: Why the CIA Gets It Wrong and What Needs to Be Done to Get It Right* (Cambridge University Press, 2007)
 - Luke Benjamin Wells, “The ‘Bomber Gap’: British Intelligence and an American Delusion,” *Journal of Strategic Studies* 40, no. 7 (2017): 963–989

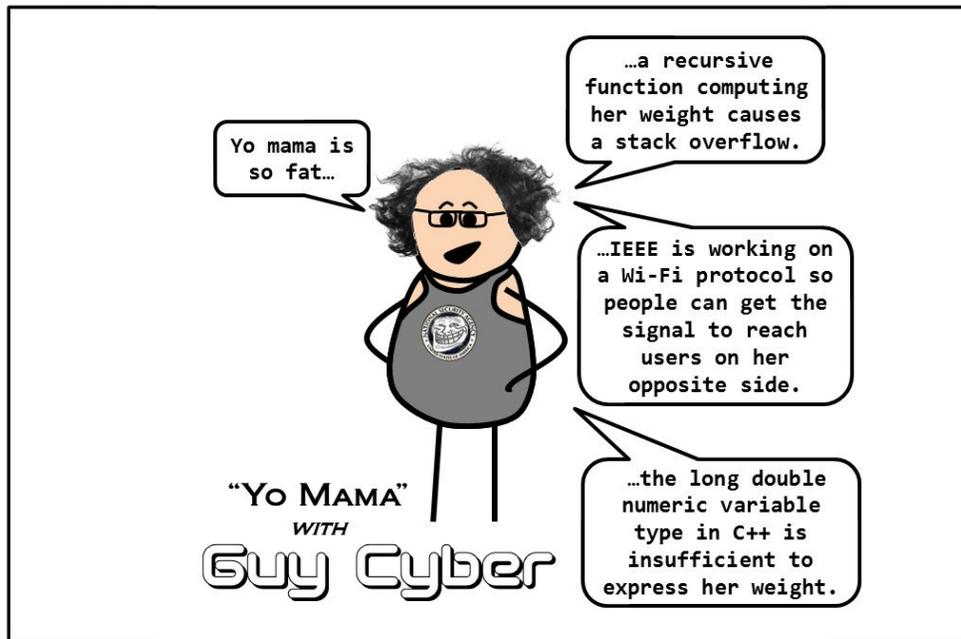
5 Teh H4Ckz0r5!: What You Thought Was “Cyber”

Day 7: Digital Exploitation 1, Hacking for N00bz

For most students, when they hear *Information and Cyber Power* they think of today’s readings. Computers play a vital role in nearly everything we do in the developed world. The power of computers also creates vulnerabilities. Computers’ ubiquity in life makes that



THE FURTHER ADVENTURES OF DOCTRINE MAN



© 2014 The Further Adventures of Doctrine Man!! | www.facebook.com/doctrineman | www.twitter.com/doctrine_man

Figure 10: This will all make sense after today. NARRATOR: No it won't.

vulnerability ubiquitous, too. For the next two days we will look at the various vulnerabilities that computer and internet systems introduce and the ways we can protect against them.

Engebretson is included in today's and tomorrow's reading *primarily as a reference*, not as a discussion tool. Penetration testing is what "white hat" hackers do—look for vulnerabilities in code and systems. Guides on penetration testing are essentially guides to hacking, and use all of the same tools. Through the last section of the course, you will encounter many terms that may or may not be familiar to you, but not all references online are equally reliable. Use Engebretson as your touchstone for vocabulary and concepts that you encounter, and be prepared to ask about unfamiliar concepts in class. If you choose to read Engebretson please remember: 1) What he is explaining how to do is *illegal* without permission, and 2) the most important take away for a strategist is the relative ease and limitations of the techniques he describes.

Required Reading:

- Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: U.S. Naval Institute Press, October 15, 2016)
- Pat Engebretson, *The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing Made Easy* (Amsterdam: Syngress, 2013)

Recommended Reading:

Many of the best resources for current cybersecurity are not books, journals or even blogs. Some of the following researchers, hackers and websites are amazing resources that students should refer to whenever necessary.

