2022-12

U.S. AND PRC STRATEGIC COMPETITION: CYBER AND RISK AVERSION

Erickson, Roy H., III; McGowan, Matthew J.

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

U.S. AND PRC STRATEGIC COMPETITION: CYBER AND RISK AVERSION

by

Roy H. Erickson III and Matthew J. McGowan

December 2022

Thesis Advisor: Ryan Maness
Second Reader: Shannon C. Houck

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2022	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE U.S. AND PRC STRATEGIC COMPETITION: CYBER AND RISK AVERSION	**5. FUNDING NUMBERS**
6. AUTHOR(S) Roy H. Erickson III and Matthew J. McGowan	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The People's Republic of China (PRC) altered its calculations from the aftermath of the 1990 Persian Gulf war and placed emphasis on the importance of technology and information. The PRC created the Strategic Support Force (SSF), which became operational in 2015, and includes space, cyber, and electronic warfare capabilities under one command. Meanwhile, the U.S. has wrapped itself in structural and cultural limitations, which hinder operational tempo. This thesis examined how the Department of Defense can adjust its positions on Cyber Titles, authorities, permissions, and risk aversion in leadership to maintain a competitive edge against the threat of the PRC's SSF in the cyber domain. This thesis used system dynamics to model the economies of both the U.S. and the PRC into cyber capabilities, which resulted in an understanding that allocating additional money alone will not solve the core issue. Understanding the limitations of cultural biases, and using decision-making tools such as prospect theory, leaders can make more effective decisions. Through proper education of staff officers about cyber capabilities and their effects, integration of cyber operations at combat training centers, and pushing permissions and rules of engagements down to Task Force Commanders, the U.S. can overcome the structural and cultural obstacles.

14. SUBJECT TERMS strategic competition, risk averse decision-making, titles and authorities, SSF, Strategic Support Force, PRC, CYBERCOM, prospect theory, rules of engagement	**15. NUMBER OF PAGES** 143
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

U.S. AND PRC STRATEGIC COMPETITION: CYBER AND RISK AVERSION

Roy H. Erickson III
Major, United States Army
BS, Florida State University, 2000

Matthew J. McGowan
Major, United States Marine Corps
BS, United States Naval Academy, 2011

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION STRATEGY AND POLITICAL WARFARE

from the

NAVAL POSTGRADUATE SCHOOL
December 2022

Approved by: Ryan Maness
Advisor

Shannon C. Houck
Second Reader

Carter Malkasian
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The People's Republic of China (PRC) altered its calculations from the aftermath of the 1990 Persian Gulf war and placed emphasis on the importance of technology and information. The PRC created the Strategic Support Force (SSF), which became operational in 2015, and includes space, cyber, and electronic warfare capabilities under one command. Meanwhile, the U.S. has wrapped itself in structural and cultural limitations, which hinder operational tempo. This thesis examined how the Department of Defense can adjust its positions on Cyber Titles, authorities, permissions, and risk aversion in leadership to maintain a competitive edge against the threat of the PRC's SSF in the cyber domain. This thesis used system dynamics to model the economies of both the U.S. and the PRC into cyber capabilities, which resulted in an understanding that allocating additional money alone will not solve the core issue. Understanding the limitations of cultural biases, and using decision-making tools such as prospect theory, leaders can make more effective decisions. Through proper education of staff officers about cyber capabilities and their effects, integration of cyber operations at combat training centers, and pushing permissions and rules of engagements down to Task Force Commanders, the U.S. can overcome the structural and cultural obstacles.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADP	Army Doctrinal Publication
AOR	area of responsibility
BRI	Belt and Road Initiative
CLD	Causal Loop Diagram
CTC	combat training centers
CYBERCOM	Cyber Command
DIMEFL	Diplomatic-Information-Military-Economic-Financial-Legal
DOD	Department of Defense
EUT	Expected Utility Theory
GCC	Geographic Combatant Command
GDP	Gross Domestic Product
IOC	initial operating capability
JP	Joint Publication
LOAC	Law of Armed Conflict
MCF	Military-Civil Fusion
NDAA	National Defense Authorization Act
NDS	National Defense Strategy
NSD	Network Systems Department
OIE	Operations in the Information Environment
PLA	People's Liberation Army
PRC	People's Republic of China
ROE	rules of engagement
SSD	Space Systems Department
TMA	traditional military activities

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The People's Republic of China (PRC) observed the United States (US) effectively, and efficiently defeat Saddam Hussein's 3rd largest army in the world during the 1990–1991 Persian Gulf War. Chinese military planners encoded an important lesson from this war: they anticipated that information and technology would be key to winning future wars. In response, the PRC streamlined their technical/information operations decision making process and created the Strategic Support Force (SSF), which became initial operating capable in 2015. This new command directly supports the PRC's theatre commands and is broken into two distinct departments: 1) the Space Systems Department, and 2) the Network Systems Department. This organization not only places, cyber, information operations, and electronic warfare under one command, but also was explicitly created to avoid bureaucratic red tape and modernize itself for the new information age.

The U.S., on the other hand, has multiple organizations that use cyber operations but are separated by different Titles and Authorities. As a result, multiple layers of bureaucracy exist that limit the ability for the Department of Defense to operate quickly and efficiently. To address this problem, this thesis examined how the Department of Defense can adjust its positions on Cyber Titles, Authorities, Permissions, and risk aversion in leadership to maintain a competitive edge against the threat of the People's Republic of China's Strategic Support Force in the cyber domain.

While the U.S. currently holds the most advanced capabilities in cyber, according to, the PRC is on the heels of the U.S. at number 2.[1] Moreover, despite its advanced capabilities, U.S. information planners and practitioners consistently report problems *using* those capabilities largely because of restrictive authorities and permissions to conduct certain operations in information / cyber domains. According to the current cyber titles and authorities, the Department of the Defense (DOD) does in fact have the appropriate titles and authorities to conduct the actions that it wants to do, but those permissions rely mostly

[1] Julia Voo et al., *National Cyber Power Index 2020: Methodology and Analytical Considerations* (Cambridge, MA: Belfer Center for Science and International Affairs, 2020), 8, https://www.belfercenter.org/publication/national-cyber-power-index-2020.

with Cyber Command. However, although the DOD has the appropriate authorities, there is a sense of risk aversion in leadership either to either preserve one's career or afraid of escalating tensions against an adversary by using said capabilities.

This thesis conducted research in several areas, first using Systems Dynamic Modeling, this thesis examined how money is allocated from the economies of both the U.S. and the PRC and found that allocating money alone to address the problem does not solve the core issue of the restrictive bureaucratic processes that exist. Secondly, this thesis examined what are the current Titles and Authorities for the DOD and whether the DOD must request additional authorities within cyber operations, which it does not need to. The third area was in the task organization of the Strategic Support Force and the streamlined threat they pose, and finally how a risk averse culture is promulgating throughout the DOD and how to combat that through prospect theory. Prospect theory delivers a new perspective to the issue of risk aversion identified within this thesis. It allows commanders to objectively look at a situation and make an informed decision that is not based on individual biases.

Based off the research, and analysis, this thesis makes the following recommendations to the DOD leadership to continue to compete within the limitations:

1. Education—provide / create education on the capabilities, effects, and planning processes for cyber operations to Task Force Commanders' **staffs** and above. This will facilitate the staffs being able to present effective and dynamic courses of actions to the decision makers based off the requisite knowledge of cyber capabilities and the effects looking to be achieved. The education can occur at resident PME schooling through the use of a mobile training team, or by sending key staff members to service component commands at USCYBERCOM.
2. Training—provide training exercises / evolutions that will allow cyber tactical teams to practice their Mission Essential Task Lists either offensive or defensive cyber in a closed network directly tied to a larger exercise for a future supported commander.

3. Rules of Engagements—push permissions along with the approval to conduct cyber operations down to Task Force Commanders to operate more dynamically and at a faster operation tempo, which will put the adversary on the defensive rather than the offensive.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to extend our deepest appreciation and thanks to the instructors, supervisors, and staff of the Defense Analysis Department at the Naval Postgraduate School. Specifically, within the Defense Analysis Department, Dr. Ryan Maness, who served as an expert guide and mentor through the cyber domain, and Dr. Shannon Houck, whose expertise and knowledge in social psychology assisted us in the development and framework of our thesis. We would also like to send our sincere and special thanks to Mrs. Greta Marlatt, who assisted us in meeting all academic standards and expectations.

Finally, we would like to thank our families who have supported us through the research design, development, and finalization of this thesis, and allowing us to work long hours on this thesis and our education at the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

I. STRATEGIC COMPETITION AND 21ST CENTURY CONFLICT

A. INTRODUCING THE STUDY

Shifting paradigms produce an air of uncertainty and chaotic discourse. The shift in modern warfare from the war on terrorism to the evolution of cyber technology and multi-domain conflict between states is proving to be no exception. Even when doctrine exists to provide a stable footing for execution of cyber operations, the aversion to risk can hinder the calculus of decision making to the detriment of advantageous alternative courses of action. Within the past 20 years, a certain philosophy has taken hold within the United States government: when facing a risk of failure, cut your losses and move on to the next mission. However, U.S. adversaries do not subscribe to this same philosophy and, as a result, continue to make strides in the advancement of innovative technologies and hybrid integration. The 4th Industrial Revolution has brought with it an added complexity that our enemies intend to exploit should we not begin to address the root causes of indolent adoption for change steered by risk averse decision makers.

1. Identifying the Problem

The United States and China find themselves vying for an edge over one another in this era of strategic competition. China has slowly and systematically become a dominant force in the domains of land, sea, air, space, and information, becoming peers with the United States.[1] Cyber has become the 5th domain for the United States and the Chinese have adopted information as a domain as well. Cyber-attacks, economic espionage, and the increasing expansion of the information environment, has placed a microscope over cyber security, capabilities, and policies. Although the United States currently holds the most exquisite capabilities in cyber, according to the Harvard Belfer National Cyber Power Index (HBNCPI) of 2020, the People's Republic of China (PRC) is on the heels of the U.S. The Japan Center for Economic Research in Tokyo believes that the Chinese economy is

[1] James Dobbins, Howard J. Shatz, and Ali Wyne, *Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue: Different Challenges, Different Responses* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/perspectives/PE310.html.

set to surpass the U.S. economy by 2030 or 2033, and the goal of the PRC's military is to surpass the U.S. military in certain areas by 2035, the DOD needs to adjust to maintain its advantage.[2] Using the Belt and Road Initiative (BRI) as a vector, the Chinese continue to expand its economy, military capability, and influence, throughout the INDO-PACOM area, the Middle East, and Eastern Africa. The BRI is a massive infrastructure initiative, mirroring the Silk Road, which seeks to spread the development and influence of China's economic and political influence from East Asia to Europe. Through this, the Chinese are bringing multiple countries either forcefully, or voluntarily under its direction. The Belt and Road Initiative, as of now, consists of "more than sixty countries—accounting for two-thirds of the world's population—have signed on to projects or indicated an interest in doing so" many of which are economic or military partners with the United States.[3] With this initiative comes the expansion of China's communications conglomerate Huawei and the allegations of the spying it conducts on behalf of the PRC. Huawei has been accused of spying on military bases, NATO, and other private industry organizations.[4] While the U.S. cannot change how or what the Chinese do, the U.S. can effectively signal capabilities and warnings to maintain its competitive edge despite this massive effort.

2. Purpose and Scope

The purpose of this study is to identify effective ways that the United States Department of Defense (DOD) can decentralize some of the decision-making process with certain cyber capabilities to maintain the competitive edge. The flexibility to fight within each area of responsibility (AOR), and specifically within Indo-Pacific AOR, will signal to the adversaries that the DOD is adapting to the accelerated pace of technology and hybrid

[2] Stella Yifan Xie, "China's Economy Won't Overtake the U.S., Some Now Predict," *Wall Street Journal*, September 2, 2022, sec. World, https://www.wsj.com/articles/will-chinas-economy-surpass-the-u-s-s-some-now-doubt-it-11662123945; John Xie, "Will China Surpass the U.S. in Military Air Superiority?," VOA, October 13, 2021, https://www.voanews.com/a/when-will-china-surpass-the-us-in-military-air-superiority-/6270069.html.

[3] Andrew Chatzk and James McBride, "China's Massive Belt and Road Initiative," Council on Foreign Relations Backgrounder, January 28, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

[4] Eva Dou, "Documents Link Huawei to China's Surveillance Programs," *Washington Post*, December 14, 2021, sec. Asia, https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.

warfare. This thesis will be scoped to analyzing the PRC's cyber threat in the task organization of the Strategic Support Force (SSF) but more specifically the Network Systems Department (NSD), which carries out their cyber capacity.

3. Thesis Question

This thesis will seek to provide recommendations to the following question. "How can the Department of Defense adjust its positions on Cyber Titles/Authorities/Permissions and risk aversion in leadership to maintain a competitive edge against the threat of the People's Republic of China's Strategic Support Force in the cyber domain?"

B. LITERATURE REVIEW

The literature review is broken into six sections. The first section discusses the limitations of the research and findings due to the classification and compartmentalization nature of cyber and the capabilities. Second, the chapter will discuss strategic competition, integrated deterrence, and the heavy importance that the U.S. National Defense Strategy (NDS) calls on the need for effectively competing against U.S. adversaries, particularly the PRC. Third, this chapter will lay out the PRC's general strategy and how the development and creation of the Strategic Support Force, more specifically the Network Systems Department, embodies their newfound strategy. Fourth, the chapter will analyze the current existing cyber permissions, titles and authorities that are permitted under the United States Code. Fifth, the chapter will detail the scholarship on the prevalence of risk aversion and how it can affect leaders' decision making based on self-interest. The final section of this chapter will advance these discussions by synthesizing core ideas and providing a foundation for understanding this thesis project.

1. Limitations of Research

Cyber capabilities, attributions, and attacks are highly classified and compartmentalized due to a country risking the exposure of such capabilities. To publicly attribute an attack to a country can, cause exposure of forensic capabilities and capacities which typically remain classified and unknown. Due to this, this paper remains at the unclassified level as not to expose potential risks/vulnerabilities/exploits. This is

advantageous due to information being open source and either widely accessible or it is known. This is also a limitation for ongoing either cyber reconnaissance or cyber operations that are currently being conducted by either side.

2. Strategic Competition

Academics and politicians have shifted from the phrase of Great Power Competition and moved to Strategic Competition. The difference between the two comes down to which political party coined the phrase, but at the heart of both phrases is the recognition that:

> The distribution of power across the world is changing, creating new threats. China, in particular, has rapidly become more assertive. It is the only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system. Russia remains determined to enhance its global influence and play a disruptive role on the world stage.[5]

The 2018 NDS shifted the DOD's focus away from violent extremist organizations, as was dictated by the wars in Afghanistan/Iraq and other military operations throughout Africa and INDO-PACOM areas. This was the first document to address the need for shifting focus back to peer & near-peer adversaries. The NDS outlined five adversaries for the DOD to begin focusing and aligning resources towards: China, Russia, North Korea, Iran, and violent extremist organizations. Of these threats, the strategy says, "long-term strategic competitions with China and Russia are the principal priorities for the Department."[6] The United States named China as the premier threat and deemed that the U.S. should start developing capabilities, modify training and equipment, and adopting new styles of thinking to compete against the adversary.

The 2018 NDS postulates that the global security environment is characterized by overt challenges to free and open international order and the re-emergence of long-term

---

[5] Joseph R. Biden, Jr., *Interim National Security Strategic Guidance* (Washington, DC: White House, 2021), 7–8, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

[6] Department of Defense, *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: Department of Defense, 2018), 4, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

strategic competition between nations.[7] This state of strategic or "Great" power competition is giving rise to a host of threats in the name of national defense that is reshaping the way the U.S. and its allies must navigate and adapt to confront modern competitive challenges. This flux is primarily due to the rapid evolution and implementation of technology. Additionally, this change is exacerbated by the hesitant nature and generational gap of policy makers unwilling or uncertain of how to proceed "in a country being revolutionized by tech."[8] This is further compounded within a society that has a "penchant for adopting new tools while still clinging to older practices."[9] This faltering approach has policy makers scrambling to behave in a reactive nature against states that are already willing to be proactive regarding the assimilation of state actions and technological advancement.

Even in the official interim national defense strategy of the United States you see that, according to Matej Kandrik, "Russia is added with a footnote that the Kremlin is not a true systemic competitor, but a regional power and major disruptor."[10] The 2020 Interim National Security Strategic Guidance says, "Russia remains determined to enhance its global influence and play a disruptive role."[11] Zach Cooper lists several reasons why Russia should not be mentioned under the same umbrella has China, when it comes to strategic competition.[12] In academia and in official White House correspondence, it is clear that China is the foremost adversarial threat that the U.S. should align its resources of the Diplomatic-Information-Military-Economic-Financial-Legal (DIMEFL) against. The 2020 Interim National Security Strategic Guidance says that "[China] is the only

---

[7] Department of Defense, 14.

[8] Avi Selk, "'There's so Many Different Things!': How Technology Baffled an Elderly Congress in 2018," *Washington Post*, January 2, 2019, https://www.washingtonpost.com/lifestyle/style/theres-so-many-different-things-how-technology-baffled-an-elderly-congress-in-2018/2019/01/02/f583f368-ffe0-11e8-83c0-b06139e540e5_story.html.

[9] John Arquilla, *Bitskrieg: The New Challenge of Cyberwarfare* (Cambridge, UK: Polity Press, 2021), 75.

[10] Matej Kandrík, "The Case against the Concept of Great Power Competition," The Strategy Bridge, June 30, 2021, https://thestrategybridge.org/the-bridge/2021/6/30/the-case-against-the-concept-of-great-power-competition.

[11] Biden, Jr., *Interim National Security Strategic Guidance*, 8.

[12] Zack Cooper, "Bad Idea: 'Great Power Competition' Terminology," Defense360, December 1, 2020, https://defense360.csis.org/bad-idea-great-power-competition-terminology/.

competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system."[13]

To attempt to curtail the efforts of the Chinese, the U.S. has developed an "integrated deterrence" policy. According to Secretary of Defense Lloyd Austin III, the U.S. will "use existing capabilities, and build new ones, and use all of them in networked ways—hand in hand with our allies and partners. Deterrence still rests on the same logic—but it now spans multiple realms, all of which must be mastered to ensure our security in the 21st century."[14] Partnering with our allies in the region is crucial in order to pose a legitimate threat towards China. However, current propaganda from U.S. adversaries will state that the U.S. is not a good ally, and when it gets tough, they will leave like they did in Iraq and Afghanistan. According to Sam Roggeveen, a few things have happened. China's "rise has accelerated" and within the region, "friends and allies in the region are quite reasonably worried about eroding credibility of American deterrence."[15] The U.S. must adapt, particularly within the cyber domain, to help restore faith in our resolve with our allies and partners. The U.S. needs to evaluate its current operations and bureaucratic processes and identify what needs to be changed to adapt to the emerging and credible threat.

3. People's Republic of China

The RAND Cooperation conducted a study analyzing China's pattern of behavior and attempted to discern what state China would be in by 2050. Their report sought to answer some of the questions proposed by the U.S. Military. The RAND Cooperation came back with three main ideas that have shaped their actions:

- Security: preserving China's basic political system and national security

[13] Biden, Jr., *Interim National Security Strategic Guidance*, 8.

[14] C. Todd Lopez, "Defense Secretary Says 'Integrated Deterrence' Is Cornerstone of U.S. Defense," U.S. Indo-Pacific Command, May 3, 2021, https://www.pacom.mil/Media/News/News-Article-View/Article/2593958/defense-secretary-says-integrated-deterrence-is-cornerstone-of-us-defense/.

[15] Edward Wong and Damien Cave, "U.S. Seeks to Reassure Asian Allies as China's Military Grows Bolder," *New York Times*, August 5, 2022, sec. World, https://www.nytimes.com/2022/08/05/world/asia/taiwan-china-united-states-allies.html..

