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
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)](image)

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

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.
3 Information Into Action

Day 2: How Do People Do Things Together?

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:
Recommend Reading:

Day 3: Social Mobilization

![Figure 6](image)

*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:**

**Recommended Reading:**
- Doug McAdam, Sidney G. Tarrow, and Charles Tilly, *Dynamics of Contention* (New York: Cambridge University Press, 2001)
**Day 4: Counter-Mobilization (What Governments Do)**

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:**
• 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:
• Donatella Della Porta, Social Movements, Political Violence, and the State: A Comparative Analysis of Italy and Germany (Cambridge, England: Cambridge University Press, 1995)
• Jennifer Gandhi, Political Institutions under Dictatorship (New York, NY: Cambridge University Press, 2008)

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:**


**Recommended Reading:**

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:
Recommended Reading:

- Appendix B.

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
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:**


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 Informationn Warfare,” in Circle City Con 2018 (Indianapolis, IN, June 1, 2018), https://youtu.be/gOrqa5dBxHY

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

- Derek E. Bambauer, “Ghost in the Network,” University of Pennsylvania Law Review 162, no. 5 (5 2014)
- Craig Fields, Task Force on Cyber Deterrence, research report (Department of Defense, Defense Science Board, February 2017)
• Brett Hawkins, *Case Study: The Home Depot Data Breach*, research report (SANS Institute, January 2015)


• Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press, 2017)


• Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009)

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

**Required Reading:**


**Recommended Reading:**


• Adam P. Liff, “The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio,” *Journal of Strategic Studies*, 2013, 1–5


16
Figure 11: There’s no kill like over kill.


• David E. Sanger, *The Perfect Weapon* (Crown/Archetype, June 19, 2018)


**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 coursework 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:**


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


Not In Reader

Recommended Reading:


● 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)


• 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


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

**Recommended Reading:**