- @Krypt3ia (as of this writing, his name is in Russian, but he is American)
- Scot Terban, “Espionage in the Modern Age of Information Warfare,” in *Circle City Con 2018* (Indianapolis, IN, June 1, 2018), <https://youtu.be/g0rqa5dBxHY>
- 1. @SwiftOnSecurity (Taylor Swift is *his* real name, so not *that* Taylor Swift.)
- @th3j35t3r
- Bruce Schneier www.schneier.com
- www.stackoverflow.com
- <https://malpedia.caad.fkie.fraunhofer.de/>

More traditional media

- Harold Abelson et al., *Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, research report MIT-CSAIL-TR-2015-026 (Cambridge, MA: Massachusetts Institute of Technology, 2015)
- Derek E. Bambauer, “Ghost in the Network,” *University of Pennsylvania Law Review* 162, no. 5 (5 2014)
- David Betz, “Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed,” *Journal of Strategic Studies* 35, no. 5 (2012): 689–711, doi:10.1080/01402390.2012.706970
- Joel Brenner, “Debating the Chinese Cyber Threat,” *International Security* 40, no. 1 (2015): 191–193, accessed July 12, 2017, <https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=108957717&site=ehost-live&scope=site&custid=airuniv>
- Myriam Dunn Cavelty, “From Cyber-bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse,” *International Studies Review* 15, no. 1 (2013): 105–122, doi:10.1111/misr.12023
- Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st (New York, NY: Ecco, 2010)
- Craig Fields, *Task Force on Cyber Deterrence*, research report (Department of Defense, Defense Science Board, February 2017)
- Michael P. Fischerkeller and Richard J. Harknett, “Deterrence Is Not a Credible Strategy for Cyberspace,” *Orbis* 61, no. 3 (2017): 381–393, accessed July 24, 2017, doi:10.1016/j.orbis.2017.05.003, <http://www.sciencedirect.com/science/article/pii/S0030438717300431>

- Brett Hawkins, *Case Study: The Home Depot Data Breach*, research report (SANS Institute, January 2015)
- Robert Jervis, “Some Thoughts on Deterrence in the Cyber Era,” *Journal of Information Warfare* 15 (2 2016)
- Timothy J. Junio, “How Probable Is Cyber War? Bringing Ir Theory Back in to the Cyber Conflict Debate,” *Journal of Strategic Studies*, 2013, 1–9
- Lucas Kello, “The Meaning of the Cyber Revolution,” *International Security* 38, no. 2 (2013): 7–40, accessed July 12, 2017, <https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=91709783&site=ehost-live&scope=site&custid=airuniv>
- Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press, 2017)
- A. Kott, J. Ludwig, and M. Lange, “Assessing Mission Impact of Cyberattacks: Toward a Model-driven Paradigm,” *IEEE Security Privacy* 15, no. 5 (2017): 65–74, doi:10.1109/MSP.2017.3681068
- Kristen A. Lee, “Colin Powell’s Personal Emails Infiltrated by Bush Family Hacker ‘Guccifer,’” *New York Daily News*, March 13, 2013, accessed August 6, 2018, <http://www.nydailynews.com/news/politics/colin-powell-emails-infiltrated-hacker-guccifer-article-1.1287354>
- Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009)

Day 8: Digital Exploitation 2, Cyberops on the Joint Battlefield

Required Reading:

- Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: U.S. Naval Institute Press, October 15, 2016)
- Max Smeets, “A Matter of Time: On the Transitory Nature of Cyberweapons,” *Journal of Strategic Studies* 41, nos. 1-2 (2017): 6–32

Recommended Reading:

- Adam P. Liff, “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War,” *Journal of Strategic Studies* 35, no. 3 (2012): 401–428, doi:10.1080/01402390.2012.663252
- Adam P. Liff, “The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio,” *Journal of Strategic Studies*, 2013, 1–5
- Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies* 22, no. 3 (3 2013): 365–404, accessed July 12, 2017, doi:10.1080/09636412.2013.816122, <https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=89481125&site=ehost-live&scope=site&custid=airuniv>