- Sovereignty: protecting national sovereignty, territorial integrity, and national unification
- Development: maintaining international conditions for China's economic development.[16]

China's primary strategy to close the gap in development has been manipulation and coercion especially when it involves information or cyber intrusions. In their book "In Cyber Strategy," cyber experts, Valeriano, Maness, and Jensen, demonstrate how China has utilized their cyber capability to conduct espionage to manipulate and coerce others. They state that the goal of China is to match and surpass the economic and military capability of the U.S. According to Valeriano et al., "how China uses cyber espionage against rivals is a crucial example of the process of information manipulation as a limited form of coercion and ambiguous signaling."[17] This is accomplished through the realigned and restructuring of their cyber, reconnaissance, and information capabilities. Valeriano et al., in their paper "What Do We Know About Cyber War," explain that "China focuses mainly on espionage operations directed at gathering information and capability for future power projection. China's cyber strategy is more long-term, where the development of its technology and military sectors are important to its rise and quest for parity with the United States. China also uses disruptive strategies, which are usually against its regional rivals when conventional disputes manifest in the South China Sea over territory."[18]

Chinese military planners began to change their views based off the lessons learned from the Persian Gulf War in 1991. In Unrestricted Warfare, Liang argues that perhaps there are new principles of war that do not result in submitting your opponent to your will militarily but rather, "using all means, including force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's

16 Andrew Scobell et al., *China's Grand Strategy: Trends, Trajectories, and Long-Term Competition* (Santa Monica, CA: RAND Corporation, 2020), 12, https://doi.org/10.7249/RR2798.

17 Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018), 144.

18 Brandon Valeriano, Ryan C. Maness, and Benjamin Jensen, "What Do We Know about Cyber War?," working paper, 15, accessed August 5, 2022, http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/valeriano_maness_jensen_cyber_what_do_we_know_v2_.pdf.

interests"[19] Holstein explores this idea and more modern ideas, in his book New Art of War, and compares it to recent China activity within the U.S. He discusses a quote from a Zhuge Liang, a Chinese politician and military strategist from around 181–234 A.D. that discusses about what a skilled attack is and uses this quote as a framework for how the Chinese currently are waging the *New Art of War.* Zhuge Liang says, "A skilled attack is one against which opponents do not know how to defend."[20] This refers to attacking an adversary in such a way to either elicit a certain response, in today's world, within a certain domain, or give the adversary the inability to respond. Attacking the economic and societal environment is where China is focusing their cyber espionage and tactics on to gain the advantage over the U.S.

Along with Unrestricted Warfare and the new principles talked about by Holstein, China has adopted the "Three Warfares" concept. Since as early as 2003, China has attempted to incorporate psychological warfare, media warfare, and legal warfare into all aspects of operational level planning.[21] These are seen throughout its international messaging, especially when it comes to freedom of navigation claims by the United States around their territorial waters surrounding the Chinese sovereign claims in the South China Sea.[22] Their efforts are further seen in their media warfare efforts.

Since the late 1990s and early 2000s, China has shaped their domestic public opinion with the "Great Firewall" and the "Great Cannon." According to Sean Kerner, the Great Firewall is considered a "splinternet," and the information is curtailed for each region of the country and prohibits the public from accessing certain content that the PRC

[19] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999), 7.

[20] William J. Holstein, *The New Art of War: China's Deep Strategy Inside the United States* (New York: Brick Tower Press, 2019), 24.

[21] Anthony H. Cordesman, *Chinese Strategy and Military Forces in 2021* (Washington, DC: Center for Strategic & International Studies, 2021), 132, https://www.csis.org/analysis/updated-report-chinese-strategy-and-military-forces-2021.

[22] Matthew Southerland, *U.S. Freedom of Navigation Patrol in the South China Sea: What Happened, What It Means, and What's Next* (Washington, DC: U.S.-China Economic and Security Review Commission, 2015), https://www.uscc.gov/research/us-freedom-navigation-patrol-south-china-sea.

government believes goes against their messaging.[23] It's the "Great Cannon" is "a distinct attack tool that hijacks traffic to (or presumably from) individual IP addresses, and can arbitrarily replace unencrypted content as a man-in-the-middle."[24] The way the "Great Cannon" essentially works is as it is scanning the information being processed through the networks, it will remove and replace information either creating a denial of service/access, or replace the information entirely with PRC sanctioned information. It is most renowned for the denial of service on GitHub in 2018. According to Marczak et al.,

> The Cannon manipulates the traffic of "bystander" systems outside China, silently programming their browsers to create a massive DDoS attack. While employed for a highly visible attack in this case, the Great Cannon clearly has the capability for use in a manner similar to the NSA's QUANTUM system, affording China the opportunity to deliver exploits targeting any foreign computer that communicates with any China-based website not fully utilizing HTTPS.[25]

China is an authoritarian government; it affords the autonomy to apply resources it deems essential to produce the most advantageous outcomes. With the fusion of the civilian and military technological development, China can have the best of both worlds with what they can generate the best capability for both economic and military use. It can manipulate information that the public can view, see, and digest. It can leverage the academic community, their private sector industry, and military systems to capitalize on the might of an entire nation most efficiently. The SSF is the military organization that is responsible for carrying out information operations for the PRC. The streamlined organizational strategy can be seen in the development, enhancement of capabilities, and task organization of the SSF. The SSF will be further discussed in Chapter 2. This organization was meant to streamline decision-making and remove the bureaucratic concern from their targeting process, counter to the United States' centralized process and risk aversion in leaders from upsetting the current status quo.

---

[23] Sean Michael Kerner, "What Is the Great Firewall of China?," Internet technologies, June 2022, https://www.techtarget.com/whatis/definition/Great-Firewall-of-China.

[24] Bill Marczak et al., *China's Great Cannon* (Toronto: University of Toronto, 2015), 1, https://citizenlab.ca/2015/04/chinas-great-cannon/.

[25] Marczak et al., 1–2.

4. Titles/Authorities and Permissions

Cyber activity is continuously debated. Central to this debate is determining which organization has the appropriate authority (Title 10 and Title 50 Authorities) to execute cyber operations. Title 10 refers to military operations and Title 50 refers to foreign intelligence operations. However, this simplified description is more nuanced. Typically, Title 10 and Title 50 are debated in terms of which agency has the appropriate "legal" authorities to conduct an operation. Within the Title 10 authority, in part 1, chapter 19, S396, it states if a cyber capability is to be used as a weapon, the Secretary of Defense must notify the congressional defense committees. However, the exceptions to the rule are if a training exercise is being conducted and the nations participating agree to it, or if it is linked "to a covert action (as that term is defined in section 503, National Security Act of 1947 (50 U.S.C. 3093)."[26] Covert action is defined as "an activity or activities of the United States government to influence political economic or military conditions abroad where it is intended that the role of the United States government will not be apparent or acknowledged publicly."[27]

According to Tittle 10, Chapter 6, S164, subsection c, "a commander of a combatant command at any time considers his authority, direction, or control with respect to any other commands or forces assigned to the command to be insufficient to command effectively, the commander shall promptly inform the Secretary of Defense."[28] This clearly states that if a commander does not believe he has the appropriate authorities to do something, he can request them from the Secretary of Defense.

The U.S. Cyber Command (CYBERCOM) responsibilities established in Title 10 state: "the commander of the cyber command shall be responsible for monitoring the preparedness to carry out assigned missions of cyber forces assigned to unified combatant commands other than the cyber command."[29] The Cyber Commander is responsible for

[26] Notification Requirements for Cyber Weapons, 10 U.S.C. § 396 (2022).

[27] "Covert Action" Defined, 50 U.S.C. § 3093(e) (2022).

[28] Commanders of Combatant Commands: Assignment; Powers and Duties, 10 U.S.C § 164 (2022).

[29] Unified Combatant Command for Cyber Operations, 10 U.S.C. § 167b (2022).

ensuring that the individuals assigned to Combatant Commanders must be ready to execute missions that the Commanding Officers need to accomplish in support of the national/ strategic objectives within their area of operations. Within the Title 10 U.S. Code, it calls out notification requirements for any cyber effects outside of hostile areas or within those areas declared hostile. It breaks down sensitive military cyber operations, into two categories: offense and defense. "The first, offensive cyberspace operations, is not defined in statute, but by DOD, as "missions intended to project power in and through cyberspace." The second, defensive cyberspace operations, is defined in statute as operations "outside of Department of Defense information networks that are aimed at defeating an ongoing or imminent threat."[30] CYBERCOM is currently taking a "defense forward" posture with regards to cyberspace. According to the Summary: Department of Defense Cyber Strategy 2018, defending forward has three main tenets:

> First, we must ensure the U.S. military's ability, to fight and win wars in any domain, including cyberspace. Second, the Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DOD's warfighting readiness or capability. Third, [DOD] will strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing.[31]

The document mentions the term "defense/defend" 15 times while using "deter" 11 times. However, when talking or hinting towards the potential for conducting offensive cyber actions, the strategy states that it will act if deterrence fails, then the U.S. will respond. The last line states that this document will "enable the Department to compete, deter, and win in the cyberspace domain."[32] However, the ability for a country to conduct deterrence and/or compellence, must be able to signal or demonstrate that the country can impose punishment. Schelling defines deterrence as, "deterrence involves a threat to keep an adversary "from starting something," or "to prevent [an adversary] from action by fear

---

[30] Michael E. DeVine, *Covert Action and Clandestine Activities of the Intelligence Community: Selected Congressional Notification Requirements in Brief*, CRS Report No. R45191 (Washington, DC: Congressional Research Service, 2019), 9, https://sgp.fas.org/crs/intel/R45191.pdf.

[31] Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, 2.

[32] Department of Defense, 7.

of consequences."[33] Compellence, on the other hand, is defined as "a threat intended to make an adversary do something."[34] In deterrence, the punishment will be imposed if the adversary acts; in compellence, the punishment is usually imposed until the adversary acts."[35] However, these strategies will only work if the targeted country perceives the United States will act on those threats. If they do not perceive the threat as real or the potential to be credible, then there is no reason to adjust current behavior.

The United States rarely in modern history has had an adversary that can truly match its capabilities. However, what would facilitating or allowing the DOD and Geographic Combatant Commanders (GCC) to execute operations more freely with less oversight allow? The GCC align resources and capabilities towards global/regional campaign plans. These documents are plans that address a threat in a given region, essentially activated during war periods. However, in the "gray zone" or "hybrid war," which is under the full spectrum of conflict, commanders need to coerce and deter their adversaries from taking actions towards stronger conflict or ultimately, warfare. By giving GCC the authorities to do more operations within their areas of responsibility, they can shape and facilitate U.S. policy within their region, specifically in the information domain as it pertains to the Chinese threat.

5. Risk Aversion

The study of risk aversion is well documented in both economics and in psychology. In economics, the scale of which a person is risk averse is tied to their wealth. According to Abram et al., they attribute risk aversion to it being "confronted with two choices with the same expected value, they would prefer the smaller and more certain of the options."[36] Furthermore, Chayes et al., state that "to the extent that managers and employees of a firm are risk averse and that their rewards (or positions) are tired to the

[33] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 67–71.

[34] Schelling, 67–71.

[35] Schelling, 67–71.

[36] Abram Chayes et al., "Law and Economics: Risk," The Bridge, accessed August 5, 2022, https://cyber.harvard.edu/bridge/LawEconomics/risk.htm.

firm's perspective, they will want the firm to behave in a certain way."[37] In order to increase the utility of the parties involved, the personnel who are less risk averse or risk neutral will have to carry the risk.

Economists have analyzed why people may or may not be risk averse, but psychologists seek to understand where it comes from. Zhang et al. published an article titled The Origin of Risk Aversion. The article states that "risk aversion emerges as a consequence of systematic risk and that risk neutrality emerges as a consequence of idiosyncratic risk, regardless of the species and without the need for any biological production function."[38] Essentially, species are naturally predicated to make choices which assist in the further reproduction of the species. Applying this theory to a corporation or an individual, a similar conclusion can be made by Chayes et al. in the behavior will be predicated on what "rewards (or positions) are tied to the firm's perspective."[39]

Researchers from the Council on Foreign relations began looking into risk aversion as related to U.S. governmental cyber responses to foreign aggressors. As noted, the U.S. is already culturally primed for weighing the costs of action versus inaction due to a historical layering of modern catastrophic events which lead to a ubiquitous sense of insecurity and fear of what future events may come.[40]

There are military leaders who have addressed the issue of risk aversion in the DOD. In 2017, Gen. Mark Milley, Chairman of the Joint Chiefs of Staff stated, "I think we're overly centralized, overly bureaucratic, and overly risk averse, which is opposite of what we need." However, in the same breath, while addressing the idea of leaders empowering subordinates to take initiative, he states "if they achieve, hang a medal on

---

[37] Chayes et al.

[38] Ruixun Zhang, Thomas J. Brennan, and Andrew W. Lo, "The Origin of Risk Aversion," *Proceedings of the National Academy of Sciences* 111, no. 50 (December 16, 2014): 17777, https://doi.org/10.1073/pnas.1406755111.

[39] Chayes et al.

[40] Monica Kaminska, "Risk Aversion Is at the Heart of the Cyber Response Dilemma," *Net Politics* (blog), March 31, 2021, https://www.cfr.org/blog/risk-aversion-heart-cyber-response-dilemma.

them, if they fail, fire them."[41] In October of 2021, Air Force General John Hyten, the vice chairman of the Joint Chiefs of Staff made comments regarding the growing propensity of risk aversion within the government and military and how it is costing the America that we know to lose advantage. These comments are significant, as he outlined initiatives and programs over the course of his career that he was either part of or had prevue of, that were passed up due to fears of uncertainty, bureaucratic sluggishness, over classification, or reprisal.[42] Although General Hyten is bringing light to the issue of risk averse leaders and the DOD as a whole, he is making these comments at the end of his 40-year career. This aspect may be a "root" of many of the problems that the U.S. government and military machine are aware of but never seem to rectify.

The human component of risk aversion is not just limited to a response of fear and uncertainty. There is no doubt that current leaders dance around the bureaucratic inequities of risk aversion and its aftermath, though there never appears to be a codification of how the inequities can be reduced. People, it would seem, are more apt to admit or discuss freely the hindrances that plague the institutions of which they work after the risk of backfire or consequences are no longer an issue. This idea is certainly not new and considering that self-preservation is a unique human trait in that we consciously influence our natural instincts, it could be argued that this type of behavior is inherent in most if not all organizations to varying degrees.

A risk averse culture can cause leaders to make decisions based off what will protect the overall organization and or the individual making the decisions. In the United States military, commanders are often relieved when they make bad decisions, and the reasoning is typically "loss in trust and confidence" in that particular leader. When this happens, the commander/decision maker is removed from his/her position and fulfills a staff role until they are dismissed from the service. If the offense is egregious enough, that

[41] Sydney J. Freedberg, Jr, "Let Leaders Off the Electronic Leash: CSA Milley," Breaking Defense, May 5, 2017, https://breakingdefense.com/2017/05/let-leaders-off-the-electronic-leash-csa-milley/.

[42] Meghann Myers, "Risk Aversion and Secrecy Are Costing U.S. Its Military Advantage, No. 2 General Says," *Military Times*, October 28, 2021, sec. Pentagon & Congress, https://www.militarytimes.com/news/pentagon-congress/2021/10/28/risk-aversion-and-secrecy-are-costing-us-its-military-advantage-no-2-general-says/.

commander may lose additional benefits, outside of maintaining a job. As a result, commanders may make risk averse decisions to maintain their status. Against an adversary who is seeking to break the international status quo, risk aversion is a limiting factor in counteracting China's initiatives.

C. CONCLUSION

The topics covered in the Literature Review show the main themes in several areas. The development of the PRC's strategy and the development of the SSF, the importance of strategic competition and the emphasis placed on the Department of Defense stemming from the 2018 NDS, issues surrounding Titles and Authorities and how they pertain to deterrence, and finally risk aversion and the command climate that it has infected in the leadership ranks of the military. These topics combine show the current status quo for the U.S. military as they begin to be overtaken by the PRC in a peer environment, and especially in the cyber domain.

Topics regarding doctrinal development, innovation, partnerships, and integration are at the forefront of current efforts and even embedded within the highest echelon policy documents of the U.S. Government. However, a substantive vantage for the organizations that are adopting the change are inherently flawed in their approaches of implementation and execution. Certain systemic aversions and human dynamics may impede not only a successful end state but are likely to contribute to failed actions if not addressed as a legitimate area of concern and reflected in not only the policies that are created to support this transition, but the lens from which we arrive at them.

Currently, the military is developing new ideas/strategies/equipment/warfighting publications, to be able to compete against a peer adversary, as dictated initially by the 2018 NDS. However, according to the Chairman and Vice Chairmen of the Joint Chiefs of Staff, the DOD is plagued with risk averse leaders who should receive a medal if they succeed or relieve them from their command if they fail. The United States has not fought a war against a peer adversary since World War II. To successfully accomplish the grand vision of some of these warfighting techniques like Expeditionary Advance Base Operations, Multi-Domain and All-domain operations, commanders must be willing to

tolerate and reward risk-seeking tactics, techniques, and procedures from their subordinate commanders.

The PRC and the U.S. have two distinctly different views of how or what information and the technology surrounding it is. The PRC has created an organization to streamline the decision making, and in Western terms, streamline their authorities and permissions. The U.S. has multiple organizations that gather and collect information and intelligence and depending what authority under U.S. code they fall under, they may or may not be able to execute an operation under that authority or title. The following chapter will look at the current economic and cyber capacity of both the U.S. and the PRC and what the status is. The model will show that both countries are competing equally, however, future projections from both economist and military theorist predict that by 2033, the PRC will surpass the U.S. Following the model, we will present the pacing threat's organization responsible for executing its cyber/information/media warfare, then the bureaucratic limitations that the U.S. has placed on itself with current cyber titles and authorities, and the cultural predisposition and risk averse nature of the U.S. decision makers. Finally, this thesis will present recommendations of how the U.S. can still compete within these limitations against the pacing threat within the cyber domain.

II. UNITED STATES / PEOPLE'S REPUBLIC OF CHINA ECONOMIC AND CYBER CAPACITY—SYSTEMS DYNAMIC MODEL

A. INTRODUCTION TO SYSTEMS DYNAMICS

Identifying the variables that exist to form the makeup of complex systems can be an exhaustive process. The field of system dynamics allows us to bound a system to provide clarity among a forest of endless possibilities.[43] A system is identified by a particular topic or area that the researcher is trying to understand what factors have the most significant impact on it. System dynamics concepts and modeling provides data-driven insights to offset mental models that often oversimplify complex problems. For this thesis, the system is the interaction of the U.S. and China's economy and the percentage of gross domestic product that is allocated to information technology research and development. Using this, along with the cyber power index (strength of a country's cyber capabilities), will show a mathematical output for the potential number of cyber-attacks within a given year. Focusing specifically on the cyber domain, this chapter will use system dynamics to model the influences that affect cyber capabilities between the U.S. and the PRC, and some of the elements that support either country's cyber power index.

