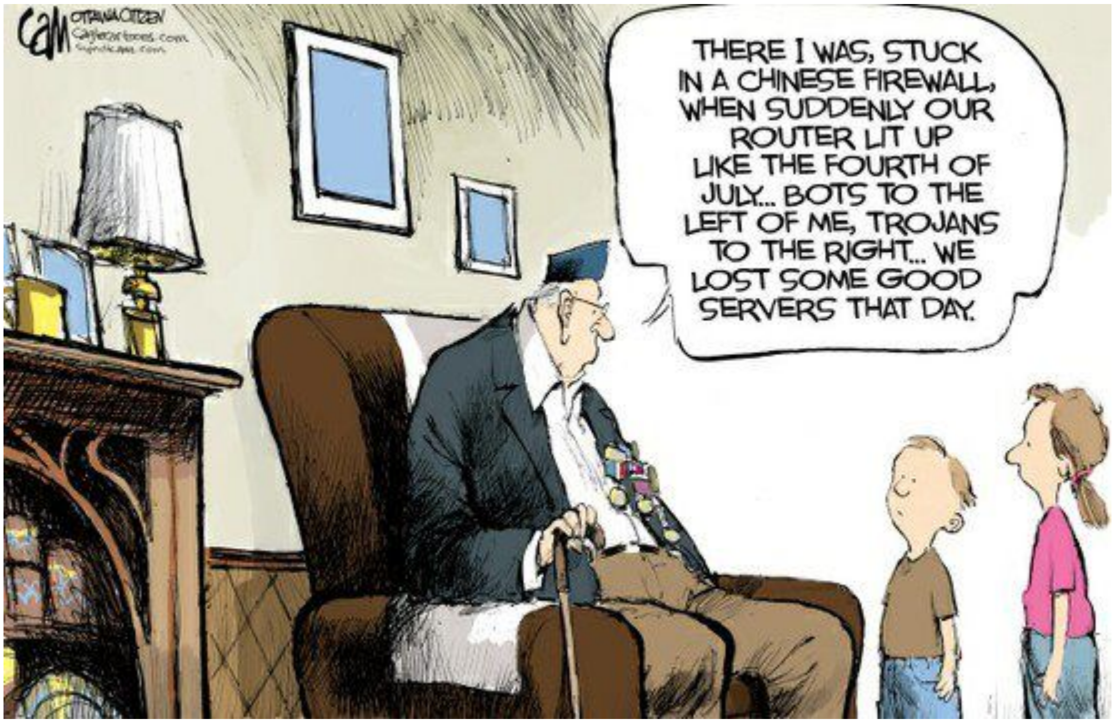
SAASS 667

Academic Year 2021

Information, Cyberspace, and Cyber Power

8 – 23 April 2021


CAM
OTTAWA CITIZEN
Cagle cartoons.com
THERE I WAS, STUCK IN A CHINESE FIREWALL, WHEN SUDDENLY OUR ROUTER LIT UP LIKE THE FOURTH OF JULY... BOTS TO THE LEFT OF ME, TROJANS TO THE RIGHT... WE LOST SOME GOOD SERVERS THAT DAY.

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.

SAASS 667 Information & Cyberpower 8-23 April 2021

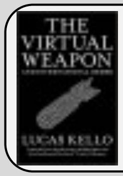
Course Faculty: Col Nate Huston (CD), Dr David Benson

Core theme: *Cyber's hard. But not as hard as you think! As it turns out, lots of things are pretty similar to other domains. Of course, lots of things are different as well. Does coercion look the same in cyberspace? What about deterrence? Is cyber all about information, or is it about hacking bad guys? Can we have an effect in cyberspace without "hacking?" What about all this big data and AI talk? Is that cyber? Or is it something else? Cyber Warfare, Information Warfare, Political Warfare, Influence Operations....which is which? Does it matter? We may not achieve consensus and will likely end up with more questions than we started with, but we're going to ask better questions and be able to leverage the capabilities more readily to conceive of and achieve better strategic outcomes.*

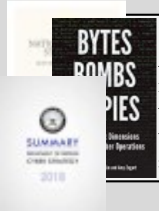
Week 1

Lesson 1: *What is Cyber Anyway?* An accessible survey of major cyber operations over the past few decades and how they impact geopolitics.