D THE FURTHER ADVENTURES OF
DOCTRINE MAN

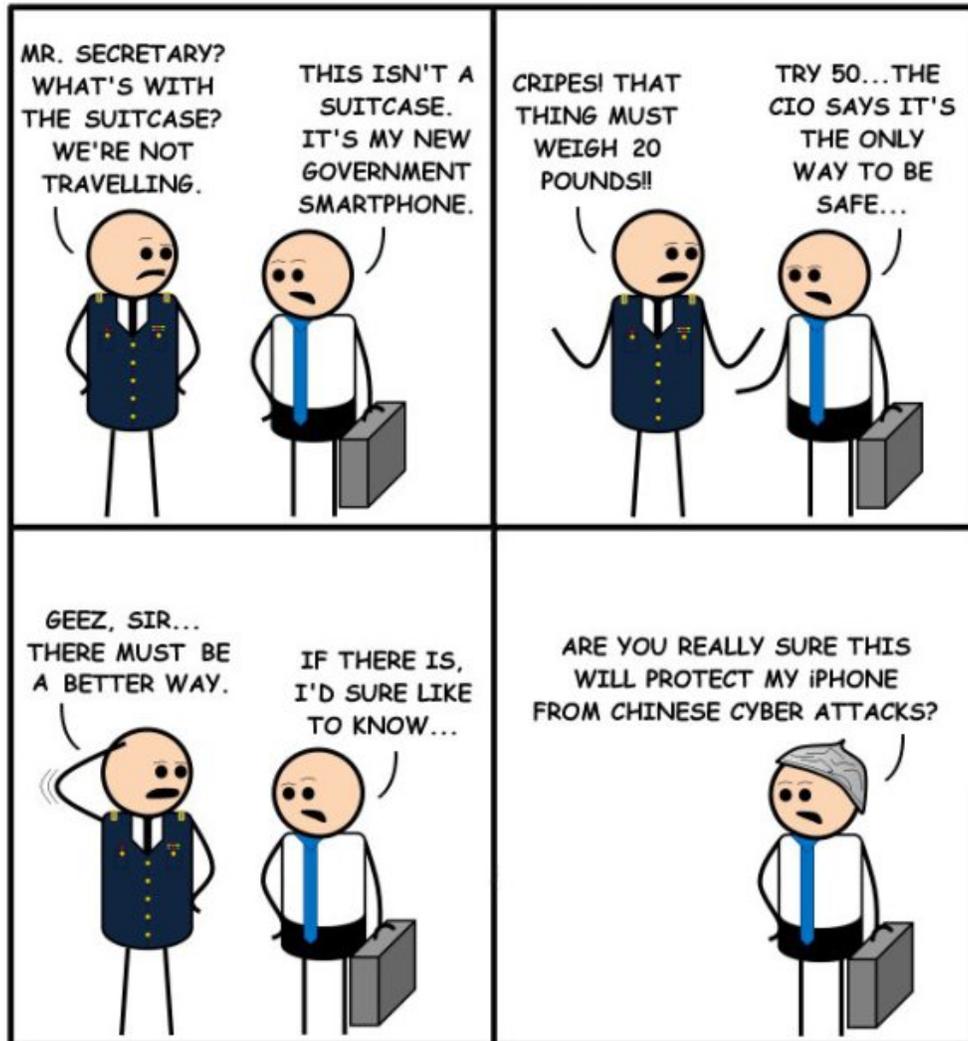


Figure 11: There's no kill like over kill.

- Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39, no. 3 (3 2015): 7–47, accessed July 12, 2017, doi:10.1162/ISEC_a_00189, <https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=101056274&site=ehost-live&scope=site&custid=airuniv>
- Jon R. Lindsay, "Debating the Chinese Cyber Threat," *International Security* 40, no. 1 (2015): 193–195, accessed July 12, 2017, <https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=108957718&site=ehost-live&scope=site&custid=airuniv>

