SAASS 667
Academic Year 2021
Information, Cyberspace, and Cyber Power
8 – 23 April 2021

Instructors:
Col Nate Huston (Course Director)
Dr David Benson

Syllabus Approved: ________________________
Date: ______________
SAASS 667
Information, Cyberspace, and Cyber Power

Introduction & Overview

Be not afraid, intrepid warriors. The end is nigh – you have nearly completed your time here at SAASS. Lucky for you, your final full course is one that contains mystery, intrigue, nerd stuff, and a whole lot of pondering (kind of like the rest of SAASS).

Now, many of you are thinking to yourselves, “Selves, how could SAASS have left this very exciting course for the end of the year? I’ve been dying to learn more about cyber and info!” Others of you (a minority, surely) may be thinking to yourselves, “Selves! How could SAASS think that here, at the end of the year, I would have any time or mental capacity to try to learn about this clearly overly nerdy world of beeps and squeaks?” Well, fear not! There is something here for everyone, from the “true believer” to the skeptic, from the generalist to the cyberspace professional. This course simply requires each of us to keep an open mind but read, think, and engage each other with a critical eye and intellectual curiosity.

Make no mistake: The intent of this course is not to make you cyberspace experts. Instead, it offers an opportunity to examine and investigate the practice of strategy within the context of cyberspace and information. What makes this domain of competition and conflict different from other domains? How is it similar? Is the information domain the same as cyberspace? What does cyberspace even mean? What is the difference between Information Warfare, Cyber Warfare, and Influence Operations, if anything? How might the introduction of cyber3e-dfc -e- capabilities to the battlespace alter how we fight, if at all? What does it mean to compete in cyberspace? Is deterrence possible in cyberspace? Is there any such thing as war in cyberspace? And why are we asking all of these questions as if cyberspace is separate and apart from all of the other domains anyway?

As we wrestle with these questions, we will no doubt discover that not only are their answers elusive, but simply through asking them we will open doors to many other unanswered questions. We hope that by the end of the course, though many of these questions may remain unanswered, we will have gained a better appreciation and comprehension of strategy by, with, and through information and cyberspace.

Below you will find an overview of this year’s course. Please note that due to the alterations in our schedule, two days have been removed. You will still receive these books, but we will not read them for class. Additionally, since we will begin on a Thursday vice a Monday, our “Week 1/Week 2/Week 3” overviews are somewhat disjointed, but suffice to say that we believe that the books still hang well together in this construct and we hope that the weekly overviews help to frame the transitions as we proceed through the course. Finally, please also note that the evaluative method for this course is different from your past courses. Strategy requires adeptness of mind and method, and we hope that you will find this slight departure from the norm to be a stimulating opportunity to frame your thoughts and arguments in a different, but perhaps more commonly utilized, format.
Week 1 Theme: Cyber 101 – On a Global Scale

Lesson 1: What is Cyber?
- Introduction to cyber concepts
- Understanding cyber threats

Lesson 2: Why is Cyber Matter?
- Importance of information security
- The impact of cyber threats

Lesson 3: What is Computer Science?
- IT fundamentals
- Common cyber security threats

Week 2 Theme: Hacking Society, Hacking the Government…The Intersection of Cyber & Info

Lesson 4: How People Connect
- Social media
- Online communication

Lesson 5: How Does AI Work, Exactly?
- Artificial intelligence
- Machine learning

Lesson 6: How does a Study of How Cyber Operations Act
- Study of cyber operations
- Understanding cyber operations

Week 3 Theme: Information in Action…The Promise (& Peril?) of Cyberspace

Lesson 7: How do Cyber’s promises hold? What is that magic algorithm actually doing?
- Cyber promises
- Algorithmic magic

Lesson 8: What is (plausibly) the most important or widely held misconception about the strategic use of cyberspace and information?
- Misconceptions about cyberspace

Lesson 9: What can it do, and what should make a single claim, and support it with logic and limited evidence.
- Claim presentation

Lesson 10: Don’t freak out! We know you haven’t had formal instruction regarding the art of writing an Op-Ed, 600 words, no formal citations, one hierarchy of section labels are allowed. You may use hyperlinks (think blog post), but they are not required.
- Op-Ed writing

Lesson 11: What is Big Data’s magic algorithm actually doing?
- Data analysis
- Algorithmic magic

- Cyber warfare
- Information warfare

Core theme: Cyber

Course Faculty: Col Nate Huston (CD), Dr David Benson

8-23 April 2021

SAASS 667: Information & Cyberpower
Evaluation

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.