Lesson 2: *Cyber Stuff Isn't War Stuff*. Cyber ops aren't war in the Clauswitzian sense, but rather sabotage, espionage, and theft.



Lesson 3: *Oh, Cyber Matters Alright.* Does it matter if we don't **call** it war? Seems like it's a pretty big deal. It alters the international order. Cyber is competition. Buckle up.

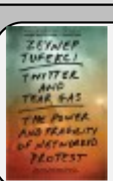


Lesson 4: *Theory to Policy & Practice.* What does all of this mean when the rubber hits the road? How do things look today and how ought they be shaped for tomorrow?

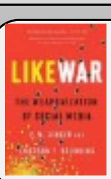
Week 1 Theme: Cybering all of the Things...on a Geopolitical Scale

Week 2

Lesson 5: *How People Connect*. Kicks off a week that could find a home in 644 (IW). Offers concepts & vocabulary to describe human connectivity.



Lesson 7: *Power to the People...or Not?* Connectivity promises the ability to organize and galvanize, but at what long-term cost?

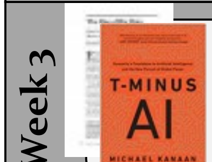


Lesson 6: *Social Media & Statecraft*. How can social media be used to influence people and politics? What role might influence operations play in the future?

Lesson 8: *It's All Fake News*. No need for guns or fancy hacking. How about simply undermining democracy from the inside? Can "great power" be exercised through the information sphere?

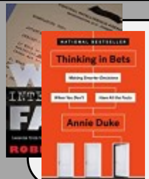
Week 2 Theme: Hacking Society, Hacking the Government...the Intersection of Cyber & Info

Week 3



Lesson 9: *Teaching Machines to Learn*. How does AI work, exactly? What can it *actually* do, and what promise does it hold? What is that magic algorithm actually doing? Bonus reading: Big Data

~~**Lesson 10**: *Just the Facts, Ma'am.* Forget computers "thinking." What about data alone? How can we harness its continual creation and avoid misinterpretation & false inferences?~~



Lesson 11: *It's Certain to be Uncertain*. Even perfect intelligence might not yield perfect decisions. How do we place bets on an uncertain future?

~~**Lesson 12**: *The Future is Now.* We end the course with a case-study of how cyber operations can have effects at a geopolitical level and ask how they might impact our future.~~

Week 3 Theme: Information in Action...The Promise (& Peril?) of Cyber-Assisted Decision-Making (Or, The New Hotness...How Hot is it Really?)

Assignment

Final Assignment: Write an Op-Ed

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 formal citations, one hierarchy of section labels are allowed. You *may* use hyperlinks (think blog post), but they are not required.

- Your Op-ed should make a single claim, and support it with logic and limited evidence.
- Don't freak out! We know you haven't had formal instruction regarding the art of writing an oped. What you *have* had, however, is practice making compelling arguments. Use that practice!
- Use the references provided in the syllabus to help guide you. Your instructor will be focused primarily on the content of your argument and your comprehension of the course material.

Note: MS Word has clearly cybered the Course Director and he is unable to fix the spacing on this overview. Be that as it may, the instructors believe it helpful enough to include.

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**:
>
> - "How to Write an Op-Ed or Column (Harvard Kennedy School) https://projects.iq.harvard.edu/files/hks-communications-program/files/new_seglin_how_to_write_an_oped_1_25_17_7.pdf (Also posted in Teams)
> - "Writing Effective Op-Eds" (Duke University): https://commskit.duke.edu/writing-media/writing-effective-op-eds/
> - "Op-Ed Writing Tips" (McGill University): https://www.mcgill.ca/newsroom/faculty-and-staff/op-ed
> - "Tips for Aspiring Op-Ed Writers" (New York Times) https://search-proquest-com.aufric.idm.oclc.org/docview/1932292551?accountid=4332 (AUL login required)
> - "The Op-Ed Project" https://www.theopedproject.org/

Faculty

Col Nate Huston
Prof David Benson

Course Texts

Buchanan, Ben. The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. United States: Harvard University Press, 2020.

Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations. United States: Brookings Institution Press, 2019.

~~Cukier, Kenneth., Mayer-Schönberger, Viktor. Big Data: A Revolution That Will Transform How We Live, Work, and Think. United Kingdom: Houghton Mifflin Harcourt, 2013~~.

Cukier, Kenneth, and Viktor Mayer-Schoenberger. "The rise of big data: How it's changing the way we think about the world." Foreign Aff. 92 (2013): 28.

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

Duke, Annie. Thinking in Bets: Making Smarter Decisions When You Don't Have All the Facts. United States: Portfolio/Penguin, 2019.

~~Greenberg, Andy. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. United States: Knopf Doubleday Publishing Group, 2020.~~

Jervis, Robert. Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War. United States: Cornell University Press, 2010.

Kadushin, Charles. Understanding Social Networks: Theories, Concepts, and Findings. United States: Oxford University Press, USA, 2011.

Kanaan, Michael. T-Minus AI: Humanity's Countdown to Artificial Intelligence and the New Race for Global Supremacy. United States: BenBella Books, 2020.

Kello, Lucas. The Virtual Weapon and International Order. United States: Yale University Press, 2017.

Rid, Thomas. Active Measures: The Secret History of Disinformation and Political Warfare. United Kingdom: Profile, 2020.

Rid, Thomas. Cyber War Will Not Take Place. United Kingdom: Oxford University Press, 2013.

Singer, P. W.., Brooking, Emerson T.. LikeWar: The Weaponization of Social Media. United States: HMH Books, 2018.

Tufekci, Zeynep. Twitter and Tear Gas: The Power and Fragility of Networked Protest. United Kingdom: Yale University Press, 2017.

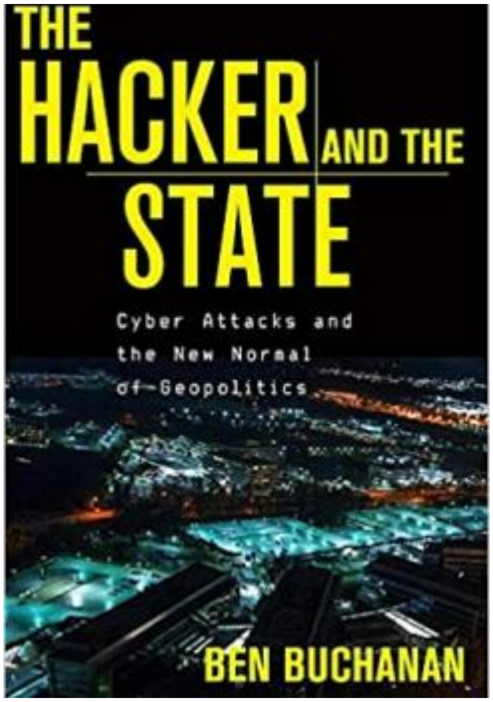
White House. National Cyber Strategy of the United States of America, text, September 2018; Washington, DC.

Week 1: Cybering All of the Things…on a Geopolitical Scale

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.

SAASS 667 Day 1 8 April 2021

A Brief (Recent) History of Cyberspace and Cyber Conflict

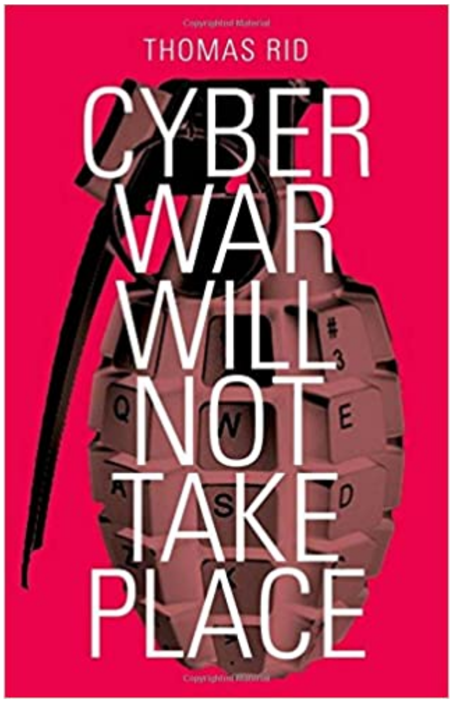


Required Reading: Buchanan, *The Hacker and the State*

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.