- Ryan C. Maness and Brandon Valeriano, “The Impact of Cyber Conflict on International Interactions,” *Armed Forces & Society* 42, no. 2 (2016): 301–323, doi:10.1177/0095327X15572997, eprint: <http://afs.sagepub.com/content/42/2/301.full.pdf+html>, <http://afs.sagepub.com/content/42/2/301.abstract>
- Mary Mcevoy Manjikian, “From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik,” *International Studies Quarterly* 54, no. 2 (2010): 381–401
- Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32
- Thomas Rid, *Cyber War Will Not Take Place* (Oxford, U.K.: Oxford University Press, 2013)
- Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38, nos. 1-2 (1-2 2014): 4–37, doi:10.1080/01402390.2014.977382
- David E. Sanger, *The Perfect Weapon* (Crown/Archetype, June 19, 2018)
- P. W. Singer and Emerson T. Brooking, *Likewar: The Weaponization of Social Media* (Houghton Mifflin Harcourt, October 2, 2018)
- P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: what everyone needs to know* (Oxford, U.K.: Oxford University Press, 2014)
- Rebecca Slayton, “What Is the Cyber Offense-defense Balance? Conceptions, Causes, and Assessment,” *International Security* 41, no. 3 (2017): 72–109, accessed July 12, 2017, doi:10.1162/ISEC_a_00267
- John Stone, “Cyber War Will Take Place!,” *Journal of Strategic Studies* 36, no. 1 (2013): 101–108

Day 9: Case Study: Russian Online Information Operations

REMINDER: *Your project is due at 1700 today.*

Please remember when reading and during discussion that the subject of today’s course-work is **Russian information operations online and in the real world** and not anything any Americans did. There is a lot of information in the recommended readings. If you want additional information, it is *recommended* you look there. Feel free to incorporate both the recommended readings, and any other readings into the course discussion. If you bring in outside information, however, be prepared to present and defend the source.

Required Reading:

- Dmitri Alperovitch, “Bears in the Midst: Intrusion into the Democratic National Committee,” CrowdStrike, June 15, 2016, accessed August 9, 2018, <https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/>
- “18 Revelations from Wikileaks’ Hacked Clinton Emails,” *BBC*, October 27, 2016, accessed August 9, 2018, <https://www.bbc.com/news/world-us-canada-37639370>

- Julia Ioffe, “The History of Russian Involvement in America’s Race Wars,” *The Atlantic*, October 21, 2017, accessed August 4, 2018, <https://www.theatlantic.com/international/archive/2017/10/russia-facebook-race/542796/>
 - Jonathan Masters, “Russia, Trump, and the 2016 U.S. Election,” *Council on Foreign Relations*, February 26, 2018, accessed August 10, 2018, <https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election>
 - Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent Us Elections*, technical report ICA 2017-01D (National Intelligence Council, January 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf
 - “Reconstructing the Russian Hacks Leading up to the Election,” *PBS Newshour*, December 14, 2016, accessed August 9, 2018, <https://www.pbs.org/newshour/show/reconstructing-russian-hacks-leading-election>
 - Raphael Satter, Jeff Donn, and Chad Day, “Inside Story: How Russians Hacked the Democrats’ Emails,” *Associated Press News*, November 4, 2017, accessed November 16, 2017, <https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a>
 - Secureworks Counter Threat Unit Threat Intelligence, *Threat Group-4127 Targets Hillary Clinton Presidential Campaign*, technical report (Secureworks, June 16, 2016), accessed August 9, 2018, <https://www.secureworks.com/research/threat-group-4127-targets-hillary-clinton-presidential-campaign>
 - Kris Shaffer, “Twitter Propaganda during ‘Unite the Right,’” *Propagandalytics*, August 15, 2017, accessed August 10, 2018, <https://pushpullfork.com/twitter-propaganda-during-unite-the-right/>
 - Scott Shane, “These Are the Ads Russia Bought on Facebook in 2016,” *New York Times*, November 1, 2017, accessed August 9, 2018, <https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html>
 - **NOT IN READER**
- Benjamin Jensen, Brandon Valeriano, and Ryan Maness, “Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist,” *Journal of Strategic Studies* 0, no. 0 (2019): 1–23, doi:10.1080/01402390.2018.1559152

Recommended Reading:

- Ed Adamczyk, “‘Guccifer’ Pleads Guilty to Hacking Emails of Clinton, Ex-presidents,” *UPI*, May 25, 2016, accessed August 6, 2018, https://www.upi.com/Top_News/US/2016/05/25/Hacker-Guccifer-pleads-guilty-to-email-break-ins/9481464195286/
- Julia Angwin, Madeleine Varner, and Ariana Tobin, “Facebook Enabled Advertisers to Reach ‘Jew Haters,’” *ProPublica*, September 14, 2017, accessed August 9, 2018, <https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters>
- Dennis Anon, “How Cookies Track You around the Web and How to Stop Them,” *Privacy.net*, February 24, 2018, accessed August 9, 2018, <https://privacy.net/stop-cookies-tracking/>

