SAASS-667: "Information and Cyberpower"

David Benson (CD) Nathaniel Huston Stephen Wright

2 March 2020

Col. Shawn T. Cochran, PhD.</ br> Commandant, SAASS

Assignment

Due: COB on the final day of class, submitted through Canvas.

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*, and you may use one hierarchy of section labels if you choose. Formatting does not matter, and you may paste the response can as text into the assignment turn-in window on Canvas. 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 available on Canvas. The discussion boards on Canvas are open to allow you to "test run" your arguments against one another. Your grade will only reflect what you submit, but you can post whatever you like to the discussion boards, respond to one another, and argue your points. Done properly, a discussion is a great way to refine your arguments.

Cybering the Cyber out of Cyber in the Cyberspace

Day 1

Cyberspace is new compared to other environments and issues strategists care about, but not as new as it may seem. The cybersecurity concerns that dominate a sizeable chunk of military planners energy today were not even considerations twenty years ago. Starting in the 1980s, strategic actors including the US Government and military squared off against one another when pursuing strategic advantages. Today's reading is *not* a novel, but it reads like one, and is a foundational text in hacker culture. The types of attacks Stoll describes continue to work today, and many of the ideas found in *The Cuckoo's Egg* reappear in contemporary cybersecurity.

NOTE: *The Cuckoo's Egg* was adapted into a film, remarkably starring Clifford Stoll, who is in no way whatsoever an actor. While you are welcome to view the film, possibly in the presence of two robotic puppets, please do not rely on it.

- Stoll. 2005. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*

What you think Cyberstrategy is about

Most people thinking about cyberstrategy will immediately jump to computers, and so will we. Computer security and the issues surrounding computer security can be difficult to comprehend at a detailed level for people unfamiliar with information security practices. Fortunately, as strategists, you do not need to understand how computer security works, per se, but only how it affects strategy. We will skim the wave tops of computer security in this section of the course. Engebretson is provided as a reference to help you delve deeper into specific cybersecurity issues if you wish.

NOTE: Engebretson does give you sufficient information to "hack" a computer or a network; do not hack computers or networks you do not own. It is illegal, and you will probably *get caught*, may *lose your security* clearance and *may go to jail*.

- Engebretsen. 2013. *Ethical Hacking and Penetration Testing Made Easy*

Day 2

While many of the principles of cybersecurity and conflict remain the same since the 1980s, many of the particulars have changed. The past 20 years have been especially important as computers and the internet has diffused beyond the western world into the former Soviet bloc and developing world. It is easy to have few cybersecurity issues when only you and your allies are online; it is a different strategic situation when international competitors and transnational actors become involved. *Dark Territory* outlines the broad arc of events, especially over the past twenty years as China and Russia became increasingly important online, and other governments and actors acquired capabilities previously monopolized by the US and its allies.

Pay attention to who is doing what to whom, but also realize there is a bias in the book towards recounting attacks in democratic countries because more information is available. When a company in the US or Great Britain suffers a cyberattack, several news organizations are likely to report on the attack from multiple sources inside the company. In Russia and China constraints on the press and lack of rule of law protections can make sharing information about cybersecurity failures costly. Operations like Stuxnet demonstrate that the US and its allies have substantial cybersecurity capabilities, even when not reported broadly.

- Kaplan. 2016. *Dark Territory: The Secret History of Cyber War*

Day 3

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 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 reading is mostly evenly divided among scholars who focus on cybersecurity-related issues and those who focus on non-cyberspace related issues. All the authors are seeking traction to apply extant theories to cyberstrategy and vice versa. Pay special attention to cases and arguments you believe that 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.

- Lin and Zegart. 2018. *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*

Day 4

How can cyberpower be used as a part of military strategy? This book attempts to introduce cyberpower to *national* military strategy, and both argues and assumes that cyberpower and military power operate with similar logics. At this point in the course, you should have an opinion on whether this book's assumptions and arguments are correct, but the book may persuade you even if you would disagree ex ante. Since cyberstrategy is so inchoate in development, look for arguments and information that you would need as a strategist to know whether this books arguments hold true generally in the future, even if they are already true now. Furthermore, focus on the argument's variables because it is possible that, while generally true, strategic interactions for which *you* are responsible may not conform to this book's theory.