1. Causal Loop Diagram

The Causal Loop Diagram (CLD) is a systems dynamic model illustrates key elements that affect a particular model or system. The CLD can provide a valuable perspective on relationships among variables, but most importantly, relationships that matter and have influence on other aspects within a system. Causal relationships are denoted by solid and hashed lines that depict either an informational relationship (hashed line), or through causal relations (solid lines). Positive or negative associations between variables are indicated by polarity measures of causal links in the CLDs. Positive polarity (+) indicates that as the independent variable increases or decreases, the linked dependent

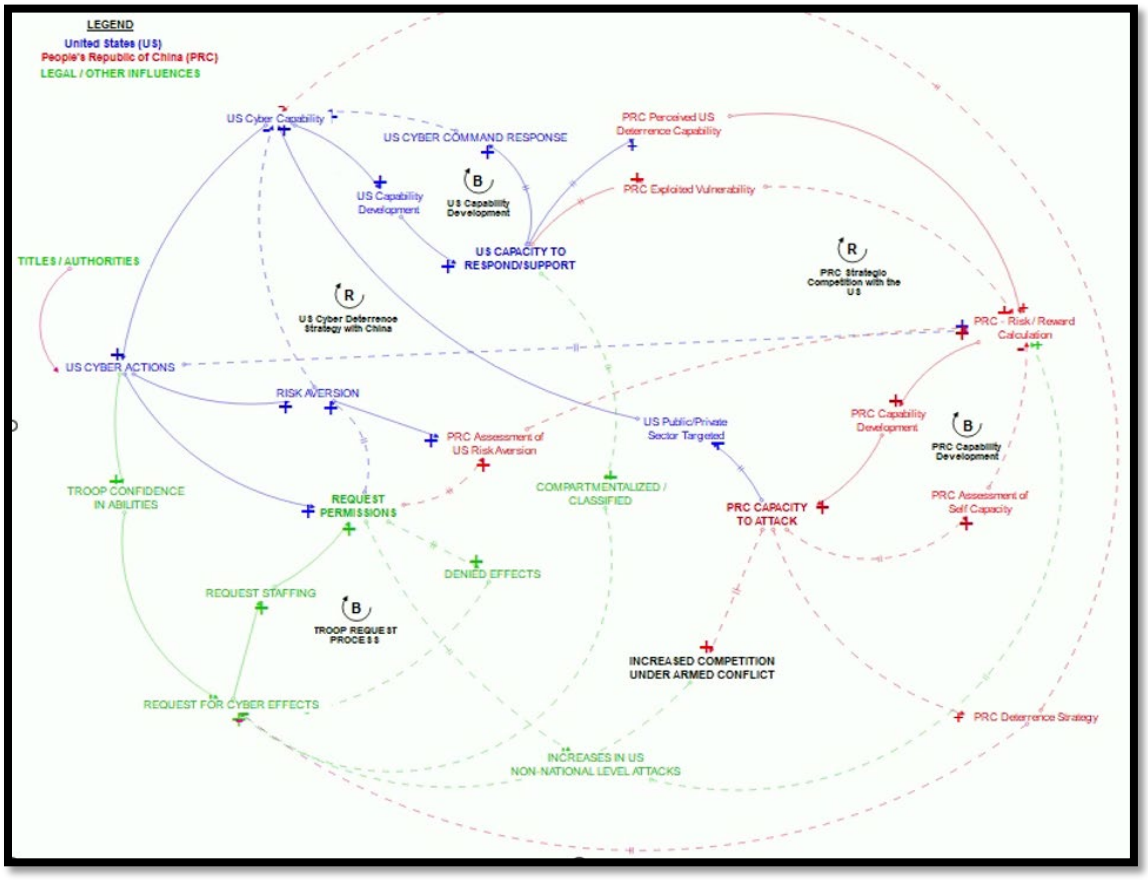
[43] John D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World* (Boston: McGraw-Hill, 2010).

variable will increase or decrease in kind beyond what it otherwise would have been (reinforcing behavior). An example of a positive polarity influence within the model is the more cyber actions the U.S. conducts, the more confidence that U.S. troops will have in its abilities. Negative polarity (-) indicates that as the independent variable increases or decreases, the linked dependent variable will decrease or increase beyond what it otherwise would have been (balancing behavior). An example of a negative polarity in our model is that the U.S. legalities surrounding over compartmentalization and classification of capabilities directly affects the number of requests for cyber effects. Overall, if a causal loop has an equal number of positive and negative polarity links, or no negative polarity links, the loop exhibits reinforcing behavior. If there is an unequal number of positive and negative polarity links in the loop, the loop will display balancing (goal seeking) behavior. Reinforcing loops are labeled with the loop identifier "R." Balancing loops are labeled with the loop identifier "B."[44]

In this thesis, our causal loop diagram, shown below in Figure 1, depicts the cycle of cyber activity and what factors help influence it. In the system modeled in Figure 1, an information warfare dynamic is taking place between the U.S. and the PRC. The blue represents the U.S. direct actions, the red represents the PRC, and the green represents other factors that either limit or reinforce an area. For example, a request is made for cyber effects, and that goes directly to "request staffing, which represents the higher headquarters staff that receives subordinate requests. The "+" indicates reinforcing, which means either positive or negative effect, it will reinforce that behavior. These requests from the staff, then move to either approval of the effect, which goes to U.S. cyber capabilities, or they are denied. If they are denied, then it reinforces (marked by the "+") the effect of less requests because of "what is the point, they will deny it anyway" mentality that permeates in the military,

[44] Sterman, 142.

Figure 1. Causal Loop Diagram of U.S. and PRC interactions ISEE Systems, Stella Software



The CLD in Figure 1 shows key variables and interactions within a system that represents U.S. and PRC opposing cyber operations. This CLD is not intended to portray behavioral outcomes of the model, but rather the underlying causes and effects that may drive the model's behavior. The intent for the CLD was to identify the fundamental causal relationships among key variables that impact the behavior of the system that represents cyber competition between the U.S. and the PRC.

While CLDs are useful for identifying the polarity of links between variables and the resultant balancing or reinforcing behavior of closed loops, it should be noted that the strength of individual links and the subsequent dominance of the loops in the behavior of the system cannot be measured without data and mathematically determining the mechanisms at play within the system. This requires the development of stock and flow

modeling and simulation. These models consist of stocks (i.e., the accumulation or integration of measurable units), in-flows and out-flows (i.e., the rate, or differentiation, of accumulation), and converters that provide mathematic inputs to the flow equations or for analysis. By reviewing the interactive cause and effect relationships of the variables within the CLD, a system dynamics stock and flow model can be created to determine how the U.S. could address the problem presented by the PRC's pursuit of offensive cyber activity.

B. DESCRIPTION OF MODELS AND ELEMENTS

As indicated from the Asia-Pacific Regional Security Assessment 2019, China has leaned heavily on the cyber domain as a path toward achieving increased economic growth and military supremacy in the decades to come.[45] A system dynamics model was created to facilitate comparative analysis of the cyber strength between the PRC and the U.S. System dynamics models are calculus-based mathematical representations of a and endogenous system that is generating problematic behavior. In this, that problem is the security threat posed by the PRC's aggressive cyber activity. These models consist of stocks (i.e., the accumulation or integration of measurable units), in-flows and out-flows (i.e., the rate, or differentiation, of accumulation), and converters that provide mathematic inputs to the flow equations or for analysis. Appendix A gives a detail description of the variables, and the naming conventions for the U.S. elements and the PRC elements of the model.

1. The United States Model

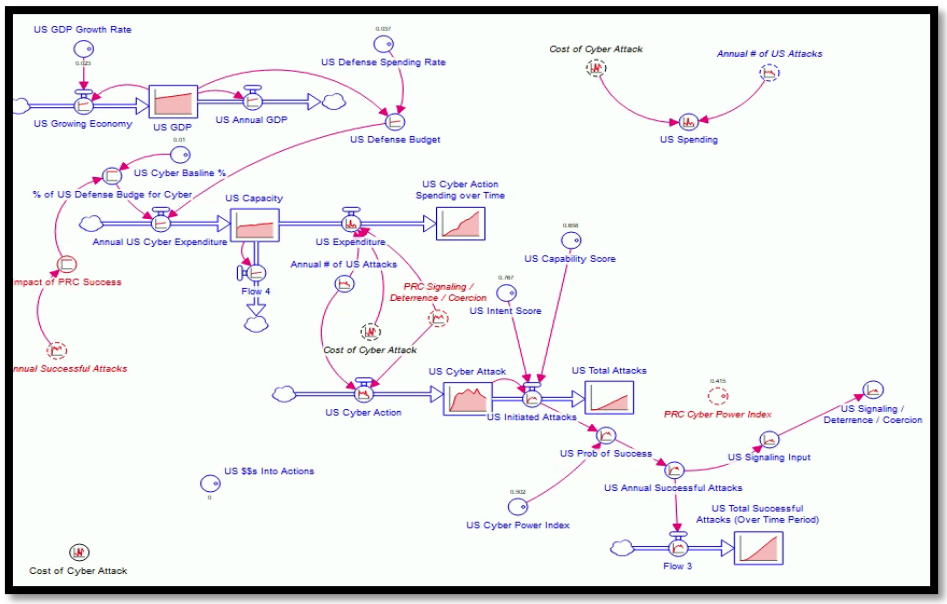
The U.S. has enjoyed an extended period of economic, military, and technological preeminence in the international community. According to the Harvard Belfer National Cyber Power Index (HBNCPI) 2020, the U.S. is also listed as number one, followed closely by the PRC at number 2, in the cyber security domain.[46] It is no coincidence that the PRC

[45] Tim Huxley and William Choong, eds., "China's Cyber Power in a New Era," in *Asia-Pacific Regional Security Assessment 2019: Key Developments and Trends* (London: International Institute for Strategic Studies, 2019), 77–90, https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5.

[46] Voo et al., *National Cyber Power Index 2020*, 8.

also has the number two economy in the world. The Gross Domestic Products (GDP) of the U.S. and the PRC were used in the model to simulate the percent spent by each country on defense and ultimately how this contributes to their respective cyber activity. The stock and flow modeling structure of U.S. and PRC cyber activity mirror each other. Figure 2 shows the U.S. section of model.

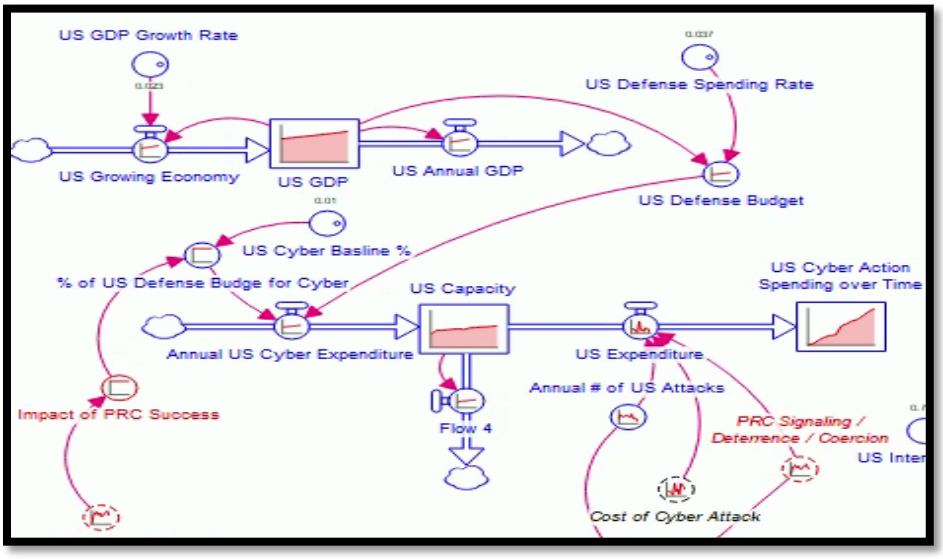
Figure 2. U.S. Model—ISEE Systems, Stella Software



In Figure 3, the converter of "US GDP Growth Rate" goes into the flow of the U.S. Growing Economy and is increased annually multiplied by the U.S. GDP Growth Rate. The GDP is calculated with an initial value based on the 2020 GDP for the United States as reported by The World Bank.[47]

47 "GDP (Current US$) – United States," World Bank, accessed November 1, 2022, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US.

Figure 3. U.S. Gross Domestic Product and Defense Budget Flow ISEE Systems, Stella Software



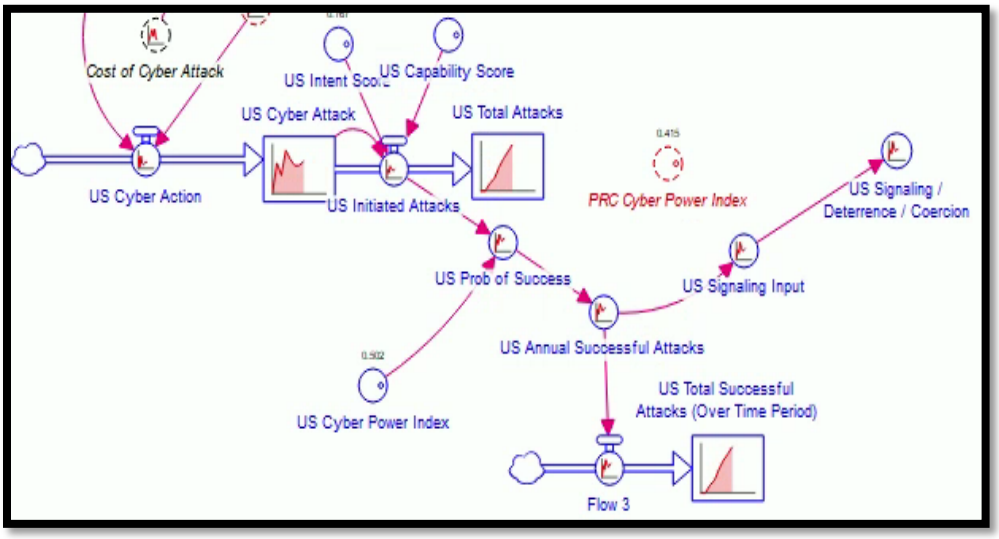
According to the International Business Times Article, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K Icefog," there is a wide range of cyber capabilities that range from as low as $10,000 U.S. dollars up to a few million.[48] A random distribution was added to the model in order to accommodate for the various costs for creating a certain type of cyber capabilities. The minimum established was $10,000 and the maximum established was $500,000 U.S. dollars.

From the converter "Annual # of U.S. attacks" into the flow cyber action, as depicted in Figure 5, U.S. cyber action is converted from U.S. Expenditures (in units of dollars) into U.S. Cyber Actions (in units of events). To determine the number of events, the formula of "Annual # of U.S. attacks" / ("PRC Signaling, deterrence, coercion" * "Annual # of U.S. attacks"). This captures the number of cyber-attacks the United States is conducting and flows into initiated attacks as shown in Figure 4. Using the HBNCPI 2020, the intent to use a cyber capability and the capability scores are incorporated into the potential number of attacks to create the number of initiated attacks in a given time step.

[48] David Gilbert, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog," *International Business Times*, February 6, 2014, sec. CyberSecurity, https://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451.

These initiated attacks are then multiplied by a binomial distribution with using the cyber power index of the United States (.502) as the probability of success, which will produce the number of attacks that are successful. These successful attacks are accumulated in the U.S. total Successful Attacks (Over Time) stock. The PRC structure in the model follows a similar process. This was done in order to do a comparative analysis.

Figure 4. U.S. Successful Cyber Attacks—ISEE Systems, Stella Software



2. People's Republic of China

The PRC has been on the rise since Chinese President Xi Jinping rose to power. According to HBNCPI 2020, China is poised in the number 2 slot by a narrow margin behind number one U.S. and is slowly increasing in capability and capacity.[49] The models listed in Figure 5 are similar in format by using the PRC GDP and breaking it down by the percent spent on defense spending and ultimately how it derives to a successful cyber-attack.

[49] Voo et al., *National Cyber Power Index 2020*.

Figure 5. PRC Model ISEE Systems, Stella Software

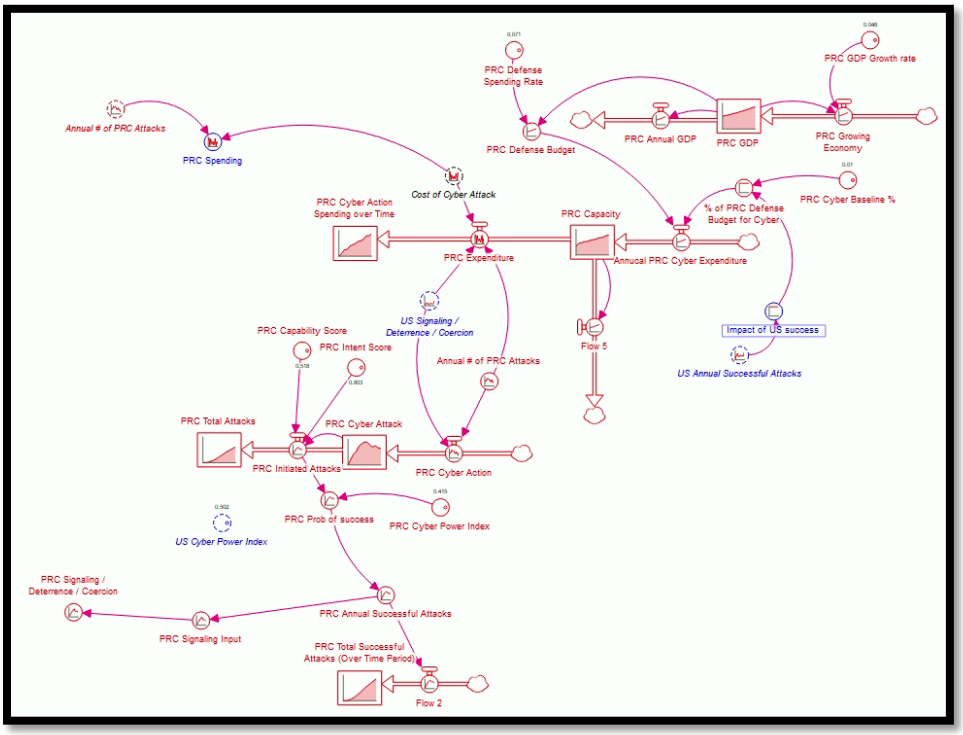


Figure 6 shows the PRC and Defense Budget Flow, which mirrors the structure of the U.S. model discussed above.

Figure 6. PRC Gross Domestic Product and Defense Budget Flow ISEE Systems, Stella Software

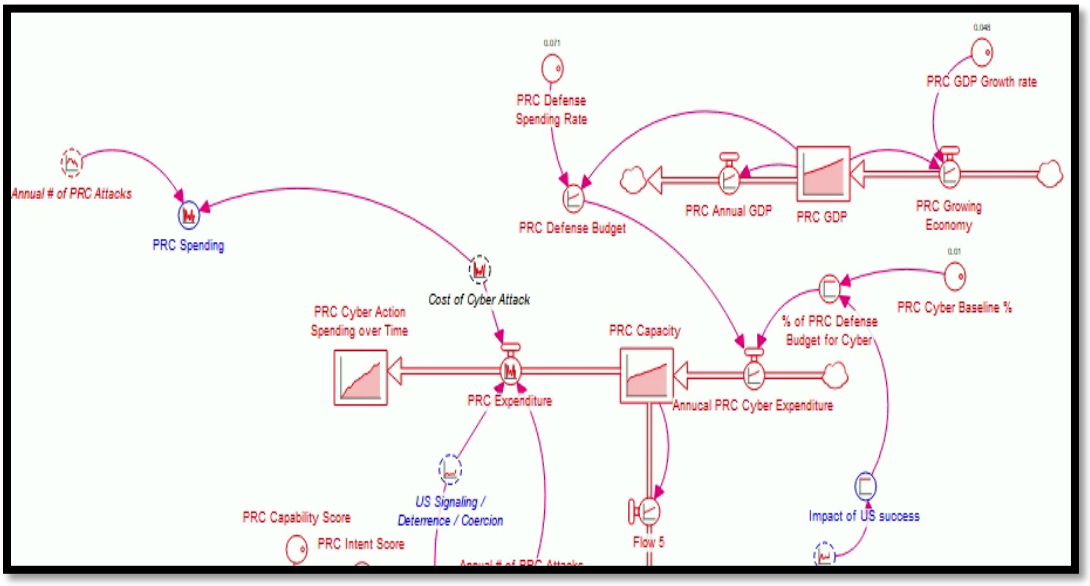
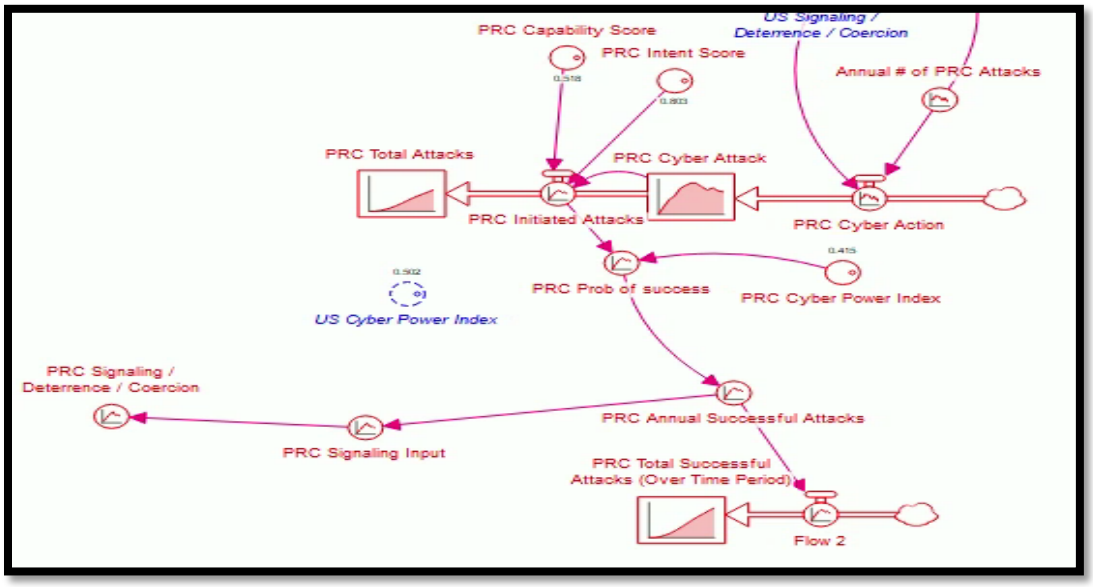


Figure 7 shows the structure of the PRC Successful Cyber Attacks portion of the model, that mirrors that of the U.S. model. cyber action is created transitioning from $US dollars into an event. Of note, the PRC Initiated Attacks are multiplied by a binomial distribution with using the cyber power index of China (.414) as the probability of success, which will produce the number of attacks that are successful.