- “Twitter Bans RT and Sputnik Ads Amid Election Interference Fears,” *BBC News*, October 26, 2017, accessed August 10, 2018, <https://www.bbc.com/news/world-us-canada-41766991>
- Daniel J Balz, *Collision 2012 : Obama vs. Romney and the Future of Elections in America* (2013)
- Lois Beckett, “Everything We Know (so Far) about Obama’s Big Data Tactics,” *Pro Publica*, November 29, 2012, accessed August 9, 2018, <https://www.propublica.org/article/everything-we-know-so-far-about-obamas-big-data-operation>
- Aaron Blake, “Elizabeth Warren and Donna Brazile Both Now Agree the 2016 Democratic Primary Was Rigged,” *Washington Post*, November 2, 2017, accessed August 9, 2018, <https://www.washingtonpost.com/news/the-fix/wp/2017/11/02/ex-dnc-chair-goes-at-the-clintons-alleging-hillarys-campaign-hijacked-dnc-during-primary-with-bernie-sanders/>
- David E. Broockman and Donald P. Green, “Do Online Advertisements Increase Political Candidates’ Name Recognition or Favorability? Evidence from Randomized Field Experiments,” *Political Behavior* 36, no. 2 (2013): 263–289, doi:10.1007/s11109-013-9239-z
- Keith Collins, “See Which Facebook Ads Russians Targeted to People like You,” *New York Times*, May 14, 2018, accessed August 9, 2018, <https://www.nytimes.com/interactive/2018/05/14/technology/facebook-ads-congress.html>
- Josh Constine, “Facebook Vows to Manually Review Ad Targeting After ‘Jew-Haters’ Scandal,” *Techcrunch*, September 20, 2017, accessed August 9, 2018, <https://techcrunch.com/2017/09/20/anticipating-the-dark-side/>
- Office of Evaluations and Special Projects, *Office of the Secretary - Evaluation of Email Records Management and Cybersecurity Requirements*, technical report ESP-16-03 (Department of State, May 2016)
- David A. Fahrenthold, Tom Hamburger, and Rosalind S. Helderman, “The Inside Story of How Bill Clinton Built a \$2bn Global Foundation May Undermine Hillary’s Chances,” *The Independent*, June 3, 2015, <https://www.independent.co.uk/news/world/americas/the-inside-story-of-how-bill-clinton-built-a-2bn-global-foundation-may-undermine-hillarys-chances-10295702.html>
- Jack Gillum, “AP Exclusive: Clinton Email Server Setup Risked Intrusions,” *AP News*, October 13, 2015, accessed August 9, 2018, <https://apnews.com/467ff78858bf4dde8db21677deeff101/only-ap-clinton-server-ran-software-risked-hacking>
- Shane Goldmacher, “Hillary Clinton’s ‘Invisible Guiding Hand,’” *Politico*, September 7, 2016, accessed August 9, 2018, <https://www.politico.com/magazine/story/2016/09/hillary-clinton-data-campaign-elan-kriegel-214215>
- Kevin Granville, “Facebook and Cambridge Analytica: What You Need to Know As Fallout Widens,” *New York Times*, March 19, 2018, accessed August 9, 2018, <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