SAASS 667 Day 2 9 April 2021

Is War in Cyberspace War?

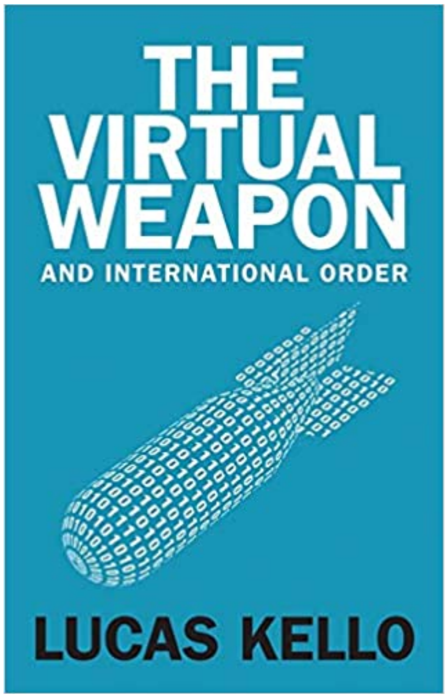


Required Reading: Rid, *Cyber War Will Not Take Place*

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?

SAASS 667 Day 3 12 April 2021

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?

SAASS 667 Day 4 13 April 2021

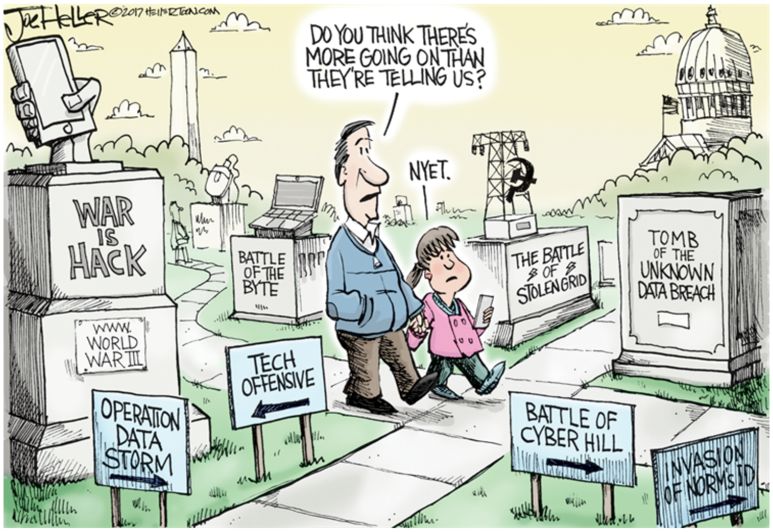
Does it Matter if "Cyber War" is "War" or Not?

Required Reading: *National Cyber Strategy of the United States** (skim), *Summary of the Department of Defense Cyber Strategy*,* Lin & Zegart, *Bytes, Bombs, & Spies* (Chs 1-3, 8-9, 11-14)

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

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


JoeHeller ©2017 HELLERTOON.COM
DO YOU THINK THERE'S MORE GOING ON THAN THEY'RE TELLING US?
NYET.
WAR IS HACK
WWW. WORLD WAR III
BATTLE OF THE BYTE
THE BATTLE OF STOLEN GRID
TOMB OF THE UNKNOWN DATA BREACH
OPERATION DATA STORM
TECH OFFENSIVE
BATTLE OF CYBER HILL
INVASION OF NORMS ID

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.