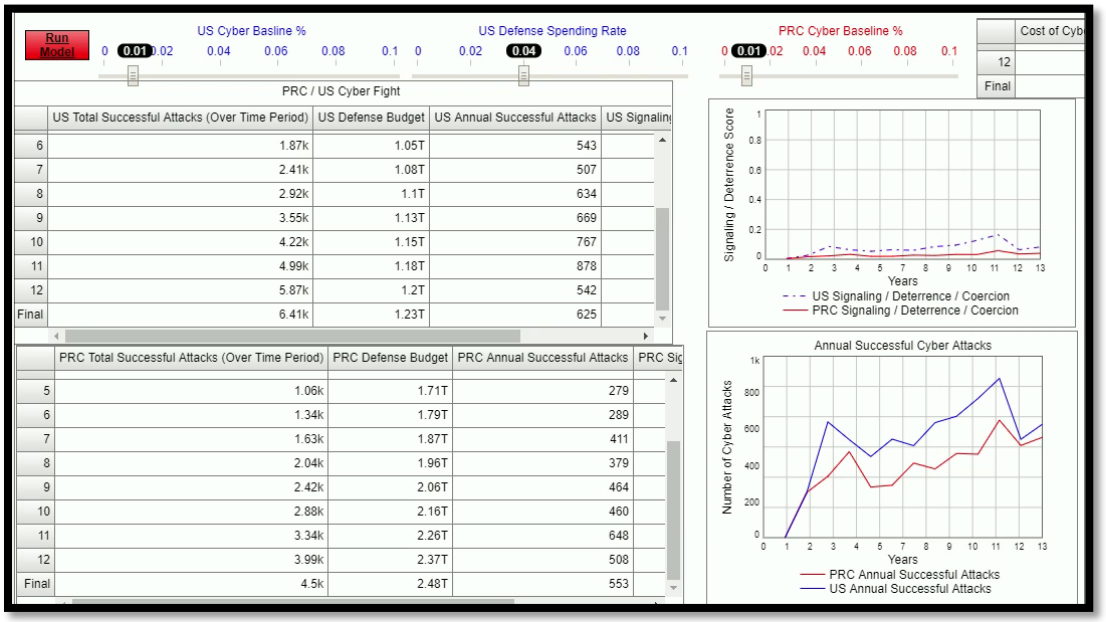
Figure 7. PRC Successful Cyber Attacks ISEE Systems, Stella Software



C. RESULTS AND INTERPRETATION

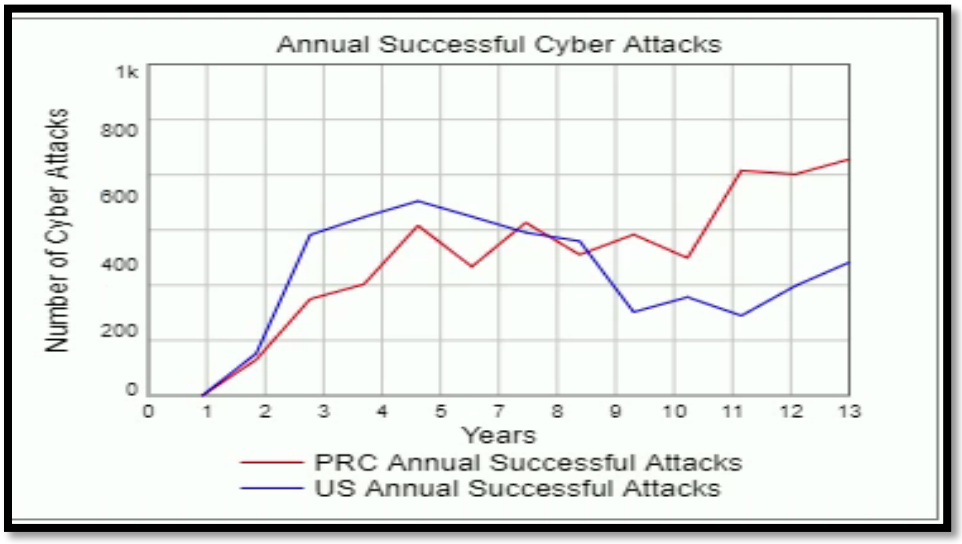
An interface was created to allow the user to shift spending percent both from the U.S. and PRC "Cyber Baseline %" converters within the model. Unless the percentages are manually adjusted, the status quo "Cyber Baseline %" holds steady at 1% for both nations. This was important to ensure results provided a baseline of understanding for the model. The interactive interface provides the user results over the models simulated run of 13 timesteps (i.e., in years). As indicated from the titles of each column, the results received are comparative; US/PRC Successful Attacks, US/PRC Defense Budget, US/PRC Annual Successful Attacks, and US/PRC Signaling Deterrence. The visual presentation of outcomes is identified through line graphs over the 13-year run of simulation.

Figure 8. Picture of Interactive Interface on Stella ISEE Systems, Stella Software



The simulation demonstrates significant variation in the number of successful cyber-attacks conducted by each country over time. The graph in Figure 9 shows the number of successful cyber-attacks by yearly timestep in one such simulation run.

Figure 9. Graph and Table of U.S. / PRC Simulation (Run 1)—ISEE Systems, Stella Software



	US Total Successful Attacks (Over Time Period)	US Defense Budget	US Annual Successful Attacks	US S
6	1.74k	1.05T	540	
7	2.28k	1.08T	492	
8	2.77k	1.1T	466	
9	3.24k	1.13T	252	
10	3.49k	1.15T	297	
11	3.79k	1.18T	241	
12	4.03k	1.2T	331	
Final	4.36k	1.23T	402	

	PRC Total Successful Attacks (Over Time Period)	PRC Defense Budget	PRC Annual Successful Attacks
5	735	1.71T	513
6	1.25k	1.79T	389
7	1.64k	1.87T	522
8	2.16k	1.96T	425
9	2.58k	2.06T	486
10	3.07k	2.16T	415
11	3.49k	2.26T	679
12	4.16k	2.37T	668
Final	4.83k	2.48T	713

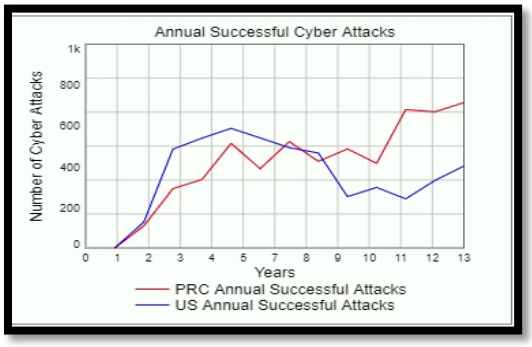
In this run of the simulation, the United States starts strong, partially due to their cyber power index being superior to that of the PRC. As the PRC continues to spend more on defense, approximately 7.3% of their GDP, their capabilities and successful attacks

increase. By year 8 and into year 9, China surpasses the U.S. in annual cyber-attacks and ultimately continues to dominate the sector. Table 1 shows the accumulation of Number of Annual Successful Attacks (US/PRC) comparative results from six total runs of the simulation.

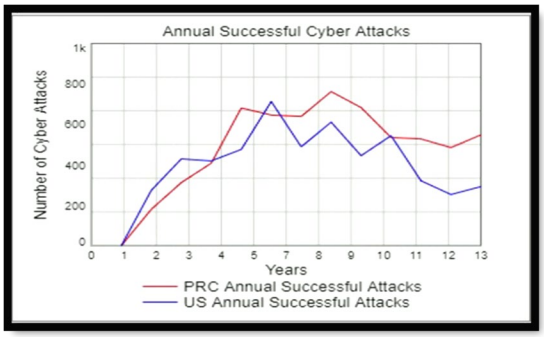
Table 1. Accumulation of Number of Annual Successful Attacks (U.S./PRC)

	Run 1 U.S. / PRC	**Run 2 U.S. / PRC**	**Run 3 U.S. / PRC**	**Run 4 U.S. / PRC**	**Run 5 U.S. / PRC**	**Run 6 U.S. / PRC**
Year 1	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
Year 2	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
Year 3	127 / 108	274 / 180	251 / 277	290 / 203	351 / 190	317 / 158
Year 4	612 / 399	703 / 492	769 / 639	694 / 467	779 / 488	679 / 435
Year 5	1.15k / 735	1.12k / 900	1.44k / 978	1.12k / 832	1.44k / 903	1.22k / 796
Year 6	1.74k / 1.25k	1.6k / 1.58k	2.21k / 1.28k	1.81k / 1.19k	2.1k / 1.33k	1.49k / 1.3k
Year 7	2.28k / 1.64k	2.31k / 2.23k	2.83k / 1.64k	2.14k / 1.43k	2.78k / 1.72k	1.76k / 1.84k
Year 8	2.77k / 2.16k	2.8k / 2.87k	3.56k / 1.91k	2.62k / 1.72k	3.34k / 2.24k	2.05k / 2.44k
Year 9	3.24k / 2.58k	3.41k / 3.63k	4.38k / 2.13k	3.08k / 1.93k	3.92k / 2.9k	2.46k / 3.07k
Year 10	3.49k / 3.07k	3.86k / 4.31k	5.2k / 2.53k	3.53k / 2.4k	4.51k / 3.41k	2.79k / 3.61k
Year 11	3.79k / 3.49k	4.4k / 4.85k	5.87k / 2.98k	3.87k / 2.78k	5.21k / 3.87k	3.16k / 4.1k
Year 12	4.03k / 4.16k	4.72k / 5.37k	6.36k / 3.33k	4.24k / 3.16k	5.87k / 4.25k	3.46k / 4.64k
Year 13	4.36k / 4.83k	4.97k / 5.86k	6.76k / 3.78k	4.85k / 3.34k	6.5k / 4.59k	3.89k / 5.11k

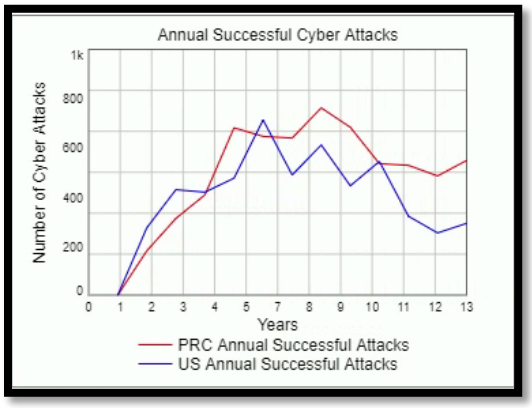
Figure 10. Runs 1 thru 6 for Number of Attacks in Each Year ISEE Systems, Stella Software



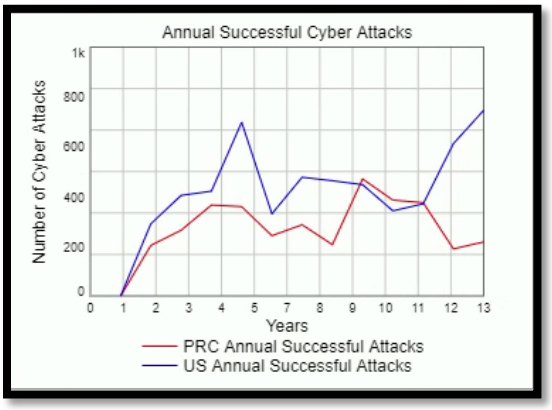
Run 1



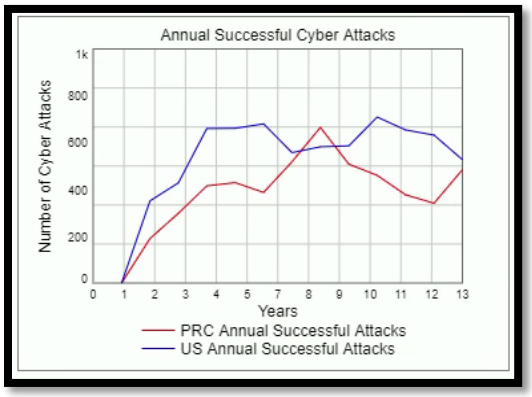
Run 2



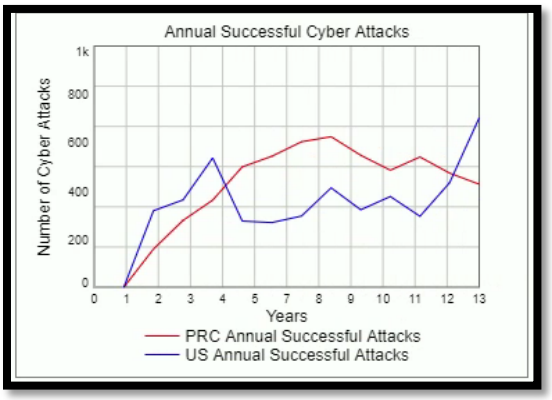
Run 3



Run 4



Run 5



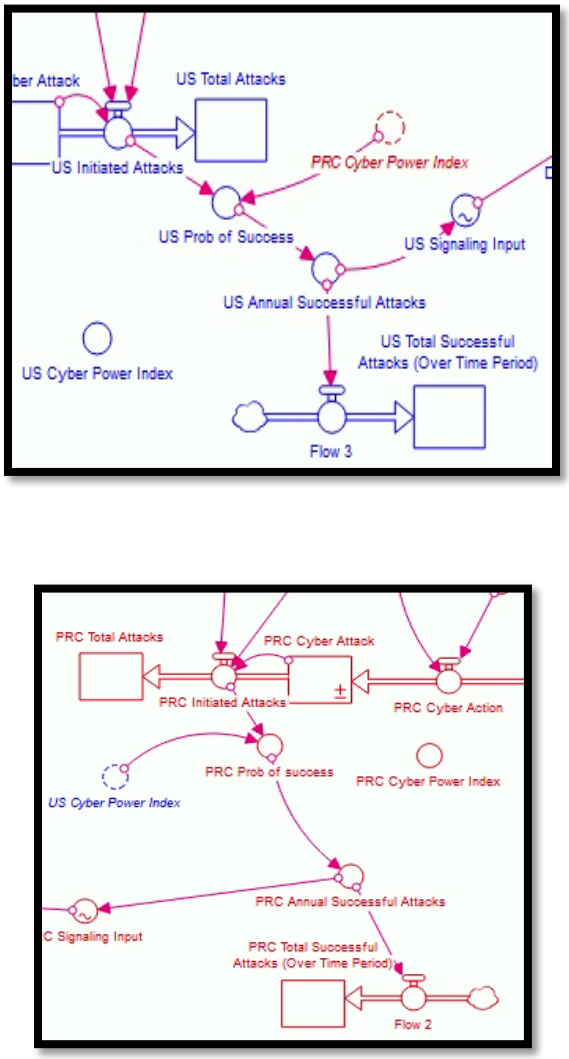
Run 6

Based on the results of the six simulations, results suggest that competition between the world's number one and number two cyber powers will result in back-and-forth cyber dominance. The U.S. had three simulations where they outperform the PRC and the PRC had three simulations where they outperformed the U.S. The histograms show the back and forth between the two countries. However, predictions from economists and cyber experts state that in the next few years, the PRC will consistently surpass the United States.[50]

Another set of simulations was run after exchanging the U.S. Cyber Power Index and the PRC Cyber Power Index converters as shown in Figure 11.

[50] Xie, "China's Economy Won't Overtake the U.S."

Figure 11. U.S. and PRC Power Index Model Change ISEE Systems, Stella Software

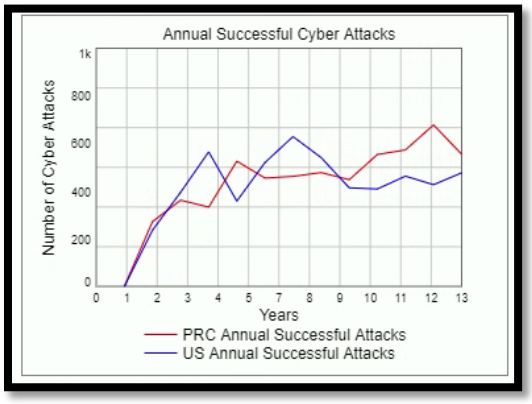


The change in the output was significant. In six runs, the U.S. (now with an inferior Power Index used to determine the probability of successA) lose in the majority of the runs. In six runs, the U.S. win only one time. Table 2 shows the runs with, again year 13 showing the final accumulation of cyber-attacks.

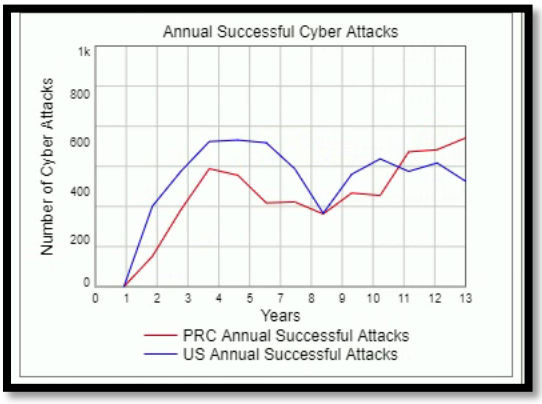
Table 2. Accumulation of Number of Annual Successful Attacks (U.S./PRC)

	Run 1 U.S. / PRC	**Run 2 U.S. / PRC**	**Run 3 U.S. / PRC**	**Run 4 U.S. / PRC**	**Run 5 U.S. / PRC**	**Run 6 U.S. / PRC**
Year 1	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
Year 2	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
Year 3	236 / 272	334 / 126	286 / 135	211 / 234	196 / 220	213 / 143
Year 4	631 / 634	813 / 445	604 / 448	514 / 636	426 / 534	644 / 412
Year 5	1.2k / 967	1.42k / 935	1.01k / 717	755 / 1.06k	557 / 859	1.08k / 675
Year 6	1.55k / 1.49k	2.03k / 1.4k	1.26k / 1.08k	1.09k / 1.59k	759 / 1.17k	1.34k / 1.19k
Year 7	2.07k / 1.95k	2.62k / 1.75k	1.47k / 1.3k	1.51k / 2.18k	897 / 1.46k	1.54k / 1.88k
Year 8	2.7k / 2.41k	3.11k / 2.1k	1.76k / 1.74k	1.96k / 2.94k	1.28k / 1.81k	1.97k / 2.32k
Year 9	3.24k / 2.89k	3.42k / 2.4k	1.97k / 2.2k	2.44k / 3.62k	1.72k / 2.12k	2.4k / 2.96k
Year 10	3.66k / 3.34k	3.88k / 2.79k	2.13k / 2.69k	3.05k / 4.11k	2.25k / 2.4k	2.74k / 3.7k
Year 11	4.07k / 3.89k	4.42k / 3.17k	2.38k / 3.07k	3.55k / 4.73k	2.68k / 2.99k	3.29k / 4.47k
Year 12	4.53k / 4.46k	4.89k / 3.73k	2.84k / 3.43k	4.12k / 5.55k	3.19k / 3.51k	3.94k / 5.23k
Year 13	4.96k / 5.14k	5.41k / 4.3k	3.26k / 3.93k	4.71k / 6.14k	3.58k / 4.08k	4.55k / 5.85k

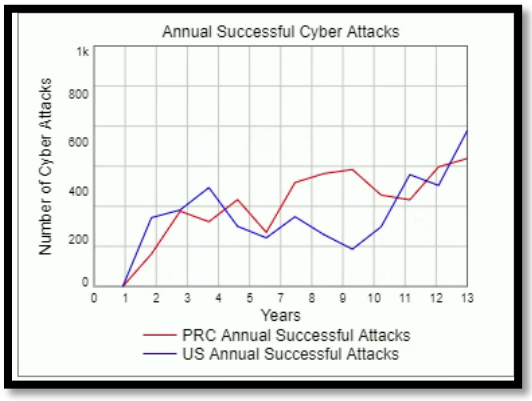
Figure 12. Runs 1–6 for Number of Attacks in Each Year—ISEE Systems, Stella Software



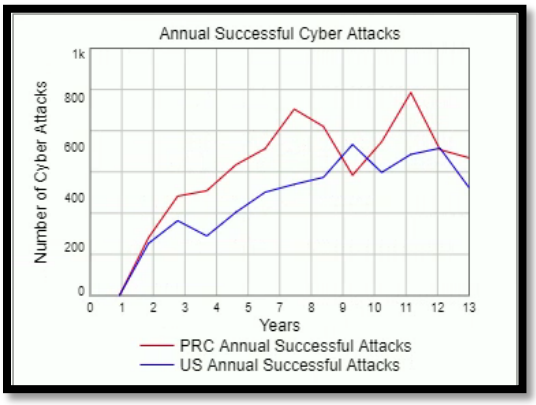
Run 1



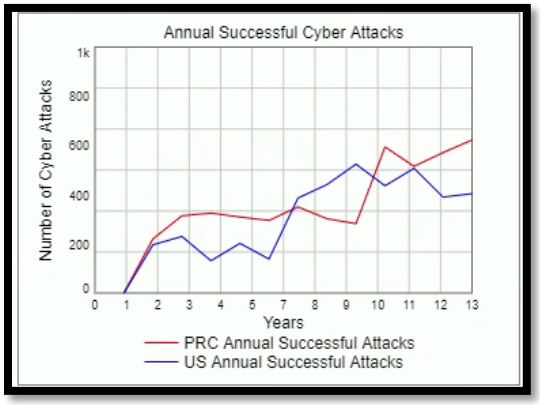
Run 2



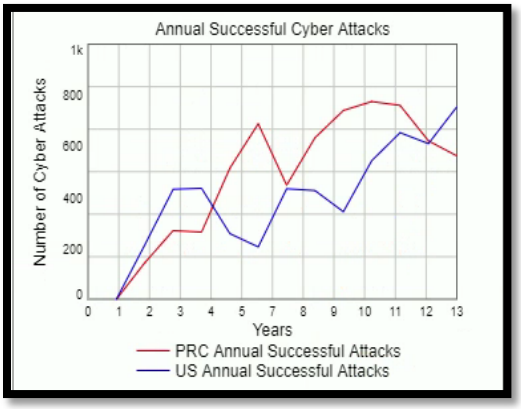
Run 3



Run 4



Run 5



Run 6

In another run of the simulation, when the interface was used to increase the U.S. Cyber Baseline % from 1% to 2%, the results showed the U.S. consistently ahead of the PRC in total successful attacks.