- Glenn Greenwald, “Bradley Manning: The Face of Heroism,” *The Guardian*, February 28, 2013, accessed August 10, 2018, <https://www.theguardian.com/commentisfree/2013/feb/28/bradley-manning-heroism-pleads-guilty>
- Glenn Greenwald and Trevor Timm, “The DNC’s Lawsuit against Wikileaks Poses a Serious Threat to Press Freedom,” *The Intercept*, April 20, 2018, accessed August 10, 2018, <https://theintercept.com/2018/04/20/the-dncs-lawsuit-against-wikileaks-poses-a-serious-threat-to-press-freedom/>
- Sasha Issenberg, “How Obama’s Team Used Big Data to Rally Voters,” *MIT Technology Review*, December 19, 2012, accessed August 9, 2018, <https://www.technologyreview.com/s/509026/how-obamas-team-used-big-data-to-rally-voters/>
- Gregory Krieg and Tal Kopan, “Is This the Email That Hacked John Podesta’s Account?,” *CNN*, October 30, 2016, accessed August 9, 2018, <https://www.cnn.com/2016/10/28/politics/phishing-email-hack-john-podesta-hillary-clinton-wikileaks/index.html>
- Bonnie Kristian, “Did Russia Read Hillary Clinton’s Emails? Robert Gates Says the Odds Are ‘pretty high.’” *The Week*, January 22, 2016, accessed August 9, 2018, <https://theweek.com/speedreads/600728/did-russia-read-hillary-clintons-emails-robert-gates-says-odds-are-pretty-high>
- Issie Lapows, “Clinton Has a Team of Silicon Valley Stars. Trump Has Twitter,” *Wired*, July 14, 2016, accessed August 9, 2018, <https://www.wired.com/2016/07/clinton-team-silicon-valley-stars-trump-twitter/>
- Dune Lawrence, “Russian Botnets,” *Bloomberg Businessweek*, no. 4549 (2017): 79, <https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=126495905&site=ehost-live&scope=site&custid=airuniv>
- Jason Le Miere, “Hillary Clinton Calls Email Scandal Fake News and ‘Biggest Nothing Burger Ever,’” *Newsweek*, May 31, 2017, accessed August 9, 2018, <https://www.newsweek.com/hillary-clinton-emails-fake-news-618557>
- John Lee, “Cyber Kleptomaniacs: Why China Steals Our Secrets,” *World Affairs* 176, no. 3 (2013): 73–79, JSTOR: 43555412
- Adam B. Lerner, “Michael Morell: Foreign Governments Have Hillary’s Email,” *Politico*, May 15, 2015, accessed August 9, 2018, <https://www.politico.com/story/2015/05/michael-morrell-foreign-governments-have-hillarys-email-118007>
- Eric Lichtblau, “Shadow of Plea Deal for David Petraeus Loomed Over Hillary Clinton Email Case,” *New York Times*, July 5, 2016, accessed August 9, 2018, <https://www.nytimes.com/2016/07/06/us/david-petraeus-hillary-clinton-fbi.html>
- Natasha Lomas, “Facebook’s Tracking of Non-users Ruled Illegal Again,” *Techcrunch*, February 19, 2018, accessed August 9, 2018, <https://techcrunch.com/2018/02/19/facebooks-tracking-of-non-users-ruled-illegal-again/>
- Alexis C. Madrigal, “When the Nerds Go Marching In,” *The Atlantic*, November 16, 2012, <https://www.theatlantic.com/technology/archive/2012/11/when-the-nerds-go-marching-in/265325/>