**Due:** COB on the final day of class, submitted via email to your instructor’s .edu email account.

**Prompt:** What is (plausibly) the most important or widely held misconception about the strategic use of cyberspace and information?

**Format:** Write your response as an Op-Ed, 600-1000 words, no citations, no title, one hierarchy of section labels are allowed. You may use hyperlinks (similar to a blog post), but they are not required. Your Op-ed should make a single claim, and support it with logic and limited evidence. To assist with crafting your op-ed, reference the guides below.

**References:**

**Faculty**

Col Nate Huston
Prof David Benson
Course Texts


Department of Defense. Summary of the Department of Defense Cyber Strategy, text, September 2018; Washington, DC.


White House. National Cyber Strategy of the United States of America, text, September 2018; Washington, DC.
What do you think about when you hear the word “cyberspace?” For most, this word immediately evokes computers, and we will begin from this natural starting point. Security and competition in cyberspace can be intimidating, and difficult to comprehend. Fortunately, as strategists we do not necessarily need to understand the intricacies of computer security, per se, but rather how they affect strategy writ large. This week begins with a survey of significant cyber operations over the last decade, progresses with a debate over the importance and definition of cyberspace operations vis-à-vis our understanding of warfare and geopolitical competition, and closes with a contemplation of what all of this means in the context of operational execution and policymaking.
A Brief (Recent) History of Cyberspace and Cyber Conflict

Required Reading: Buchanan, *The Hacker and the State*

A wise SAASS professor once said that “history is the evidentiary database for strategy.” We begin our study of information and cyber power with a survey of recent significant cyber operations and ponder how, if at all, they have altered the geopolitical landscape upon which states compete.
Is War in Cyberspace War?

Required Reading: Rid, *Cyber War Will Not Take Place*

Is “war” in cyberspace even war? Our author today suggests that Uncle Carl would say that it is not. Rid relies heavily on a definitional argument to suggest that whatever is going on in cyberspace, it is not war. Is that a valid premise from which to argue? Does it matter? Is this argument optimistic or pessimistic about the introduction of cyberspace operations into the realm of interstate competition?
Does it Matter if “Cyber War” is “War” or Not?

Required Reading: Kello, *The Virtual Weapon*

Does it matter if we consider what is happening in cyberspace “war” or something else? In contrast to our last author, Kello suggests that whatever you call it, it matters. Kello submits, in fact, that not only do cyberspace capabilities matter, indeed they have the ability to destabilize the international system. In making his argument, Kello advocates moving past an antiquated Clauswitzian view of technology and warfare, which he suggests is overly focused on the state, and contends that the rise of cyberspace capabilities have empowered new, sub- or extra-state players to subvert the existing international system and disrupt it from within or without. What do you think about this argument? Does Kello make a persuasive case that operations by, with, and through cyberspace have the potential to disrupt the Westphalian system? What about Rid’s argument that these capabilities are nothing truly revolutionary, that they instead represent simply the latest technological iteration of the age-old “dark arts” of sabotage, espionage, and theft? Might they both be right?
Does it Matter if “Cyber War” is “War” or Not?

We make the leap today from theory to application (sort of...we can’t let go of theory entirely!). Our readings reflect how we (and by “we,” we mostly mean the US) think about these problems today and where we think we might need to look in the future. Cyberstrategy is a developing branch of strategy, and it is in the very early phases of that development. Theoretically, cyberstrategy is closer in development to Giulio Douhet than to Thomas Schelling, especially when we consider that what we consider to be the global internet did not exist at all until 1995, and China and Russia only surpassed 10% broadband internet penetration in the last decade. Today’s readings are mostly evenly divided among scholars who focus on cybersecurity-related issues and those who focus on non-cyberspace related issues. All the authors in Lin & Zegart are seeking traction to apply extant theories to cyberstrategy and vice versa. Pay special attention to cases and arguments that you believe pull assumptions from strategic interactions that may apply unevenly in cyberspace, or assumptions that hold true in cyberspace which may not be accounted for in theories developed to explain other interactions.

* Posted to Teams
The theme for this week suggests that we will discuss the intersection of cyberspace power and the information sphere…consider critically whether these two intersect at all, or whether they are inseparable in the first place. Hacking is not just about computers, as we can see in our current political climate. Hacking using computers interacts with people, and even when cyberspace operations are not involved, or are simply means to an end, information is a vital component of political and strategic interaction. Even without using a single “cyber attack,” it may be necessary to “hack” a society to create strategic outcomes.