D. CONCLUSION

The HBNCPI 2020 data set provide a baseline of comparative values thru culminating indices of intent, capability, and power, which all coalesce to form the ranked power index of each country. These statistics along with economic forecasting provide the foundation of the model. Time perimeters for the entire model range from 2022 to 2035. The significance of this span is based on economic and power predictions suggesting that the PRC will surpass The U.S. in overall GDP, military strength, and cyber superiority by the year 2030.[51] The year 2035 is also the projection backstop of U.S. defense planning. The results yielded from the present base line settings substantiate this assumption thru the thirteen cycles of growth and interaction despite U.S. current and projected spending trends.

As indicated in the baseline simulation results, the U.S. and PRC (globally numbers one and two respectively in both GDP and Cyber Power Index,) are closely matched year to year in successful cyber-attacks. According to projections, China is estimated to reach an investment in their digital economy of $16 Trillion by 2035.[52] If these projections were applied to the US/PRC stock and flow model, China would reach a dominant status in defense budget cyber spending almost immediately compared to the growth rate currently projected for the U.S. The purpose of this chapter was to demonstrate that the answer is not to only investing more money into the cyber development because frankly, the PRC will outspend the U.S. regardless of the change of investment by the U.S. but rather begin to develop a new framework for how the DOD has to frame the problem and execute effectively and more importantly efficiently. The following chapter will look at the PLA's

[51] Ralph Jennings, "China's Economy Could Overtake U.S. Economy by 2030," VOA, January 4, 2022, https://www.voanews.com/a/chinas-economy-could-overtake-us-economy-by-2030/6380892.html.

[52] Huxley and Choong, "China's Cyber Power in a New Era."

SSF and the restructure that occurred in order to streamline the capabilities of the PRC's operations in the information environment.

III. THE PEOPLE'S LIBERATION ARMY'S STRATEGIC SUPPORT FORCE

A. HISTORY

2015 and into early 2016 was a momentous time for the Chinese communist party. After years of working in secrecy, they announced a complete reorganization structure of their entire military complex. Xi Jingping officially announced the initial operating capability of several operational theatres and the "reorganization also established a separate PLA Army headquarters element, and a service-level PLA Rocket Force (formerly the Second Artillery) on par with the PLA Army, Navy, and Air Force; and established an entirely novel entity known as the Strategic Support Force (SSF), which appears to be responsible for information warfare support to the PLA."[53]

During the 1991 Persian Gulf War, China, along with the rest of the world, watched the largest army in the Middle East and the third largest army in the world, get dismantled within days by the superiority of the United States. After this, the PRC realized that there was a gap in their development and technology versus their future adversary. Development, here, aligns towards technological capability to include both economic and military sectors. In its own individual analysis from the war, according to Costello and McReynolds, China's military planners changed their view on "the future of warfare as well as an understanding of its own vulnerabilities, prompting a decades-long upheaval in Chinese thinking on the strategic role of information in warfare."[54] The Chinese recognized a need to change not only their ways of thinking, , but also the roadblocks in their structure and organizations to the advancement of technological capabilities. According to the Cyber Strategy 2018, "China is eroding U.S. military overmatch and the Nation's economic

[53] Timothy R. Heath, Kristen Gunness, and Cortez A. Cooper, III, *The PLA and China's Rejuvenation: National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities* (Santa Monica, CA: RAND Corporation, 2016), 42, https://www.rand.org/pubs/research_reports/RR1402.html.

[54] John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, China Strategic Perspectives, No. 13 (Washington, DC: National Defense University, 2018), 7, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

vitality by persistently exfiltrating sensitive information from U.S. public and private sector institutions."[55]

B. TASK ORGANIZATION AND STRUCTURE

The PLA's SSF is responsible for executing the information warfare strategy for the PRC. The SSF was established in 2015 to "to centralize the PLA's strategic space, cyber, electronic, and psychological warfare missions, and capabilities. The SSF's creation highlights the PRC's understanding of the information domain as a strategic resource in modern warfare."[56] What is unique about the SSF versus the NSA/U.S. Cyber Command, is that the "PLA fundamentally supports the ruling party — generals and other top Chinese defense officials are recognized party members. The SSF is, as a result, an extension of The Communist Party of China."[57] In contrast, the NSA/U.S. Cyber Command support the current needs of the policies of the President and Congress, who ultimately answer to the people of the U.S. Furthermore, the U.S. holds itself to a certain moral standard and cares about their international public opinion, where the PRC does not necessarily need nor do not have the same constraints.[58]

There are two key components to the structure: the Space Systems Department (SSD) and the Network Systems Department (NSD), known as their cyber division. Segments of China's previous cyber organizations have merged under the SSF, the former 3PLA (cyber), and 4PLA (radar and computer attack) divisions.[59] Both capabilities are stored under one command structure and can streamline decision making and cut out the

---

[55] Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, 1.

[56] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China, 2021* (Washington, DC: Office of the Secretary of Defense, 2021), 64, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

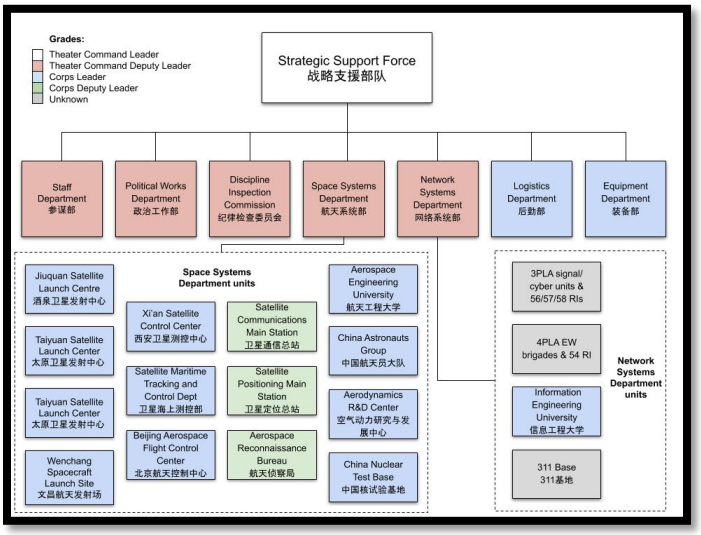
[57] Chris Bing, "How China's Cyber Command Is Being Built to Supersede Its U.S. Military Counterpart," CyberScoop, June 22, 2017, https://www.cyberscoop.com/china-ssf-cyber-command-strategic-support-force-pla-nsa-dod/.

[58] Anthony H. Cordesman, *Making America Great? Global Perceptions of China, Russia, and the United States: The International Scorecard* (Washington, DC: Center for Strategic & International Studies, 2021), https://www.csis.org/analysis/making-america-great-global-perceptions-china-russia-and-united-states-international.

[59] Costello and McReynolds, *China's Strategic Support Force*, 26.

bureaucracy as it was intended to do. Chris Bing describes the SSF to be the counter to the CYBERCOM and in theory have the capabilities of the NSA, Army, Air Force, Homeland Security NASA, State Department and CYBERCOM underneath one command structure. He says, "if you combined all of those government entities and added companies like Intel, Boeing and Google to the mix, then you would come close to how the SSF is built to operate."[60] Figure 13 shows the known task organization of the SSF. The SSF format and structure counters the current U.S. construct in that multiple commands and government agencies have capabilities and resources that are classified, compartmentalized, and can rarely be shared or even talked about. The SSF seeks to streamline that process and utilize its full capabilities.

Figure 13. Strategic Support Force Task Organization[61]



The SSF is attempting to streamline information operations for the Chinese. Costello and McReynolds state, "For strategic-level information operations, this operational requirement would have demanded unprecedented coordination between

60 Bing, "How China's Cyber Command Is Being Built."

61 Source: Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019," *China Brief* 19, no. 10 (May 29, 2019), https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

General Staff Department, General Armament Department, General Political Department, and military region units across multiple echelons. The creation of the SSF and the theater commands has simplified this process dramatically by organizing both China's conventional and information warfare units into permanent operational groupings that are designed to transition seamlessly into wartime command structures."[62] The Chinese outlook to information resulted in one organization housing all the capabilities, thus eliminating the bureaucracy and coordination across multiple departments and government agencies.

Under this new headquarters, referring to Figure 13, you can see in the construct there are multiple different units with different capabilities. This is partially due to how the PLA view deterrence. Chinese deterrence philosophy has evolved alongside its modernization effort. To deter an adversary, the capability or the messaging needs to transmit to the adversary two important things: capabilities and willpower.[63] In order to be successful in your deterrent capabilities, you must demonstrate the willpower to use your capabilities or make your adversary believe you will use it. If successful, it will have a psychological impact on the opponent and manipulate the decision-making process.

The SSF will be responsible for information deterrence with two important points: "The first, more operational, aspect is the ability to influence the flow of information on the battlefield. The side that can better exploit information is seen as exercising information deterrence. The second (and more strategic) aspect is the ability to influence decisionmakers and the public of one's own country, an opponent's public, and third parties. This includes not only affecting the flow of information, but also having the ability to provide one's own information and narrative."[64] With information deterrence being as important as conventional deterrence, the PLA have organized exercises to not only raise the technological knowledge of the force, but also to fight with integrated systems. As a result, according to Costello, the "SSF's cyber corps approach the cyber domain in a much

[62] Costello and McReynolds, *China's Strategic Support Force*, 12..

[63] Heath, Gunness, and Cooper, III, *The PLA and China's Rejuvenation*, 45.

[64] Heath, Gunness, and Cooper, III, 46.

more comprehensive way, reflecting a highly integrated approach to information operations that actualizes critical concepts from PLA strategic and doctrinal approaches.'[65]

1. Network Systems Department

The Space Systems Department (SSD) and the Network Systems Department (NSD), two theatre level commands, fall under the SSF Task Organization. The NSD is responsible to the PRC government for all things related to information operations. This includes but not limited to, technical reconnaissance, electronic warfare, cyber warfare, and cyber operations.[66] According to the Office of Secretary Defense report, the intent to place all these capabilities under one organization is two-fold. The first is "to remedy the operational coordination challenges that hindered information sharing under the PLA's pre-reform organizational structure."[67] The second is that "The integration of cyber and EW elements under one organization is a crucial step towards realizing the operational concept of integrated network and electronic warfare that the PLA has envisioned since the early 2000s."[68]

The NSD can execute all three types of warfare against adversaries under one command. The three-warfare concept is a political warfare that the Chinese use legal warfare, psychological warfare, and media warfare (public opinion) to erode at an adversaries will or credibility. According to Anthony Cordesman, "China views the cyberspace domain as a platform providing opportunities for influence operations, and the PLA likely seeks to use online influence activities to support its overall 'Three Warfare' concept and to undermine an adversary's resolve in a contingency or conflict."[69]

---

[65] Elsa B. Kania and John K. Costello, "The Strategic Support Force and the Future of Chinese Information Operations," *Cyber Defense Review* 3, no. 1 (Spring 2018): 105–21, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1589125/the-strategic-support-force-and-the-future-of-chinese-information-operations/.

[66] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China, 2021*, 65.

[67] Office of the Secretary of Defense, 65.

[68] Office of the Secretary of Defense, 65.

[69] Cordesman, *Chinese Strategy and Military Forces in 2021*, 43.

The PRC have also evolved their view of what information is and developed the NSD to attack this view within cyberspace. According to Costello and Kania, they state that the PLA may be expanding their definition of cyberspace and "including all aspects of information warfare, such that the concept is effectively synonymous with the information domain."[70] Accordingly, viewing cyberspace operations as one entity and including the information domain will streamline operations and acquisition of new technology and products. They further state that although the Strategic Support Force has housed a multitude of the PLA's capability, it seems that it is primarily for offensive purposes and the Cyberspace Administration of China, and the Ministry of Public Security are responsible for cyber defense and protection of critical infrastructure.

2. Military-Civil Fusion

Military-Civilian Fusion (MCF) is a concept which is tasked by the PRC Government to its economic and military sectors. The central theme of it is that the military will "take advantage of dual-use technological advances and leveraging civilian talent."[71] There are six interrelated efforts from the MCF development strategy:

- fusing China's defense industrial base and its civilian technology and industrial base;
- integrating and leveraging science and technology innovations across military and civilian sectors;
- cultivating talent and blending military and civilian expertise and knowledge;
- building military requirements into civilian infrastructure and leveraging civilian construction for military purposes;
- leveraging civilian service and logistics capabilities for military purposes; and,
- expanding and deepening China's national defense mobilization system to include all relevant aspects of its society and economy for use in competition and war.[72]

[70] Kania and Costello, "The Strategic Support Force," 111–12.

[71] Kania and Costello, 110.

[72] Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China, 2021*, IV–V.

With this strategy, the PRC seeks to further drive innovation and development of dual-use technology and integrate them into both military and civilian sectors. In 2017, the PRC reorganized the construct surrounding these new and developing technologies and how they are applied to national and operational strategies and concepts.[73] For example, Chinese universities now directly support the SSF.

With the MCF strategy, the SSF has control over two distinct universities: Information Engineering University and the Space Engineering University, along with two research institutes. The two universities are tied in so much to the SSF that each university is listed under the task organization of the two theatre level commands (reference Figure 13). The Information Engineering University is a very capable and influential military academy. The Australian Strategic Policy Institute place the University in a "very high-risk category" due to its "record of training signals intelligence and political warfare officers and carry out offensive cyber operations."[74] This university is known for several things. It is primarily known for "research and training on hacking, cryptography, signals processing, surveying, and mapping, and navigation technology. Since absorbing the PLA Foreign Languages University, it now serves as one of the most important language schools for Chinese military intelligence officers, describing itself as a 'whole-military foreign languages training base for individuals going abroad."[75] The University supplies a direct link of education and technological development and feeds directly into the NSD of the SSF.

[73] Office of the Secretary of Defense, 60.

[74] "Information Engineering University," Chinese Defence Universities Tracker, May 13, 2021, https://unitracker.aspi.org.au/universities/information-engineering-university-2.

[75] Australian Strategic Policy Institute.

C. THE SSF THREAT

The United States is currently ranked number one in cyber capability according to the HBNCPI of 2020. The U.S. may possess exquisite capabilities that may be better than the PRCs, but the PRC can resolve that by utilizing mass and just mass-producing attacks. Table 3 shows a potential hypothetical to attempt to demonstrate the capacity that the PLA could possess. By taking the number of cyber command employees and obtaining a rough percentage that is from the total workforce of the DOD, we can then apply the same percentage to the total workforce of the PLA military to determine a rough estimate of the SSF numbers. Understand that this is an assumption that the percentage of workers will be the same, this percentage does not hold true for the PLA, in fact a likely assumption is that it is greater.

Table 3. U.S. Cyber Workforce

	Number of Total Personnel (2020)	Number of Cyber Workforce (CYBERCOM, ARCYBER, 10th FLEET, MARFORCYBER, 16th AF)	% of the Service
CYBERCOM	-	5,000[76]	
Army	481,254[77]	16,500[78]	3.42
Navy	341,996[79]	19,000[80]	5.56
Marines	180,958[81]	800[82]	0.445
Air Force	329,614[83]	44,000[84]	13.3
Total	1,333,822	85,300	6.39

76 "Command History," U.S. Cyber Command, accessed October 28, 2022, https://www.cybercom.mil/About/History/.

77 "U.S. Military Force Numbers, by Service Branch and Reserve Component 2020," Statista, accessed November 16, 2022, https://www.statista.com/statistics/232330/us-military-force-numbers-by-service-branch-and-reserve-component/.

78 "About Army Cyber," U.S. Army Cyber Command, accessed October 5, 2022, https://www.arcyber.army.mil/About/About-Army-Cyber/.

79 Statista Research Department, "U.S. Military Force Numbers, by Service Branch and Reserve Component 2020."

80 "Command Description," U.S. Fleet Cyber Command/U.S. 10th Fleet, accessed October 5, 2022, https://www.fcc.navy.mil/.

81 Statista Research Department, "U.S. Military Force Numbers, by Service Branch and Reserve Component 2020."

82 H.R., *Operating in the Digital Domain: Organizing the Military Departments for Cyber Operation: Hearing Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the Committee on Armed Services House of Representatives*, House of Representatives, 111th Cong. 2, 2009, 38, https://www.govinfo.gov/content/pkg/CHRG-111hhrg62398/pdf/CHRG-111hhrg62398.pdf.

83 Statista Research Department, "U.S. Military Force Numbers, by Service Branch and Reserve Component 2020."

84 Tobias Naegele, "16th Air Force Is Fully Up and Running," *Air & Space Forces Magazine*, July 16, 2020, https://www.airandspaceforces.com/16th-air-force-is-fully-up-and-running/.

Table 4. PLA Cyber Workforce

	% of the Service	Number of Military Personnel	Number of Cyber Workforce
PLA SSF	6.39	2,200,000[85]	140,580

The assumption that is made in this example is that the PLA's SSF has the same percentage as the U.S. in total workforce that works in cyber. According to the calculation, the PLA SSF is almost double the capacity of the U.S. cyber effort. These numbers are not broken down by actual cyber mission teams or individuals who can conduct missions. These include support staff, contractors, and other employees that support the overall commands. However, viewing how much emphasis on strategy, time, and money into the information sector and research, development, and acquisition, it is a safe assumption that this percentage is greater than only 6%, meaning the PLA will have more cyber actors than the CYBERCOM.