- Seth E. Masket, “Did Obama’s Ground Game Matter? the Influence of Local Field Offices during the 2008 Presidential Election,” *The Public Opinion Quarterly* 73, no. 5 (2009): 1023–1039, JSTOR: 40467656
- Andrew C. McCarthy, “Clinton Emails: What the IG Report Refuses to Admit,” *National Review*, June 19, 2018, accessed August 9, 2018, <https://www.nationalreview.com/2018/06/ig-report-clinton-emails-fix-was-in/>
- David W. Nickerson and Todd Rogers, “Political Campaigns and Big Data,” *The Journal of Economic Perspectives* 28, no. 2 (2014): 51–73, JSTOR: 23723484
- Will Oremus, “‘Is This Something That’s Going to Haunt Me the Rest of My Life?’” *Slate*, December 14, 2016, accessed August 9, 2018, http://www.slate.com/articles/technology/future_tense/2016/12/an_interview_with_charles_delavan_the_it_guy_whose_typo_led_to_the_podesta.html
- Publius Decius Mus, “The Flight 93 Election,” *Claremont Review of Books*, September 5, 2016, accessed August 9, 2018, <https://www.claremont.org/crb/basicpage/the-flight-93-election/>
- Ned Parker, Jonathan Landay, and John Walcott, “Putin-linked Think Tank Drew up Plan to Sway 2016 Us Election - Documents,” *Reuters*, April 19, 2017, accessed August 10, 2018, <https://www.reuters.com/article/us-usa-russia-election-exclusive/putin-linked-think-tank-drew-up-plan-to-sway-2016-us-election-documents-idUSKBN17L2N3>
- Maryalice Parks, “What We Learned from the Purported John Podesta Emails from Wikileaks,” *ABC News*, October 12, 2016, accessed August 9, 2018, <https://abcnews.go.com/Politics/learned-purported-john-podesta-emails-wikileaks/story?id=42713413>
- Adam Pasick and Tim Fernholz, “The Stealthy, Eric Schmidt-backed Startup That’s Working to Put Hillary Clinton in the White House,” *Quartz*, October 9, 2015, accessed August 9, 2018, <https://qz.com/520652/groundwork-eric-schmidt-startup-working-for-hillary-clinton-campaign/>
- Mcnamara Paul, “Buzzblog: Palin E-mail Snoop Sentenced to a Year in Custody,” *Network World*, November 12, 2010, accessed August 15, 2011, <http://www.networkworld.com/community/blog/palin-e-mail-snoop-sentenced-year-prison>
- Jarred Prier, “Commanding the Trend: Social Media As Information Warfare,” *Strategic Studies Quarterly* 11 (4 2017), http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf
- Beth Reinhard, “Who Will Inherit Obama’s Voter Database?,” *National Journal*, 2012, 12, <https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=84134945&site=ehost-live&scope=site&custid=airuniv>
- Ariel Rosenstein, “The Stats Don’t Lie: Almost 20 Years Later, the Drudge Report Is Still the Top News Aggregator,” *The Market Intelligence Blog*, October 6, 2015, accessed August 10, 2018, <https://www.similarweb.com/blog/the-stats-dont-lie-almost-20-years-later-the-drudge-report-is-still-the-top-news-aggregator>

- Michael Scherer, “Inside the Secret World of the Data Crunchers Who Helped Obama Win,” *Time*, November 7, 2012, accessed August 9, 2018, <http://swampland.time.com/2012/11/07/inside-the-secret-world-of-quants-and-data-crunchers-who-helped-obama-win/>
- Alex Seitz-Wald, “Bernie Sanders Camp: The Fix Was in against Us,” *NBC News*, November 4, 2017, accessed August 9, 2018, <https://www.nbcnews.com/politics/elections/bernie-sanders-camp-fix-was-against-clinton-n817501>
- Travis Sharp, “Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony,” *Journal of Strategic Studies* 40, no. 7 (2017): 898–926, accessed November 24, 2017, doi:10.1080/01402390.2017.1307741
- Xiaokui Shu et al., “Breaking the Target: An Analysis of Target Data Breach and Lessons Learned,” *ArXiv*, 2017, accessed August 20, 2018, arXiv: 1701.04940
- “Hacker Begins Distributing Confidential Memos Sent to Hillary Clinton on Libya, Benghazi Attack,” *The Smoking Gun*, March 18, 2013, accessed August 6, 2018, <http://www.thesmokinggun.com/buster/sidney-blumenthal/hacker-distributes-memos-784091>
- Justin Worland, “Edward Snowden and Wikileaks Disagree Over How to Share Government Secrets,” *Time*, July 29, 2016, 59
- Andrea Valdez, “Everything You Need to Know about Facebook and Cambridge Analytica,” *Wired*, March 23, 2018, accessed August 9, 2018, <https://www.wired.com/story/wired-facebook-cambridge-analytica-coverage/>
- Sarah Westwood, “14 Things We Learned from Wikileaks’ New Clinton-related Emails,” *Washington Examiner*, October 11, 2016, accessed August 9, 2018, <https://www.washingtonexaminer.com/14-things-we-learned-from-wikileaks-new-clinton-related-emails>
- Kim Zetter, “Palin E-mail Hacker Says It Was Easy,” *Wired*, September 18, 2008, accessed August 6, 2018, <https://www.wired.com/2008/09/palin-e-mail-ha/>
- Simon van Zuylen-Wood, “Does This Man Know More Than Robert Mueller?,” *Daily Intelligence*, January 2018, accessed August 10, 2018, <http://nymag.com/daily/intelligencer/2018/01/glenn-greenwald-russia-investigation.html>

Day 10: Cyberspace in International Relations and Strategy

Today’s class focuses on how information changes change global political strategy. Cyberpower and cybersecurity will influence strategy for the foreseeable future. How has it shaped strategy so far? What have you learned in SAASS 667 that changes how you view national security? What would you like to know that you have not yet learned?