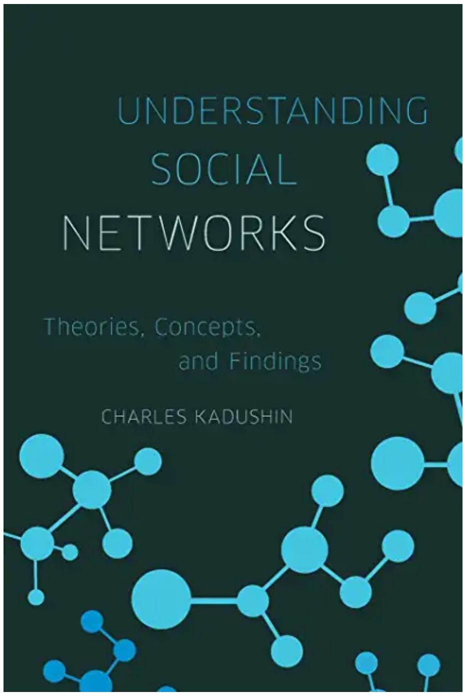
Some of the ideas presented in this section will seem familiar, especially in light of your explorations of irregular warfare and technology and innovation, but cyberspace specifically and information generally have idiosyncratic characteristics strategists should account for. Computers are a major component 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."[1] Consider that sentiment as we move forward this week.

[1] Robert O. Keohane and Joseph S. Nye, Jr., "Power and Interdependence in the Information Age," *Foreign Affairs*, September/October 1998, 84.

SAASS 667 Day 5 15 April 2021

How People Connect



UNDERSTANDING SOCIAL NETWORKS

Theories, Concepts, and Findings

CHARLES KADUSHIN

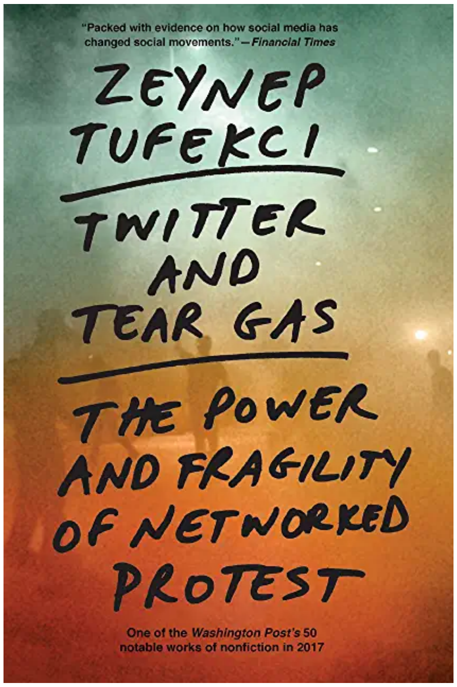
Required Reading: Kadushin, *Understanding Social Networks*

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.

SAASS 667 Day 6 16 April 2021

Hacking the Government: Power to the People…or Not?

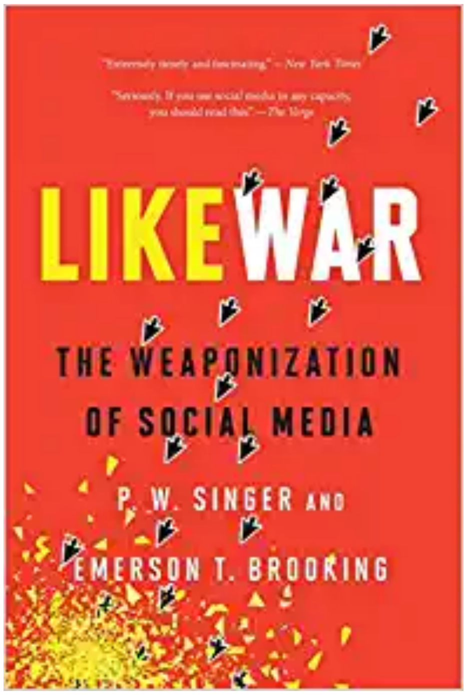

"Packed with evidence on how social media has changed social movements."—Financial Times
ZEYNEP TUFEKCI
TWITTER AND TEAR GAS
THE POWER AND FRAGILITY OF NETWORKED PROTEST
One of the Washington Post's 50 notable works of nonfiction in 2017

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


"Extremely timely and fascinating." — New York Times
"Seriously. If you use social media in any capacity, you should read this." —The Verge
LIKEWAR
THE WEAPONIZATION OF SOCIAL MEDIA
P. W. SINGER AND EMERSON T. BROOKING