D. CHINESE CYBER ATTACKS & THE OBAMA-XI AGREEMENT

Valeriano, Maness, and Jensen, in their research studying adversarial cyber operations, created and designed a table of Chinese cyber-attacks against various targets, some of which include the U.S., the Philippines, Taiwan, and Vietnam. Their data set dates to 2001 and continues to present day operations. The information and data collected are open source and unclassified. Looking at the range of United States targets, the Chinese hacked the White House, State Department, Senators, Lockheed Martin, and Google to name a few. The Chinese attacks on a U.S. target are listed in Table 5.

[85] Sin "Military Size by Country 2022," World Population Review, accessed November 16, 2022, https://worldpopulationreview.com/country-rankings/military-size-by-country.

Table 5. China Offensive Cyber Operations[86]

Name	Year	Target / Description
Hainan Island Incident	4/29/2001	Retaliation for the death of Chinese fighter pilot Wang Wei, after collision with U.S. spy plane. Secondly, to register displeasure at the recent U.S.—Taiwan arms deal.
Titan Rain	9/1/2003	Information theft campaign against the DOD and defense contractors
State Dept theft	5/28/2006	Information probe against loosely defended State Dept networks to seek information about Southeast Asian and Pacific Affairs.
Shady RAT_A	8/1/2006	Multiple targeted data theft campaign that included the U.S. government and several corporations
Fred Wolf espionage	8/1/2006	Access of militantly intelligence and sensitive information from ongoing investigations regarding human rights cases.
Commerce disable	10/1/2006	Retaliation for the cancellation in June of a $1.3m USD plan to purchase Lenovo computer systems due to cyber security concerns.
Naval War College disable	12/1/2006	US Naval strategic studies group brought offline
750,000 American zombies	3/1/2007	Widespread DDoS strikes against various targets vital to the U.S. economy.
GhostNet_A	5/27/2007	Data breach of state secretive information from several government networks
Commerce Sec hack	12/1/2007	Data breaches of several networks containing sensitive information
2008 Campaign hack	8/1/2008	To assess campaign positions on China and the evolution of potential future U.S. policy
Hikit_A	9/1/2008	Axiom group launches 6-year information theft campaign against multiple countries including U.S., Taiwan, and Japan
Byzantine series	10/30/2008	Data theft campaign against the oil and gas sectors, targets also included lawyers pursing claims against Chinese exporters and energy companies
FAA hack	2/4/2009	Chinese hack steals sensitive info from the FAA
Senator Nelson theft	3/1/2009	To access foreign policy information from a prominent Senator's network

[86] Adapted from Ryan C. Maness et al., "The Dyadic Cyber Incident and Campaign Data (DCID), Versions 1, 1.1, 1.5, and 2.0," Cyber Conflict Database, accessed November 2, 2022, https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset.

Name	Year	Target / Description
Lockheed F-35 plans stolen	3/29/2009	Data breach on Lockheed Martin and its F-35 fighter jet plans
Aurora	6/1/2009	Google hacked and breached by the Chinese PLA, Tech giant comes forward and admits; a first from the private sector.
Night Dragon	11/1/2009	Theft of oil and gas field production systems, field exploration and bidding processes for leases.
Commerce theft	11/1/2009	Data breach of the Commerce department, sensitive information stolen
Htran_A	1/1/2010	Advanced listening device root kit able to capture corporate secrets in unsecured networks
Dancing Panda	4/1/2010	Top U.S. national security officials' emails hacked and read
FDIC Hack	10/1/2010	Data breach of the FDIC, theft of sensitive and personal information
Intellectual Property Hack	11/3/2010	APT3 targets U.S. financial and manufacturing sectors for intellectual property
Energy Dept hack	2/1/2011	Energy Dept hacked multiple times due to outdated software and patches
Pentagon Raid	3/1/2011	Information theft campaign in the unsecured networks of the DOD
Operation Beebus/APT 10	4/12/2011	China hacks several U.S. defense contractors and steals drone technology
White House theft	11/7/2011	Signaling campaign against White House networks
Mofang	2/4/2012	Mofang RAT targets and steals information from energy companies
Penn State Engineering breach	9/1/2012	Personal and sensitive information stolen from the Penn State College of Engineering network
Wen Jiabao Retaliation	10/26/2012	Signaling data breach on the New York Times and Washington Post for publishing negative stories about then-President Wen Jiabao
Iron Tiger/APT 31	1/15/2013	Iron Tiger sophisticated APT information theft on U.S. military and defense contractors
Black Coffee/ APT 17	4/1/2013	APT17 group hacks Microsoft Tech Net forum to trick users into downloading the backdoor
UConn Engineering Hack	9/24/2013	Chinese hack steals University of Connecticut's Engineering school's personnel and research data
CloudHopper	1/1/2014	APT 10 private sector breach
Operation SnowMan	2/1/2014	Chinese hackers infiltrate VVW page to access personal info of active U.S. military personnel

Name	Year	Target / Description
Register.com breach	3/1/2014	Register.com, which manages more than 1.4 million websites for businesses worldwide, steals network and employee passwords
OPM Hack	3/15/2014	OPM hack, revealed in spring of 2015, steals personal information of 20 million people
Premera Blue Cross Breach	5/5/2014	State-sponsored Chinese data breach group steals personal information of 11 million Premera customers
UCLA Health system breach	9/1/2014	UCLA health system breach by state-sponsored Chinese group, 4.5 million personal information stolen
DHS employee hack	11/6/2014	25,000 DHS employees' information stolen from OPM, this preceded the larger April 2015 OPM hack
USPS breach	11/8/2014	Personal information of 800,000 USPS employees compromised, including Postmaster General
Anthem Breach	12/10/2014	Black Vine hacker group that does cyber-intelligence work for China steals sensitive information from health insurance giant Anthem
GitHub Hack	3/26/2015	China throttles GitHub site to get rid of all anti-Chinese content on the site, Great Cannon
United Airlines breach *	**5/25/2015**	**Chinese APT group hacks U.S. airline United**
EvilNugget	1/1/2017	Chinese state-sponsored hackers were revealed to have targeted multiple U.S. cancer institutes to take information relating to cutting edge cancer research.
Dispute Portal Exploit	3/1/2017	150 million customer records compromised: birth dates social security numbers
Submarine University Hacks	4/1/2017	steal research on submarine technologies.
Satellite and Telecom Company Hack	6/19/2017	satellite, telecom, and defense organizations
Navy Personnel Data Hack	11/1/2017	APT 10 DIB breach
Sea Dragon	1/1/2018	CSIS: Chinese Hackers attack a contractor working for the Naval Undersea Warfare Center for military equipment
China 2FA Bypass	1/1/2018	A Chinese state-sponsored operation attacked government entities and managed service providers by bypassing the two-factor authentication used by their targets.
Failed Exams-Lookback	7/19/2019	State-sponsored Chinese hackers conducted a spear-phishing campaign against employees of three major U.S. utility companies

Name	Year	Target / Description
Wicked Spider Telecom Hack	9/15/2019	"In August 2019 and August 2020, a federal grand jury in Washington, D.C., returned two separate indictments charging five computer hackers, all of whom were residents and nationals of the People's Republic of China (PRC), with computer intrusions affecting over 100 victim companies in the United States and abroad, including software development companies, computer hardware manufacturers, telecommunications providers, social media companies, video game companies, non-profit organizations, universities, think tanks, and foreign governments, as well as pro-democracy politicians and activists in Hong Kong….facilitated the theft of source code, software code signing certificates, customer account data, and valuable business information. These intrusions also facilitated the defendants' other criminal schemes, including ransomware and "crypto-jacking" schemes, the latter of which refers to the group's unauthorized use of victim computers to "mine" cryptocurrency."
Chinese Moonlighting	9/15/2019	Same as above
Chinese Multiple Exploit	1/20/2020	APT41 attempts to breach U.S. tech sector
BioTech Firm Attacks	1/27/2020	CSIS: May 2020. U.S. officials accused hackers linked to the Chinese government of attempting to steal U.S. research into a coronavirus vaccine
Cybersecurity Spoof	3/1/2020	Attempt to breach U.S. political campaign posing as cybersecurity company
Posing Security	3/1/2020	Attempt to breach international companies posing as cybersecurity company
Exchange Hack Webshell	1/5/2021	Microsoft Exchange Server Hack
*** Last attack before the Sept 2015 agreement.**		

In September 2015, due to the OPM hack and the information stolen of over 20million people, President Barack Obama and President Xi formed an agreement on a wide range of topics. Most importantly was cybersecurity. This meeting established rules and lateral limits between the Chinese and the U.S. Table 5 further shows there was significant activity against the U.S. Government and private corporations and after the

2015 agreements, those have seemed to taper off. The memorandum of agreement between both Presidents established a set of rules circulating cyber operations and what would be considered off limits. According to the Obama White House archives, below is what both Presidents agreed to under the category of cybersecurity:

- The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate.
- The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
- Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic.
- The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community, and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests.

> Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015 and will occur twice per year thereafter.[87]

The biggest agreement between the two countries was the bilateral agreement of "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[88] It is important to re-iterate the significant drop off in "unclassified" known activity after 2015.

The important thing to note about the Obama & Xi agreement is that it is explicitly an agreement between the U.S. and China. It is not an agreement with U.S. allies or its partners. It solely refers to stopping the economic and intellectual theft from the U.S. and its corporations but does not bring into account economic and intellectual theft from the U.S. allies. Although the PRC maybe deterred from stealing from U.S. entities, it may not be deterred from attacking and stealing from others within the INDO-PACOM aor. The U.S. must be willing to step in and assist/protect its allies, in order to allow the integrated deterrence strategy to actually take effect.[89]

E. CONCLUSION

The SSF is an all-encompassing organization designed specifically to target, manipulate, and exploit in the information domain. Currently, the U.S. still has the technological and capability advantage, however, China has established the infrastructure and streamlined process to move faster and ultimately create domain supremacy for its forces within a given area. China saw that placing all necessary capabilities to fight and win in the information domain was necessary in order to streamline operations. For the Chinese, cyberspace operations and information operations are viewed one in the same.

---

[87] White House, "FACT SHEET: President Xi Jinping's State Visit to the United States," The White House – President Barack Obama, September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

[88] White House.

[89] Lopez, "Defense Secretary Says 'Integrated Deterrence' Is Cornerstone of U.S. Defense."

The U.S. has an issue with over-compartmentalizing and over classifying information. This makes sharing information/intelligence or capabilities next to impossible in a timely manner. Another inhibitor is whether an organization has the correct authorities to conduct a certain type of operations as dictated under Title 10 and Title 50. If they do not have the proper authorities, then they must push the operation to the correct organization or abort the mission and potentially lose the window of opportunity. To counter the emerging threat, the U.S. must look at the current cyber titles and authorities and potentially see what permissions can be pushed to Task Force commanders to operate faster than the adversary in order to maintain a competitive edge.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. UNITED STATES STRUCTURAL LIMITATIONS

With the rise of the international influence, military capability, particularly within cyber, the Chinese have placed the U.S. in a Thucydides paradox potentially dethroning the current World Order. After WWII, China began its quest to strengthen and increase its influence and ultimately overthrow the U.S. hegemony, and this is shown through Power Transition theory and international philosophies.[90] The rift between these two countries is continuing to grow through advances of technology "poised to retool economies, and transform militaries."[91] Through advances in digital technology and the incorporation of cyber, the fear of escalation through retaliatory actions within the cyber domain remains a significant point of concern to political officials in Congress, though research suggests that escalation through cyber alone is highly unlikely.[92] This conjecture is partially based on biased assumptions of kinetic options and nuclear deterrence philosophy; however, the premise still anchors the escalation perspective as a topic of concern. According to Libicki, the probable begetting of retaliatory action from using a cyber weapon is extremely small, with no historical suggestions to hinting to a plausible scenario of grand scale reprisal.[93] This concern is an aspect that drives some of the hesitant approaches of military leaders avoiding a domain that is new and uncertain at the fear of making substantial mistakes and the personal or profession fallout that may result.[94]

Cyber operations have caused both the DOD and intelligence communities to argue who should be legally responsible to address the new emerging threats. The acting agency

---

[90] Woosang Kim and Scott Gates, "Power Transition Theory and the Rise of China," *International Area Studies Review* 18, no. 3 (2015): 219–26, https://doi.org/10.1177/2233865915598545.

[91] Joseph R. Biden, Jr., *National Security Strategy* (Washington, DC: White House, 2022), 32, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[92] Martin C. Libicki, "Correlations between Cyberspace Attacks and Kinetic Attacks," in *2020 12th International Conference on Cyber Conflict (CyCon)* (2020 12th International Conference on Cyber Conflict (CyCon), Estonia: IEEE, 2020), 199–213, https://doi.org/10.23919/CyCon49761.2020.9131731.

[93] Libicki.

[94] Catherine Lotrionte, "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations under International Law," *Cyber Defense Review* 3, no. 2 (2018): 73–114, https://www.jstor.org/stable/26491225.

must now be able to operate within cyber space, maintain the initiative, keep the equilibrium, and the status quo. Nevertheless, the growing tensions of strategic competition, specifically within cyber, have led Congress to evaluate standing policy, and evolved the cyber authority framework with the implementation of the Defend Forward Strategy. This would eventually permit the DOD to lean forward in the competition continuum conducting preventative rather than reactive measures within the domain.[95]

This chapter will first, discuss some of the historic legal proclivities attributed to the anxious behavior amongst decision makers and cyber operations. Second, it will discuss how these regulatory restrictions patterned the behavior of leadership, and lessons learned from this behavior could also serve future leaders of the DOD as guidelines to move forward towards acceptance. Third, it will provide potential suggestions on implementation and rules of engagement that will allow for leaders to be more adept in making informed, timely, equitable, and confident decisions. Finally, it will address how these actions force a need from top military leaders and policy makers to pursue appropriate budgeting to compete within the space.

U.S. policy, authorities, and permissions for conducting cyber operations have evolved since the creation of CYBERCOM in 2008. Beginning in 2019, Congress expanded the authorities of the DOD, specifically CYBERCOM, that permit extensive flexibility with varied degrees of oversight to execute cyber effects as is applied to the Defend Forward Strategy.[96] The National Defense Authorization Acts (NDAA) for Fiscal Years 2019 and 2020 redefined how the DOD shall conduct operations in the cyber domain which continued to shape boundaries of procedure. It defined cyber operations to be consistent with what is called Traditional Military Activities (TMA) and scoped proportionally for oversight through Congress pending the nature of the effects and what risks might be associated with use at the strategic level.[97] The 2019 NDAA further scaled

95 Authorities Concerning Military Cyber Operations, 10 U.S.C. § 394 (2022).

96 Angus King and Mike Gallagher, *Cyberspace Solarium Commission Report* (Washington, DC: Cyberspace Solarium Commission, 2020), https://www.solarium.gov/report.

97 John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. no. 115–232, 132 Stat. 1636 (2018). https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

the definitions of what it meant to be clandestine versus covert, and specifically which departments will be more effective as the lead in the fight against foreign/domestic cyber adversaries.[98] Covert, in this context, meaning "the role of the U.S. Government will not be apparent or acknowledged publicly" and where clandestine activity in cyberspace is considered a traditional military activity and "the role of the U.S. Government will not be apparent or acknowledged publicly."[99] Covert action is particularly important, especially in cyber, because it can prevent the crossing of the armed conflict threshold, where as an overt action may break the threshold.[100]

The common perception of Title 50 is that it is refers to the intelligence community and those entities conducting intelligence operations. The main reason for the intelligence community operating under Title 50, was to protect the operations and intelligence collected against the Soviet Union, but more importantly tread under the threshold of mutually assured destruction.[101] Today, operating under the threshold of armed conflict, Congress places importance surrounding foreign intelligence, and the CIA became the main consumer of Title 50 privileges. Under Executive Order 12333, during the Reagan administration, these actions became known to Congress as "special activities."[102] During this time, military operations were scoped and limited by Title 50 authorities and were only authorized in designated areas of hostility, times of declared war, or when deemed appropriate through the War Powers Resolution 1973. The War Powers Resolution Act of 1973 authorizes the President to initiate or escalate military actions abroad.[103]

---

98 John S. McCain National Defense Authorization Act for Fiscal Year 2019.

99 Presidential Approval and Reporting of Covert Actions, 50 U.S.C. § 3093 (2022).

100 J. Robert Kane, "Covert Action, Military Operations and the DOD–CIA Debate," *Real Clear Defense*, August 9, 2018, https://www.realcleardefense.com/articles/2018/08/09/covert_action_military_operations_and_the_dodcia_debate_113701.html.

101 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020).

102 White House, *Executive Order 12333- United States Intelligence Activities*, 1981, https://dodsioo.defense.gov/Library/EO-12333/.

103 "War Powers Resolution of 1973," Richard Nixon Presidential Library and Museum, July 27, 2021, https://www.nixonlibrary.gov/news/war-powers-resolution-1973; Laura B. West, "The Rise of the 'Fifth Fight' in Cyberspace: A New Legal Framework and Implications for Great Power Competition," *Military Law Review* 229, no. 3 (2021), https://tjaglcs.army.mil/mlr/the-rise-of-the-fifth-fight-in-cyberspace-a-new-legal-framework-and-implications-for-great-power-competition.

Throughout the evolution of Titles 10/50, there is debate as to where each of the U.S. Government agencies fit regarding the execution of authority and the oversight that is inherent with each.[104] Oversight measures increased due to the growing prevalence of abuses in covert special activities, therefore prompting Congress to intervene at various points over the decades. For example, the 1974 Hughes-Ryan Amendment instituted the presidential findings clause to further regulate and restrict how each of the agencies conducted covert operations.[105] This amendment was followed by the Church Committee of 1975 that was formed to investigate substantial abuses by multiple agencies within the intelligence community involving covert action programs.[106] The DOD also had its fair share of controversy with covert operations when Reagan's Iran Contra rose to infamy, which prompted the Intelligence Authorization Act of 1991 and the initial act of Congress defining TMA. TMA is defined as military routine support and its relation to covert and clandestine operations.[107] This Act furthered the legal groundwork by refining the roles of covert and clandestine operations as they are applied to military operations, which was said to provide flexibility to commanders but also limiting them in areas not traditional with evolving warfare methods of the day. This muddled soup of legal indiscretions gives pause to military leaders and decision makers when weighing options of capabilities while managing operations.

Despite clouded historical statute and oversight debates, the persistent nature of emergent technology and the importance of anonymity, forced the need to revise current process, specifically in conjunction with CYBERCOM's Defend Forward Strategy. U.S. adversaries have grown and identified the value of cyber operations and related technology

104 Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action," *Harvard National Security Journal* 3 (2011): 85–142, https://www.soc.mil/528th/PDFs/Title10Title50.pdf.

105 "Congressional Precedents and Powers," Organization of the Congress: Final Report of the Joint Committee on the Organization of Congress, December 1993, https://archives-democrats-rules.house.gov/Archives/jcoc2ar.htm.

106 Timothy B. Lee, "In the 1970s, Congress Investigated Intelligence Abuses. Time to Do It Again?," *Washington Post*, June 27, 2013, sec. Economic Policy, https://www.washingtonpost.com/news/wonk/wp/2013/06/27/in-the-1970s-congress-investigated-intelligence-abuses-time-to-do-it-again/.

107 DeVine, *Covert Action and Clandestine Activities of the Intelligence Community*.

against peer or stronger opponents.[108] Due to cyber operations having no defined boarders, it is imperative that U.S. forces operate with a sense of anonymity and deniability.

The debates have now turned to more of a discussion of convergence, whereas the overlap of intelligence and speed in which cyber operations can be executed, is fusing both Intelligence and military communities to realign to effectively compete in the domain.[109] This convergence across department lines became more prevalent in the post 9/11 aftermath with the growing demand of blending missions and capabilities across each agency.[110] The cyber domain remains a place where ambiguity and concealment are essential to remain competitive.[111] Rovner, who served as a scholar for both the National Security Agency and CYBERCOM, states, "the intelligence contest is an effort to steal secrets and exploit them for relative advantage."[112] His perspective from operating under both Title 10/50 perspectives, could construe that the comment certainly laments the cyber domain as a mainstay of the intelligence community. As stated in the Harvard National Security Journal, Title 10/50 "are not mutually exclusive, but mutually reinforcing."[113] Even though this distinction should be understood by intelligence and military leaders, the constant pressure of maneuvering for positions of power are still prevalent, and though the intelligence community does not hold a monopoly on Title 50, it became a common practice of avoidance by some military leaders who would choose more conventional methods over political and costly time constraints to achieve effects.[114] This dilemma creates additional barriers in an era of "whole of government" approach, where integration

108 Arquilla, *Bitskrieg*, 33.

109 West, "The Rise of the 'Fifth Fight' in Cyberspace."

110 Jennifer D. Kibbe, "CIA/SOF Convergence and Congressional Oversight," *Intelligence and National Security* 0, no. 0 (August 7, 2022): 1–17, https://doi.org/10.1080/02684527.2022.2104015.