Required Reading:

- Brandon Valeriano, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford University Press, May 15, 2018)

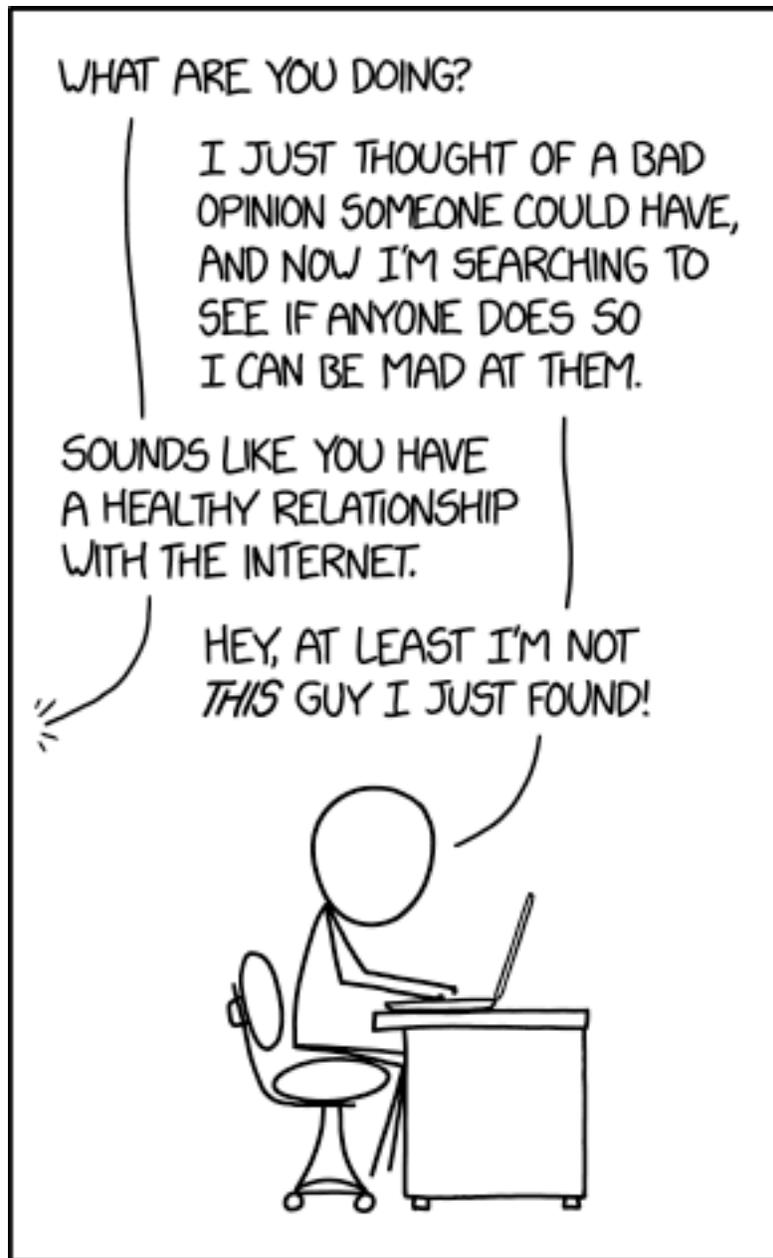


Figure 12: “This means war!” if only in our own minds.

Recommended Reading:

- Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, May 26, 2015)
- Lucas Kello, “The Meaning of the Cyber Revolution,” *International Security* 38, no. 2 (2013): 7–40, accessed July 12, 2017, <https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=91709783&site=ehost-live&scope=site&custid=airuniv>
- Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press, 2017)

- Ryan C. Maness and Brandon Valeriano, “The Impact of Cyber Conflict on International Interactions,” *Armed Forces & Society* 42, no. 2 (2016): 301–323, doi:10.1177/0095327X15572997, eprint: <http://afs.sagepub.com/content/42/2/301.full.pdf+html>, <http://afs.sagepub.com/content/42/2/301.abstract>