Some of the ideas presented in this section will seem familiar, especially in light of your explorations of irregular warfare and technology and innovation, but cyberspace specifically and information generally have idiosyncratic characteristics strategists should account for. Computers are a major component of modern innovation, and are vital to technologies like Artificial Intelligence. There will, therefore, be overlap between technological innovation in strategy and information strategy, but the overlap is not perfect. Similarly, networks and network operations inform a sizable portion of unconventional warfare. Unconventional warfare varies based on terrain and social structure, and strategic use of information operations has its own set of constraints and capabilities. Build on the similarities, but recognize the differences, for in the gaps lie strategic advantage.

Whereas last week we focused more on the technology itself, this week we focus more on those purposes for which technology might be leveraged. Specifically, we hone in on the cognitive domain and how information might be manipulated, through cyberspace or otherwise, to influence geopolitics to one’s advantage. Discussions involving information or cyberspace operations often find themselves mired in the technical, as if the activities undertaken in a single domain are constrained to it. Keohane and Nye, however, reminded us way back in 1998, in the age of the information superhighway, that “information does not flow in a vacuum but in a political space that is already occupied.”

Consider that sentiment as we move forward this week.

---

How People Connect

Required Reading: Kadushin, Understanding Social Networks

Today’s reading is essentially an undergraduate textbook on social network analysis (SNA) that would probably occupy the better part of a semester for undergraduates. As graduate students, you get a day, but you also are not going to be called upon to actually conduct any of these analyses. SNA is a common tool in strategic and academic analysis, and is especially popular in intelligence. Unfortunately, just because something is popular does not mean that everyone does it right. Most people in Alabama drive, but almost no one drives in such a fashion that inspires great confidence.

When reading this book you should learn the concepts and verbiage that will help you more systematically explain and reason through networks. Although the book uses social networks as an example, the math for network analysis describing computer networks is identical. Many of the concepts and perhaps even some of the cases described have appeared in other classes. This book has proven both popular and challenging with past graduates, because it introduces more precise words for concepts that they are already familiar with and adds new ideas that occur frequently in life. Come to class prepared to ask and answer questions about the ideas herein, and if you do not completely understand at the start, try to know what you do not understand so you can understand at the end.
Hacking the Government: Power to the People…or Not?

Required Reading: Tufekci, *Twitter & Tear Gas*

Almost from the moment the internet was developed, people projected their political hopes and fears on it. People blamed the internet for the Oklahoma City bombing in 1995, as if poor white supremacists were a rampant part of the text based pre-World Wide Web internet. People hoped the internet would collapse the nation state system, or enable a “people power” revolution. Today we take a hard look at those claims, with an eye towards strategically important issues. Generally speaking, analysts argue that the internet either makes control harder or easier to establish. While military strategy is not the whole of political control, political control is an element of military strategy.

Pay close attention to arguments about political control and the relationship between causation and co-occurrence. We like democracy at SAASS, and many people who like democracy think the internet is a tool to create democracy. Today’s reading explores some of the ways the internet can help democracy develop in countries where it did not exist before, but it also points to the perils that reliance on this new technology can bring. This book is one of the latest in a lineage dating back twenty years, and attempts to account for some of the previously hoped-for revolutions that never materialized or fell apart. Notably, if this book is correct about the importance of the internet in social movements, several ongoing conflicts will be shaped by their internet origins, for better or for worse.
Social Media and Statecraft

Required Reading: Singer & Brooking, Likewar

Online society is still society, and hacking that society is more a social than a technological exercise. Today’s reading explores the use of social media as a tool against the US (predominantly). The core case is the US election in 2016, which before the 2020 election was arguably the most discussed source of angst in the American body politic. While we all have political feelings, please try to set them aside to understand what actually happened, and what the potential effects were. Feel free to argue however you choose, including introducing outside information, but be prepared to defend your information sources.

The role of information in social networks is a tricky thing made more complicated by the need to use information to talk about information. Thinking clearly about information is closely related to thinking clearly about epistemology, which is extremely challenging. Unfortunately, information and its effects in society are vital to strategists in a way that pure epistemology is not. Perhaps what is most important in understanding information’s role in social “hacking” is remembering that even within agreed upon objective truth, weighting the relative importance of empirical, verifiable facts creates materially different viewpoints. If Ben Kenobi can argue that cutting off his friend’s legs and leaving him burning in a pit of lava is the same as a villain murdering that same friend is “True…from a certain point of view…” then we must remain open to the idea that even without any variance at all in the truth, people might arrive at different conclusions. The ability to speak and think clearly about what is causing those differences will prove a boon to all strategists.
It’s All Fake News

Required Reading: Rid, Active Measures (Intro, Chs 1-11, 13, 24-31, Conclusion)

We close this week with an examination of operations within the information sphere that have not and do not require cyberspace capabilities, though their use may ultimately enhance the effectiveness of the underlying efforts. Variously referred to as “active measures,” “disinformation,” “political warfare,” and a myriad of other terms, our focus today is on operations arguably of particular concern to those in open, democratic societies. As we will discover, the sunlight of open societies is at once a spectacular disinfectant and also an opportunity for nefarious actors to cast shadows in directions of benefit to themselves.