111 Jon R. Lindsay, "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem," *Intelligence and National Security* 36, no. 2 (2021): 260–78, https://doi.org/10.1080/02684527.2020.1840746.

112 Joshua Rovner, "The Intelligence Contest in Cyberspace," *Lawfare* (blog), March 26, 2020, https://www.lawfareblog.com/intelligence-contest-cyberspace.

113 Wall, "Demystifying the Title 10-Title 50 Debate," 58.

114 John Donnelly and Gopal Ratnam, "US Is Woefully Unprepared for Cyber-Warfare," S&P Global Market Intelligence, June 26, 2019, https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/us-is-woefully-unprepared-for-cyber-warfare-52560026.

and interoperability are key tenants to accessing the entirety of a state's capabilities and capacity.[115]

Along with Congress's clarification of roles, the terminology brought just as many questions as well as reservations for implementation. Another debate revolves around what signifies what TMA are and how they apply to cyber operations, more specifically covert cyber operations. Historically, the need of oversight and executive level permissions for covert operations to prevent escalatory complications, attribution, or plausible deniability is required. Defined in section 1632 of FY 2019 NDAA, certain military operations are exempt from prior notification, pending the stipulated need, which has made conducting military operations a more alluring route of execution.[116] That said, the debate as to what constitutes "traditional," weighs heavily due to the non-existence of the cyber domain in the annals of U.S. history, which makes it extremely difficult to provide bearing and precedence for comparison.[117]

With U.S. adversaries like China gaining momentum in the cyber domain, the deliberations of Congress have permitted military forces to comprise a more active role to play along with interim parameters for which to engage. However, it remains to be seen how a full spectrum of adversarial cyber operations can be thwarted through limited high level strategic operations. At the strategic level, the use of these permissions is primarily executed, and the lower levels of command are bogged down through levels of approval. CYBERCOM's 2018 actions against Russian troll farms, were executed by a strategic deterrent vision, rather than for an operational or tactical necessity.[118] However, the need

[115] Biden, Jr., *National Security Strategy*.

[116] John S. McCain National Defense Authorization Act for Fiscal Year 2019

[117] Jack Goldsmith, *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment* (New York: Oxford University Press, 2022).

[118] Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post*, February 27, 2019, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

to compete in the domain extends beyond strategic effects where friction points are induced, and uncertainty is amplified to effectively compete and/or promote stability.[119]

The driving need for prevailing in the cyber domain has initiated what Congress has authorized to date and they are indeed important first steps. Moving forward, the military needs to take advantage of these newly formed authorities and expand the scope and capacity. This can be accomplished by squashing current debates through the DOD initiating the responsibility of levying principles, preventing procedural abuses, and identifying acceptable echelon effects of warfare that span beyond only strategic and delve into tactical implementation. This will build credibility, precedence, and familiarity for traditional military activities as well as reducing pitfalls that have plagued covert and clandestine activities within the intelligence community. The next section suggests ways in which decision makers can further increase comfortability within the cyber domain and its implementation in warfare. Suggestions revolve around an environment well suited for the military by urging guidelines and rules of engagement. Unfortunately, more exacting guidelines may bound decision makers by limiting options. In an environment already determined to be overwhelmed with information and ambiguity, perhaps the best course of action is to adopt new concepts and technology at an advanced rate and implement left and right lateral limits where tactics, techniques and procedures can be developed.

A. PERMISSIONS AT THE OPERATIONAL AND TACTICAL LEVEL

With the release of Joint Publication 3-04, Information in Joint Operations in September 2022, the services are provided with the most up to date blueprints of how to begin incorporating Operations in the Information Environment (OIE), (including cyber), into strategies and planning. This document is meant to provide commanders with fundamental procedures for leveraging essential elements of the information space, therefore expanding a commander's options across the range of the competition continuum.[120] It also lays out what could be interpreted as the substantial

[119] Nakashima.

[120] Joint Chiefs of Staff, *Information in Joint Operations*, Joint Publication 3-04 (Washington, DC: Joint Chiefs of Staff, 2022).

compartmentalization of departments, legal stipulations, and permissions structure that exist to properly conduct and coordinate as well. Military planners are expected to use this doctrine to familiarize themselves with a newly incorporated style of warfare that is proliferating over more traditional and familiar forms of kinetic conflict with an implicit need to remain below the threshold of war.[121] What this document shows is that the information environment is not only new, but also a brutally complex maze of obstacles that a commander, or his staff, must navigate and infuse to compete and dominate to accomplish a mission.

Achieving an information advantage is no easy task and although JP 3-04 provides elementary guidelines to achieve this advantage, what is missing are more refined stipulations that better assist leaders to traverse the murky waters of uncertainty. For example, if we review the elements of a call for fire mission, there are six features involved to properly execute: observer identification, warning order, target location, target description, method of engagement, method of fire and control. Of these components, the decision maker has become proficient well before having to use this skill in a mock or real-world scenario. Granted there are other factors to consider that are implicit within the six elements, but the point to focus on is that the process is familiar and rigid in its execution. JP 3-04 provides a template for a leader to leverage through an integrative process and leverage for effect.[122] Considering the wide birth of options that the cyber domain offers, the implied task would be to devise a more regimented level of employment to build a similar type of reflexive response as compared to calling for fire. Understanding that JP 3-04 is the introductory document that leaders need to begin this process, the intent behind devising more structured means in which to channel the potential of the cyber domain is meant to further the current acceptable use to achieve effective results.

Within JP3-04, it alludes to the fact that Congress authorizes the DOD the authority to delegate permissions of execution for cyber capabilities and their attributed effects.[123]

---

121 Goldsmith, *The United States' Defend Forward Cyber Strategy*.

122 Joint Chiefs of Staff, *Information in Joint Operations*.

123 Joint Chiefs of Staff.

Commands and the chain of command should still implement control measures, however, an environment to practice and execute within the cyber domain should be developed. As it stands presently, the barriers of authority level permissions tend to serve as influential deterrent considerations in an era where you can become irrelevant within 12 to 24 hours and the initiative lost within the information space according to U.S. Northern Command Commander General VanHerck.[124]

B. RULES OF ENGAGEMENT AND AVAILABILITY (KNOWLEDGE, TRAINING, EXPERIENCE)

Looking into potential rules for cyber usage, there are two courses of action that could occur. First, Congress could choose to further define the left and right lateral limits for the who, what, when, and how cyber capabilities are executed. The second option is for the DOD to take ownership of the expansive authorities and delegate down dependent on circumstance, context, and scale. Common practice already dictates what the U.S. military uses in general terms when conducting operations. What is referred to as the Laws of Armed Conflict (LOAC), rules of engagement (ROE), are defined principles of operational domestic and international law that outline the context and degree of use of force.[125] As Legal Support JP 3-84 issues, legal reviews of actions to be taken are scrutinized for operations to determine if the ROE are sufficient to accomplish a specific mission.[126] This is important to understand because it provides an overview of standing rules and is then further scoped to ensure the legalities of specific mission sets for a commander. ROEs can be created from historic experiences and reviewed under both kinetic actions and weapon systems and how they apply to a particular situation. This means military commanders could have had either direct experience or at the very least, can apply basic principles that are familiar for a higher degree of certainty and confidence. As Leslie Zebrowitz suggests,

---

[124] C. Todd Lopez, "Low-Level Commanders Need Authority to Counter Information Operations, Northcom Leader Says," DOD News, September 22, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2785305/low-level-commanders-need-authority-to-counter-information-operations-northcom/.

[125] Joint Chiefs of Staff, *Legal Support to Military Operations*, Joint Publication 1-04 (Washington, DC: Joint Chiefs of Staff, 2016), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_04.pdf.

[126] Joint Chiefs of Staff, *Legal Support*, Joint Publication 3-84 (Washington, DC: Joint Chiefs of Staff, 2016), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_84.pdf.

this availability of repetitive action promotes the tendency for people to prefer things simply because they are familiar with them, which further validates a need for military leaders to practice the new skillsets of the cyber domain to attain the constant exposure.

1. Training: Realism, Venues, Tactics

ROEs will play a significant role in the understanding and usage for further development of military operations in the cyber domain. Train as you fight is a familiar term within U.S. Forces. It is a colloquial term that is most recognizable to services writ large, hence the constant push for training to build reflexive responses. Therefore, the practice of implementing cyber and cyber enabled information operations to training venues that are shifting to multi-domain and large-scale combat operations, should not come as a surprise to military leaders. With the increasing knowledge of foreign adversarial capabilities and organizational structures, such as the PLA's SSF, the assumption is that "Train as You Fight," would play a more substantial role in the design of training events to better reflect real world threats.

There is increasing discussion and directives from higher military echelons of decision makers to incorporate new age technologies to training events, these venues are slow to adopt, as can be ascertained in some Army training venues still reminiscent of counter insurgency design and Middle Eastern culture.[127] As a professional force that is constantly evolving, it is incumbent on military leaders to assist in the adaptation of organizations to keep pace with these changes. Whether the slow adaptation is due to unfamiliarity, lack of funding to develop, or personal preference and apprehension, it remains that "train as you fight," must prevail to sustain efficacy of capabilities.[128] Continued development of ROE will help bridge the gap in this slow acceptance as well as building the reflexive responses that are incumbent in warfare.

[127] Katherine Kjellström Elgin, "How the Army Is (NOT) Preparing for the Next War," *War Room* (blog), September 25, 2019, https://warroom.armywarcollege.edu/articles/the-next-war/.

[128] Corey Robertson, "Train as We Fight," U.S. Army, May 7, 2015, https://www.army.mil/article/148095/train_as_we_fight.

There exists a certain degree of compartmentalization within training events and the inability to experience the true impacts of cyber effects on the battlespace. In December of 2021, the DOD conducted the largest multinational cyber exercise to date. Cyber Flag 21–1 is one of the three training exercises that CYBERCOM conducts and is certainly a valuable training event for building integration and interoperability amongst U.S. allied forces in addition to signaling to adversaries at the strategic level.[129] Another example is the Army's Muscatatuck Urban Training Center located in Butlerville Indiana. It serves as a training site for developing tactical cyber units that sit outside of CYBERCOM and fill the gap that exists between CYBERCOMs strategic level interaction and tactical operations.[130] Accepting of the complex and multi-tiered environment, the need for these skills and units are increasing and both training venues provide cyber units the capacity to develop, execute, and hone their skills within the cyber domain. Training events like Cyber Flag and Muscatatuck are great places to work the tactics, techniques, and procedures for delivering effects within the cyber domain, however, the effects that they achieve are not necessarily transferrable to other organizations that would be using the capabilities both in a mock environment and /or real-world application.[131] The inability to manifest these effects are not necessarily due to lack of want, but in some instances due to aged facilities. The Combat Training Centers (CTC) of Fort Polk and Fort Irwin are not yet designed to accommodate the real-world battlespace of cyber and the information space.[132] Indeed, there have been massive strides in refurbishment towards modernizing and the style of combat, however this is primarily focused on kinetic activities. Commanders and decision

129 "DOD's Largest Multinational Cyber Exercise Focuses on Collective Defense," U.S. Department of Defense, December 6, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2863303/dods-largest-multinational-cyber-exercise-focuses-on-collective-defense/.

130 Mark Pomerleau, "New U.S. Army Cyber Unit Is Building Concepts for Tactical Cyber Operations," C4ISRNet, December 29, 2021, https://www.c4isrnet.com/cyber/2021/12/29/new-us-army-cyber-unit-is-building-concepts-for-tactical-cyber-operations/.

131 David Vergun, "Multi-Domain Battle Requires Non-Stovepipe Solutions, Say Leaders," U.S. Army, May 25, 2017, https://www.army.mil/article/188282/multi_domain_battle_requires_non_stovepipe_solutions_say_leaders.

132 David Doyle and Aaron Coombs, "How Has the Joint Readiness Training Center Changed to Adapt to Large-Scale Combat Operations?," *Military Review* 98, no. 5 (September 2018): 72–79, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2018/Doyle-and-Coombs/.

makers across the board need to also be versed and subjected to the prospective effects and rules of engagement that the cyber domain has to offer. As these specialized units continue to train in isolation from their potential supported units, the supported units do not become anymore familiar with the domain, and certainly do not build the confidence in their capabilities. As a result, commanders withhold the authorization and permission to remove barriers that exist and delegate down to subordinate commanders. This lack of familiarity will continue to push back the proficiency and aptitude for using such effects as well as slowing the release of permissions to levels of operational need that will grow in demand to compete and dominate.[133]

An approach to fully understand cyber capabilities and its effects may be to draw a comparison to targeting and how targets are arrayed across the three levels of warfare, strategic, operational, and tactical. According to Dr. James Lewis, "target selection and careful graduation of effect will also help manage risk."[134] He states this under the context of continuing to build a framework for coercive cyber strategy, however at the core of his argument is the blatant need of systemized implementation. Applying this under the pretext of rules of engagement and targeting doctrine, the military can mature the process of what is deemed acceptable use regarding the visibility, scale, and damage imposed as the result of a cyber action. Notwithstanding the vast separation of strategic and tactical operations, it is important to note, as stated in JP 3-60 Joint Targeting, "many of the ways and means associated with targeting result in tactical-level effects relative to selected targets."[135] Meaning it is just as imperative for the operational and tactical levels of warfare to comprehend and plan for cyber capabilities as is the high level of strategic implementation.

---

[133] Lopez, "Low-Level Commanders Need Authority."

[134] James Andrew Lewis, "Toward a More Coercive Cyber Strategy: Remarks to U.S. Cyber Command Legal Conference, March 4, 2021," Center for Strategic & International Studies, March 10, 2021, https://www.csis.org/analysis/toward-more-coercive-cyber-strategy.

[135] Joint Chiefs of Staff, *Joint Targeting*, Joint Publication 3-60 (Washington, DC: Joint Chiefs of Staff, 2013), https://www.justsecurity.org/wp-content/uploads/2015/06/Joint_Chiefs-Joint_Targeting_20130131.pdf.

C. CONCLUSION

Congress and the Executive Branch have broadened the scope of the potential usage of cyber operations for the DOD under the threshold of armed conflict. It is generally understood that there is a desire to remain anonymous and conduct actions that are non-attributional. This is not to say that cloak and dagger and spy vs. spy is the main goal of DOD operations under the auspices of title 50 covert allowances, however, considering the implicit need of secrecy to prevent assumed backlash from adversarial nations, the proper elements and designations for clandestine and traditional military activities are in place for military units to manage as needed. Due to the limitless boundaries and complexity that the cyber domain presents, there needs to exist a basic left and right lateral limit for which commanders at various levels can operate within. By allowing commanders the freedom to employ relative capabilities within their areas that they have earned the "special trust and confidence" to lead and command, the military prepare these decision makers at large beyond the isolated knowledge of specialized cyber units so that commanders can request appropriate effects. This proficiency can only be fostered in a relative environment permissive of typically non delegated authorities and pre-determined rules of engagement, which reinforce lessons learned of cyber integration. Only at this point will JP 3-04 begin to fill true potential for properly integrating and synchronizing effects in the cyber domain.

In the following chapter of cultural limitations, the United States military has yet to fully integrate and accept cyber operations into its campaigns and strategy. Academic literature exists to support the added complexity of biased judgement and leery hesitation that the cyber domain not only brings with it, but also expresses the tendency of systemic modes of decision making and compartmentalization that serve as barriers for quick adaptation.[136] It also provides a look into some of the cultural predispositions that exist and suggests alternative methods to approach and overcome these barriers and the new paradigm shift to U.S. military cyber integration.

[136] Lopez, "Low-Level Commanders Need Authority."

THIS PAGE INTENTIONALLY LEFT BLANK

V. UNITED STATES CULTURAL PREDISPOSITION

Henry Ford, a successful entrepreneur, and pioneer of the early 20th Century that changed the dynamics of business and manufacturing worldwide, stated, "If you always do what you've always done, you'll always get what you've always got."[137] If you want to achieve different results, then change is required. His philosophy and approach to problem solving proved to be invaluable to his success by adapting to circumstances and accepting change as an inescapable variable. Applying this perspective, the U.S. military touts itself to be experts in adaptability, but still struggles when confronted with something unfamiliar.[138] This can be exemplified through the last 20 years and $145 billion in spending, where the U.S. conceded to the struggles of Afghanistan reconstruction with little to show for their efforts.[139] Arguably, there is a certain comfort in the environment of the known; change can be difficult.[140] However, there are methods and processes that exist that facilitate the scope and scale of change. Prior to change, an individual must recognize the barriers that exist, accept the need to change, and prevent reverting back to the past.[141] According to Janis, the need for change can additionally be obfuscated by collaborating with the like-minded individuals who confirm rather than challenge or enhance our opinions.[142] This can all too often lead to groupthink, stagnation of growth, and it forces a predisposition of certain courses of action without exploring alternatives.[143]

---

[137] Lydia, "'If You Always Do What You've Always Done, You'll Always Get What You've Always Got.' ~ Henry Ford," *Hidden Gem* (blog), November 8, 2021, https://hiddengemprofiles.com/2021/11/if-you-always-do-what-youve-always-done-youll-always-get-what-youve-always-got-henry-ford/.

[138] David Barno and Nora Bensahel, "Falling into the Adaptation Gap," War on the Rocks, September 29, 2020, https://warontherocks.com/2020/09/falling-into-the-adaptation-gap/.

[139] Special Inspector for Afghanistan Reconstruction, *What We Need to Learn: Lessons from Twenty Years of Afghanistan Reconstruction* (Arlington, VA: Special inspector for Afghanistan Reconstruction, 2021).

[140] Charlotte Nickerson, "What Is the Mere Exposure Effect?," Simply Psychology, March 8, 2022, https://www.simplypsychology.org/mere-exposure-effect.html.

[141] Kendra Cherry, "The 6 Stages of Behavior Change," Verywell Mind, July 28, 2021, https://www.verywellmind.com/the-stages-of-change-2794868.

[142] Irving L. Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, 2nd ed. (Boston: Houghton Mifflin, 1982), http://archive.org/details/groupthinkpsycho00jani.

[143] May Busch, "Why Being with Like-Minded People Is Dangerous," May Busch, December 6, 2015, https://maybusch.com/why-being-with-like-minded-people-is-dangerous/.

Afraid to take risks because the problem does not fit what is expected, the problem does not adhere to an organizational prescribed methodology, or the problem induces fear of individual punishments.[144] The thought of adding just another item on the list of things to know, resource, and plan is daunting enough for military leaders. The most troubling aspect is that, even if the U.S. is not willing to move beyond certain self-imposed barriers, our adversaries will.

A. INTRODUCTION

Twenty years ago, the U.S. military had to adapt to a new style of warfare contrary to what had been experienced during Global War on Terror. It was not easy to adapt, but because the focus was still on kinetic capabilities, brute force remained the primary means by which success could be measured.[145] The kinetic assessment of risk was calculated by tangible attributes such as life, limb, or eyesight and was relatively easy to interpret through percentages, charts, or graphs. This provided decision makers with decision matrices that were clean and concise and offered hard lines of risk to determine future operational levels of acceptability.[146] Today, the United States is on the precipice of change again and with this change comes the uncertainty and apprehension to accepting it. Homeland Defense & Security Information Analysis Center describes this transitional state for emerging technologies as "politically difficult, if not precarious, to militarily define and respond to non-kinetic activities."[147] Adding even more degrees of difficulty, the U.S. is navigating this intermediate state this time in a threshold below armed conflict, not war, meaning that states have not formally declared a state of war, yet there exists conflict among different parties that could eventually result in armed conflict. The state of strategic power

144 Janis, *Groupthink*.

145 Cole Livieratos, "Bombs, Not Broadcasts: U.S. Preference for Kinetic Strategy in Asymmetric Conflict," *Joint Force Quarterly, JFQ*, no. 90 (2018): 60–67, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1567411/bombs-not-broadcasts-us-preference-for-kinetic-strategy-in-asymmetric-conflict/.