- Valeriano, Jensen, and Maness. 2018. *Cyber Strategy: The Evolving Character of Cyber Power and Strategy*

Hacking Society

Hacking is not just about computers, as we can see in our current political climate. Hacking using computers interacts with people, and even when cybersecurity violations are not involved, information is a vital component of political and strategic interaction. Even without using a single "zero-day" 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 the previous two courses, but the internet 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. Technological innovation in strategy will overlap with 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 operations online and using information has different constraints and capabilities. Build on the similarities, but recognize the differences, for in the gaps lies strategic advantage.

Day 5

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 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 this book uses social networks as an example, the math and language to describe computer networks is identical. Many of the concepts and perhaps even some of the cases described herein have appeared in other classes. This book has proven both popular and challenging with past graduates because it introduces more precise words for concepts 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 the end.

- Kadushin. 2012. *Understanding Social Networks: Theories, Concepts, and Findings*

Day 6

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 is an open seeping wound in the American body politic. While we all have political feelings, please try to set them aside to understand what happened, and what 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 also 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, agreed-upon facts creates materially different viewpoints. If Ben Kenobi can argue that cutting off his friends 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 differences of perception will prove a boon to all strategists.

- Singer and Brooking. 2019. *Likewar: The Weaponization of Social Media*

Hacking Government

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. This section looks 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-occurence. While both causal and correlational relationships can be helpful to strategists, it is important to know which is which. Correlation can provide information, but is not necessarily a fruitful indicator for strategic choices. Similarly, some things only correlate by chance, or co-occur, creating seeming relationships where none exist. Take careful note of claims both authors make, and consider well which you believe are causal, correlational and happenstance.

Day 7

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. This book is one of the latest in a lineage dating back twenty years, and attempts to account for some of the previous 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 students will leave here to participate in—or at least care about as planners—were caused by the internet.

- Tufekci. 2017. *Twitter and Tear Gas: The Power and Fragility of Networked Protest*

Day 8

Not everyone who likes democracy thinks the internet is an unalloyed good for democratic governments. Today's reading was not the first book to argue that the internet might make control easier, but it may be the most vitriolic. When first published *The Net Delusion* was pushing against the dominant sense about the internet but the last five years have made Morozov's arguments more popular. Read this book with an eye to the strategic logic of control, and how the internet and information can be used to control societies and political space.

- Morozov. 2011. *The Net Delusion: The Dark Side of Internet Freedom*

Data and Information to Strategy

Information is necessary for strategy, but is not sufficient: strategists must internalize and act on information. Sometimes information is not even information, but raw data. Whether dealing with intelligence reports or databases, converting raw data and pure information into actionable, or even comprehensible information is a strategic challenge. Organizations and leaders that efficiently use information have strategic advantages over organizations and leaders that use information inefficiently. This section focuses on the process of using information.

Day 9

Todays readings come at information from two directions: converting data to meaningful information and properly using that information. *The Decision Makers Handbook* is a handbook, and a guide for people at your level in organizations on how to make organizations produce and consume data effectively using modern technology. While the specific techniques are useful, do not get bogged down in the minutiae like database structuring, and focus instead on the larger concepts of an organization and leaders creating and using information. Jervis revisited and revised some of his theory from *Perception and Misperception* in *Why Intelligence Fails* at the end of his career. We read *Why Intelligence Fails* both to see how Jervis applies his theory to intelligence specifically, rather than international relations generally, and to compare his (and your)

intellectual growth over the course of a career.

- Jervis. 2012. *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War.* Chapters 1–2,4
- Kampakis. 2020. *Decision Maker's Handbook to Data Science a Guide for Non-Technical Executives, Managers, and Founders*

Where are we now

After a whirlwind two and a half weeks, you are more educated at cyberstrategy than most people in the military, even those who outrank you. If that scares you, it should. The world is increasingly complex, and technology is an increasingly important part of that world. Realistically, very few people in the world today have a solid grasp on both the strategic and theoretical aspects of cyberspace. You now have an uncured foundation on which to build. If we could give you "the answer" we would have, but in the plus column, it is unlikely that competitors are getting "the answer" there either. Take this section as an opportunity to look back on what you have learned, and consider what you will need to know to make good decisions in the future.

Day 10

Today's reading, like the first day's reading, explores some specific issues in recent cyberspace. Hopefully, most of the ideas this reading explores now seems familiar. Pay special attention to the ways your thinking has changed over the course, and what changed your mind. If this book's account is unpersuasive, what would you need to know to believe? Consider also, given what you know now, what you think would have been better courses of action in the recent past, and what you might do should you find yourself in a similar circumstance in the future.

- Greenberg. 2019. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*