For argument’s sake, let us consider that some adversary did achieve some level of influence on that which this country, and many other western democracies, hold most dear: the exercise of democracy through free, fair, and transparent elections. Consider, in fact, that the adversary need not actually have any direct effect on said elections, but to simply sow doubt in the population over their veracity. As we have already seen, this has the potential to increase discord and friction within those populations to such a level so as to displace all but the most clear and present danger. Now consider that those effects might be achieved without deploying a single troop, rolling a single tank, or launching a single aircraft.
Today’s readings comprise the opening salvo in our final (shortened and off by two days) week of Cyber & Info. You’ll note that there is no “overarching” summary for this week. It pains your Course Director too deeply to reflect on what could have been. Instead, you’ll get a sense for the theme right here and in the discussion of the reading for tomorrow. This week we turn from the information itself and focus more closely on its use in decision-making. That’s not to suggest that we have not talked about its use over the last two weeks, but the readings for today and tomorrow focus more squarely on “information in action” and specifically, how we might think about “cyber-assisted” decision-making and its promises and perils.

The short Foreign Affairs article assigned is a very brief look at the argument made by Cukier and Mayer-Schoenberger in their book. It will give you a birds-eye view of what we mean when we talk about “big data.” Keep in mind that this term is increasingly thrown about with a very loose interpretation of what it means and how it can be realistically utilized. One thing that Cukier and Mayer-Schoenberger do point out is that in some cases, big data offers the promise to leverage correlation alone without always requiring that ever-elusive enchantress, causation. But not in all cases! As you’ve hopefully learned here at SAASS, asking the right questions is often at least as important as finding the right answers.

Our main reading for today is from 2011 USAFA grad, former USAF AI Chairperson, and current Director of Operations for Air Force/MIT Artificial Intelligence (what have I done with my life?). This book continues the AI journey you began in 660, with a slightly deeper dive into both the history and current uses of AI at the nation-state level. Whereas during 660 we asked you to consider AI primarily through a technological lens as a recent innovation, we peer here through an information and decision-making lens, examining AI’s role on the geopolitical stage. Consider how these lenses alter your view of AI and how Kanaan’s viewpoint differs from that of Lee, if at all.
It’s Certain to be Uncertain

Required Reading: Jervis, *Why Intelligence Fails* (Chs 1, 3-4) and Duke, *Thinking in Bets*

On this sad, sad day, as we bid you adieu, we begin with a reading by a perennial favorite of SAASS, Bob Jervis. This book is a compilation of a recently declassified study he did for the CIA that sought to uncover why the intelligence community missed the fall of the Shah in Iran paired with an examination of why the same community missed on WMDs in Iraq. Though we won’t read the Iran chapter for class, you may not be surprised to learn that the report was less thoroughly read by Agency leadership than Jervis had expected. My bet, after working for the government for twenty years or so, is that its length played a significant factor (the executive “summary” alone is over twenty pages!). The Iraq chapter is based on open-source information. Consider your own perceptions of our “failure” regarding WMDs in Iraq, then consider Jervis’s conclusions about said failure. What does it portend for the future? Are we destined to fall short, no matter how exquisite our intelligence is?

Our final reading of the course is written by Annie Duke, a World Series of Poker champion and “decision strategist.” One of your SAASS professors is fond of describing strategy as placing bets on the future. Duke asks her readers to get comfortable with the discomfort of uncertainty. You may find some parallels between her discussions about weighing the future and your own discussions in Strategy to Practice. You’re certainly familiar with her discussions of cognitive biases. What do you think about her advice regarding how to deal with uncertainty? Keep in mind that this more “accessible” book has a higher likelihood of being read outside the halls of SAASS, especially as compared to the fantastic but admittedly weightier and perhaps more intimidating tomes of Kahneman and Jervis. As you move beyond SAASS and back into the real world of military operations, with its constant demands on your, and perhaps more importantly, your people’s, time, consider how you will impart the lessons you’ve learned here at SAASS in a way that is similarly accessible and long-lasting.