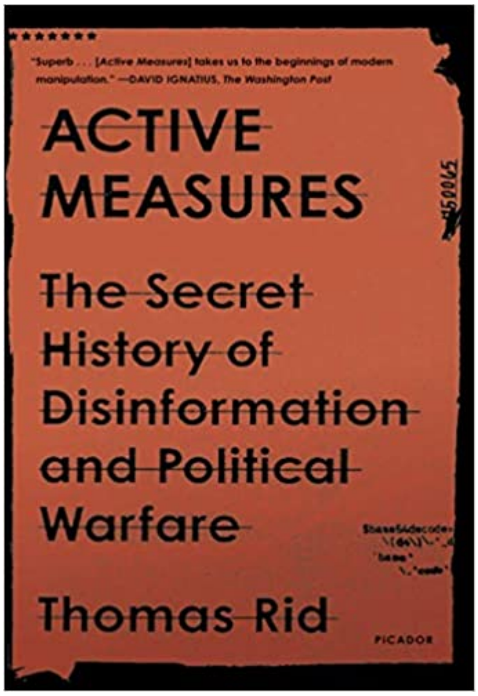
Required Reading: Singer & Brooking, *Likewar*

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.

SAASS 667 Day 8 20 April 2021

It’s All Fake News


"Superb . . . [Active Measures] takes us to the beginnings of modern manipulation." —DAVID IGNATIUS, The Washington Post
ACTIVE MEASURES
The Secret History of Disinformation and Political Warfare
Thomas Rid
PICADOR

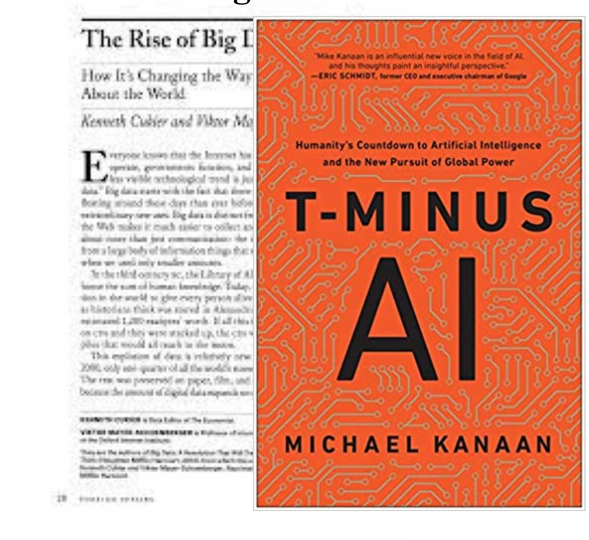
Required Reading: Rid, *Active Measures* (Intro, Chs 1-11, 13, 24-31, Conclusion)

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.

SAASS 667 Day 9 22 April 2021

Teaching Machines to Learn


The Rise of Big D
How It's Changing the Way
About the World
Kenneth Cukier and Viktor Ma
"Mike Kanaan is an influential new voice in the field of AI, and his thoughts paint an insightful perspective."
—ERIC SCHMIDT, former CEO and executive chairman of Google
Humanity's Countdown to Artificial Intelligence and the New Pursuit of Global Power
T-MINUS
AI
MICHAEL KANAAN

Required Reading: Kanaan, *T-Minus AI* and Cukier & Mayer-Schoenberger, *Rise of Big Data*

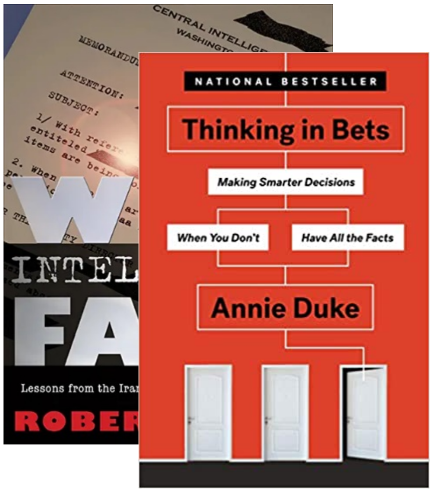
Today's readings comprise the opening salvo in our final (shortened and off by two days) week of Cyber & Info. You'll note that there is no "overarching" summary for this week. It pains your Course Director too deeply to reflect on what could have been. Instead, you'll get a sense for the theme right 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-Shchoenberger 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.

SAASS 667 Day 10 23 April 2021

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.