146 Bradley DeWees et al., "Toward a Unified Metric of Kinetic and Nonkinetic Actions: Meaning Fields and the Arc of E," *Joint Force Quarterly, JFQ*, no. 85 (2017): 16–21, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-85/jfq-85_16-21_DeWees-et-al.pdf.

147 Joseph Defranco et al., "Emerging Technologies for Disruptive Effects in Non-Kinetic Engagements," *Homeland Defense & Security Information Analysis Center* 6, no. 2 (Summer 2019), https://hdiac.org/articles/emerging-technologies-for-disruptive-effects-in-non-kinetic-engagements/.

competition is giving rise to a host of threats in the name of national defense that is reshaping the way the U.S. and its Allies must navigate and adapt to confront modern competitive challenges. This is forcing an entirely new calculus of risk to be introduced thru incorporated advances in the cyber domain and operations in the information environment. Additionally, this change is exacerbated by the hesitant nature and generational gap of policy makers unwilling or uncertain of how to proceed "in a country being revolutionized by tech."[148] This is further compounded within a society that has a "penchant for adopting new tools while still clinging to older practices."[149]

Sweeping technological advances in the cyber domain and the information environment is altering the dynamics of decision making within governmental policy development and military implementation of capabilities. Senior leaders of the military and government are becoming more risk averse in their decision-making calculus as adversarial momentum grows in the digital realm.[150] For example, this was overtly indicated by Northern Command Commander General VanHerck's 2021 public address to risk aversion in the information space and the US's inability to react effectively to peer competitors.[151] Additionally, this aversion to cyber is not limited to effects of capabilities in the battlespace alone.

In October of 2021, retiring Vice Joint Chiefs of Staff Gen Hyatt issued that the 2000 Quadrennial Defense Review was significant in that it indicated that the U.S. no longer had direct adversaries and that the U.S. would move to a capabilities based defense strategy over a specific threat model.[152] What this created for national defense, was an environment that government agencies could pick and choose at their discretion what capabilities were considered best to combat future asymmetric threats. Simultaneously, this

148 Selk, "'There's so Many Different Things!'"

149 Arquilla, *Bitskrieg*, 75.

150 Lopez, "Low-Level Commanders Need Authority."

151 Lopez.

152 Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, 2001), https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/qdr2001.pdf.

strategy introduced a no fail atmosphere for execution of ideas.[153] This situation produced a generation of leaders reluctant to attempt new things that were not guaranteed to succeed.[154]

At its basic core, risk aversion is "a reluctance to take risks or make decisions that may fail to accomplish the individual's desired ends or goals."[155] Lieutenant Colonel William Bell, United States Army, spoke at the 1999 Joint Services Conference on Ethics of a fundamental change that had been occurring for quite some time, risky behavior, zero defect mentality, and decision makers being at odds with self-preservation at the expense of core values.[156] Organizations are composed of individuals, each with their own sets of values and beliefs that sometimes conflict. Industrial Social Scientist Jean Hartley suggests that when ideologies are established within organizations, they become the central nervous system in maintaining social group member identification.[157] This group membership plays a significant role in the cognitive framework for utility and effectiveness binding the system together. In a culture that preaches uniformity, it is challenging for individual viewpoints to emerge.[158] In 2019, Colonel G.I. Wilson, United States Marine Corps (retired), reaffirmed what Bell had cited as a systemic and growing problem in the services. Split ideologies of individual advancements compared to a prime directive of "winning wars" is just as pervasive, with the end result being a weakening of national defense.[159]

The cultural influences that risk aversion creates, or the one that Wilson and Bell discuss, can have negative effects. Some effects of this type of environment are a concern

---

153 Department of Defense.

154 Myers, "Risk Aversion and Secrecy Are Costing US."

155 William Bell, "Risk Aversion in the U.S. Army Officer Corps," in *Joint Services Conference on Professional Ethics: The Impact of Policies on Organizational Values and Culture*, 1999, http://isme.tamu.edu/JSCOPE99/Bell99-2.html.

156 Bell.

157 Jean F. Hartley, "Ideology and Organizational Behavior," *International Studies of Management & Organization* 13, no. 3 (1983): 7–34, https://www.jstor.org/stable/40396913.

158 "Understanding and Developing Organizational Culture," SHRM, July 21, 2022, https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/understandinganddevelopingorganizationalculture.aspx.

159 GI Wilson, "Careerism and Psychopathy in the U.S. Military," Fabius Maximus website, June 23, 2019, https://fabiusmaximus.com/2019/06/23/generals-careerism-and-psychopathy/.

for careerism, fear of being ostracized for differences of opinion, becoming irrelevant or a liability by association, and being passed over for promotions.[160] All of these to varying degrees have a direct correlation with how someone will act within an organization. Within this context, innovative thought, progressing to confront adversaries, and answering the call to "dominate" the information environment becomes much more of a challenge when you have more than just the enemy to consider.

B. BUREAUCRATIC VANTAGE

There is an important distinction to unpack regarding this concept of values, orders, and risk when evaluating how a bureaucratic system like the military, government, or any other public service function for purpose. There are certainly times when following an order to the letter is exactly what is needed, however, the values ingrained within the organization should reflect and extend the individual professionalism and trust to exercise the autonomy to be flexible when circumstances dictate the need. Unfortunately, it can be argued that this autonomy is being attritted and authorities and permissions being held at the highest levels to avoid backlash within communities.[161] Von Mises *Bureaucracy,* proposes that the merits which we gauge success and risk is indicative of whether it is a private enterprise or is government sponsored. Whereas private industry adapts and adjusts to conditions within a standard motive and criterion for profit, a government/military entity's success can be vague and subject to interpretation.[162] In lieu of an inability to rely on profit seeking as a foundation for success and risk balance, governments concentrate on restrictive actions as a pre-emptive means to reduce squandering of resources and abuses of power, thereby controlling through avoidance. For example, in December 2021, Vice Chairmen of the Joint Chiefs of Staff Admiral Grady discussed America's need to "accept

[160] Myers, "Risk Aversion and Secrecy Are Costing US"; Trent Lythgoe, "Our Risk-Averse Army: How We Got Here and How to Overcome It," Modern War Institute, May 9, 2019, https://mwi.usma.edu/risk-averse-army-got-overcome/.

[161] Kaminska, "Risk Aversion Is at the Heart of the Cyber Response Dilemma."

[162] Ludwig Von Mises, *Bureaucracy* (New Haven, CT: Yale University Press, 1945).

failure to learn faster."[163] He issued that the risk averse nature of today's military is a product of the peerless adversary era of the 90's.[164] The U.S. is now having to contend with the aftermath of this avoidant behavior for zero defect weapons and systems. Wilson's Bureaucracy: explores principles that can address some of these shortcomings that Admiral Grady described. He said that successful bureaucracies must exercise autonomy.[165] A certain trust must exist to permit decision makers to be flexible in their actions as new problems arise.[166] As discussed in Admiral Grady's statement in December 2021, the military bureaucracy had not historically promoted trust through an age of zero-defect acceptability.

On the surface, the military reinforces the concept that trust is bestowed to subordinate commanders through doctrine. The military uses this not as a prescription, but guidelines, understanding that circumstances can change, therefore providing leeway for adaptation. Army Doctrinal Publication (ADP) 6–0 Mission Command is a good representation of this with rhetoric such as "using disciplined initiative to empower agile and adaptive leaders" to make the right call.[167] An increasing and limiting trend is the restriction of empowerment to lower echelons due to a comfortability factor induced by uncertainty in rising technologies and how they should be employed at all levels as compliments to existing instruments of power.[168] Wilson's, *Bureaucracy,* further adds a degree of complexity to the already existing ambiguity for decision making within governments and militaries. The values within the organization should be inherently meshed to foster success, however, there exists a multitude of bosses within the chains of

163 Sam LaGrone, "Eliminating 'Risk Aversion' Key to Weapons Development, Says Vice Chair Nominee Grady," USNI News, December 9, 2021, https://news.usni.org/2021/12/08/eliminating-risk-aversion-key-to-weapons-development-says-vice-chair-nominee-grady.

164 LaGrone.

165 James Q. Wilson, *Bureaucracy: What Government Agencies Do and Why They Do It* (New York: Basic Books, 1989).

166 Zachary Griffiths, "In Defense of the Military Bureaucrat," American Politics, Modern War Institute, April 4, 2018, https://mwi.usma.edu/defense-military-bureaucrat/.

167 Department of the Army, *Mission Command: Command and Control of Army Forces*, ADP 6–0 (Washington, DC: Department of the Army, 2019), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18314-ADP_6-0-000-WEB-3.pdf.

168 King and Gallagher, *Cyberspace Solarium Commission Report*.

command that also have opinions that are varied and driven by personality.[169] To make matters even more difficult to navigate, decision makers often find themselves bogged down by conflicting policies that often distort the decision makers original objectives.[170] Policies can bind them despite what might be considered to be an illogical choice. A bureaucratic machine is safer to traverse not by subverting the status quo or fundamental attributes of the institution, but by "following the rules," and obeying the order.[171] In Kahneman's *Thinking Fast and Slow*, he suggests that decision making is only part of the characteristics of a bureaucratic system.[172] They are designed to function over generations with slight adjustments to continue functionality.[173] Even with the slight adjustments over time, this type of system does not bode well for creative and adaptive thought. The U.S. is finding it difficult to adapt and compete compared to autocratic adversaries not having to contend with slow adaptive process or regimented compartmentalization due to the inherent design of a bureaucracy.

C. CYBER RISK AVERSION

Cyber and cyber-enabled information operations are causing officials to become closed off and apprehensive to making decisions of employment. This is partially due to senior officials, and down the chains of command, having continued uncertainty, complexity, knowledge gaps, and risk averse temperament, in fear of causing escalation between adversaries. In our current competitive status with our pacing threat, China, the U.S. manages to find itself between a rock and a hard place. It must balance competing with a peer threat and managing escalation against this foe is the true crux of the problem because ultimately, the U.S. is tired of being at war.[174] There exists a fine line between ensuring that we don't forfeit advantage through the increased cost imposition of persistent engagement, compared to weak and hollow responses that chip away at credibility and the

169 Wilson, *Bureaucracy*.

170 Wilson.

171 Wilson.

172 Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

173 Kahneman.

174 Myers, "Risk Aversion and Secrecy Are Costing US."

ineffective legitimate response. Comparatively to nuclear deterrent philosophy, the cyber domain and information environment realm pose as a substantial issue in this respect because of potential for the unknown. Exchanges in this domain continue to raise fears of unintentionally escalating to conflict.[175] Though recent research suggests that cyber or information operations by themselves do not achieve the escalatory reaction by themselves. However, their ability to triggering responses are just as important to factor into the strategic use of options and the balancing act that occurs on the escalatory pendulum.[176]

The Cyberspace Solarium Commission was established to "develop a consensus on a strategic approach for U.S. cyber defense."[177] Due to the adverse risk nature in decision making, the Commission's intent is to coalesce the known variables to manage a strategic layered cyber deterrence and tackle the ambiguity that is plaguing the tentative integration of the cyber and informational spheres.[178] The heavy burden of identifying the "how" continues to elude policy makers. That said, the Commission is giving structure and clarity so that when our political and military leaders say they will impose a defend forward posture with persistent engagement, it is not just words but actions and concrete meaning that will accompany those words. Valeriano states that cost imposition is at the core of the commission's report.[179] Through this report, the gaps of inadequacy are being addressed and to achieve theoretical tangible success, a realignment of government structures must be an acceptable way forward. Unfortunately, this will once again introduce an air of uncertainty because it moves against the grain of familiar and comfortable practices. Ironically, having to try something new in order to accept something new, suggests that it must be tried to evaluate the results from present process. The inference would be that knowledge, understanding, familiarity, and permissions must unite to even attempt new and innovative implementation within the domain.

---

175 Kaminska, "Risk Aversion Is at the Heart of the Cyber Response Dilemma."

176 Kaminska.

177 King and Gallagher, *Cyberspace Solarium Commission Report*.

178 King and Gallagher.

179 Brandon Valeriano, "Cost Imposition Is the Point: Understanding U.S. Cyber Operations and the Strategy Behind Achieving Effects," *Lawfare* (blog), March 27, 2020, https://www.lawfareblog.com/cost-imposition-point-understanding-us-cyber-operations-and-strategy-behind-achieving-effects.

D. ACCEPTING THE NEW PROSPECT THEORY

Understanding our predispositions will be a key factor in how the U.S. approaches new concepts and interaction. Known principled biases at work are a preventative for future actions within the U.S. This means that with a given set of circumstances from lack of knowledge or interaction with cyber capabilities within the information environment, decision makers are prone to accept the lesser of the two evils. The lesser of the evils is the concept that is already familiar. The less familiar environment as defined by JP 3-04, the Information Environment is "an intellectual framework to help identify, understand, and describe how those often intangible factors may affect the employment of forces and bear on the decisions of the commander."[180] Prospect theory, also known as "loss aversion" could be used as guidelines for our leaders and their capacity to accept or at the very least concede to the notion that modern problem sets like that of Chinese cyber advancements, cannot be met, addressed, and incapacitated by traditional modes of U.S. thought. We will look deeper into how prospect theory can provide clarity of thought and structure to an ongoing controversy of decision making within the cyber domain and what this might mean for future applications in military actions, activities, and training.

Military leaders will have to make decisions in stressful situations and in times of uncertainty. This is not a new concept, so much so, that some private industry revere and look to emulate military models of structure and decision making in order to blend them with business crisis management techniques.[181] This borrowing of military standards is in part designated for quick and decisive action along with long term planning and resource management. We discuss process and decision making because it can be the success or failure of an organization. Just as private industry is borrowing from the military because circumstances have revealed a need for change, so must the military borrow from outside sources in light of a shifting technology driven environment. The doctrine that has been developed over generations of U.S. warfare, is not enough to address the needs and

[180] Joint Chiefs of Staff, *Information in Joint Operations*, ix.

[181] Yuval Atsmon, David Chinn, and Sven Smit, "Lessons from the Generals: Decisive Action amid the Chaos of Crisis," Our Insights, May 18, 2020, https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/lessons-from-the-generals-decisive-action-amid-the-chaos-of-crisis.

fluctuations that the computer age as brought. Therefore, the basis of decision making must be adjusted to fit the circumstance, as has been the requirement with every jump in weapons technology.[182] Due to this need for decision making in uncertainty, we have to unpack exactly how leaders decide to make a decision in the first place and what has determined the model of thought. In this section we will discuss an academic view of decision making as it pertains to past popular thought and present-day advances in decision making theory and how it relates to decisions under risk within the cyber domain. Specifically, we will address what was considered a backbone of decision principles, namely, Expected Utility Theory and then move into the modern approach of prospect theory, a decision theory that incorporates human dynamics within its model, as well as tangents of organizational influence factors. Both theories have been highly documented, therefore we will provide a base understanding to highlight potential insight for leaders to relate the application of cyber assets and other aspects of information operations from a rejuvenated perspective with the intent of decreasing the lag of acceptance for cyber operations applicable use within Strategic Competition.

1. Expected Utility Theory

Top military officials are hesitant to delegate certain authorities to lower-level commanders for the new domain of cyber due to risks of unknow territory. In 2021, General VanHerck, Commander of U.S. Northern Command, stated "I think we're getting our rear end handed to us in the information space because we're so risk-averse in the environment that we operate in today."[183] Many of his comments codify the significance of the necessity to push permissions to operational commanders. By doing this, it would reduce bureaucratic red tape and increase the ability to respond to threats in a timely fashion. Yet the issues of a risk averse military environment still persist.[184] What he didn't discuss is how to achieve this and who will decide how barriers will be surmounted. Enter Expected Utility Theory (EUT), a foundation of rational decision making since it was first introduced

[182] Darren M. Stewart, "New Technology and the Law of Armed Conflict," *International Law Studies* 87 (2011): 271–98, https://digital-commons.usnwc.edu/ils/vol87/iss1/12/.

[183] Lopez, "Low-Level Commanders Need Authority."

[184] Myers, "Risk Aversion and Secrecy Are Costing US."

in the early 1700's. First presented and applied in the economic realm by Daniel Bernoulli, it was a tool to analyze or predict outcomes under uncertain circumstances regarding risk and reward, and gains and losses.[185] It provided a model of how people do make decisions with heavy emphasis on the highest expected utility of the predicted outcome with an overall premise of rationale thought.

Expected Utility takes into consideration all known available options that a person or organization has to choose from and from those choices, the presumably rational actor(s) makes decisions based on best outcome, involving preference and expected consequences.[186] EUT is a useful tool for a broad approach to the unknown with respect to rational thought and developing a classification system of optimal choices, however certain flaws exist with regard to its purpose. It provides a great model of logical thinking, but it fails to incorporate human dynamics and potential biases of those making the decision as postulated by Kahneman and Tversky's research on the applied incorporation of judgement and heuristics biases.[187] So, in effect, it provides an incomplete picture for actor(s) to address the unknown, but EUT provides a solid foundational starting point to narrow the scope of a problem.[188] For example, Herbert Simon believes that decisions made solely from rational choice are limited by subjective limitations of the decision maker.[189] Time, perspective, and cognitive capability play a substantial part in an actor(s) rational thought process and presents a bounded context from the decision makers ability to choose optimal options.[190]

---

185 Nicola Giocoli, "The 'True' Hypothesis of Daniel Bernoulli: What Did the Marginalists Really Know?," *History of Economic Ideas* 6, no. 2 (1998): 7–43, https://www.jstor.org/stable/23722513.

186 James G. March, *A Primer on Decision Making: How Decisions Happen* (New York: Free Press, 1994).

187 Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (September 27, 1974): 1124–31, https://doi.org/10.1126/science.185.4157.11.

188 R. A. Briggs, "Normative Theories of Rational Choice: Expected Utility," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Fall 2019 (Stanford, CA: Metaphysics Research Lab, Stanford University, 2019), https://plato.stanford.edu/archives/fall2019/entries/rationality-normative-utility/.

189 Herbert A. Simon, "A Behavioral Model of Rational Choice," *Quarterly Journal of Economics* 69, no. 1 (February 1955): 99–118, https://doi.org/10.2307/1884852.

190 Simon.

Logical rational thought is the basis of military planning and preparation. Framing the problem and developing strategy based on the known information is indicative of joint planning. This planning and preparation are based in part of principles and doctrine that has developed over the centuries within the U.S. military. Commanders and staffs are asked to develop strategies using Operational Art where they employ their knowledge, experience, and creativity to a given problem set.[191] They must stay flexible and adaptable to the circumstance, but always keeping in mind risks and probabilities of success and failure.[192] The above are only aspects of the process, however, important to note is that there is always an emphasis on knowledge and experience throughout the planning process. So, what is to be done when the principles of warfare change and differ from previous experience and knowledge? Perhaps the enemy doesn't subscribe to the same theory of logic and process, consequently changing the rules that have developed over those centuries. Russia's "Active Measures" or China's "Unrestricted Warfare" strategies, both U.S. rivals are revising the way in which they conduct war and are adapting to the modern technological era, and the U.S. would be remiss if it did not also attend to the way in which we perceive warfare as well.[193]

2. Prospect Theory

Military doctrine provides a basis for developing a common operating picture for the decision maker to make judgements and assessments of a given circumstance. Just like expected utility theory, doctrine can assist in framing a problem set with efforts to address the uncertain, but there are still certain aspects that need/must be accounted for. With its origins stemming from expected utility theory, prospect theory was developed in the 1970s by Tversky and Kahneman to address what they saw as a considerable flaw in the design of EUT, which was that it did not take into account heuristics and biases that human dynamics are inherently wrought with.[194] Prospect theory in a very basic sense states that

[191] Joint Chiefs of Staff, *Joint Planning*, Joint Publication 5-0 (Washington, DC: Joint Chiefs of Staff, 2020), https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/5-0-Planning-Series/.

[192] Joint Chiefs of Staff.

[193] Liang and Xiangsui, *Unrestricted Warfare*.

[194] Tversky and Kahneman, "Judgment under Uncertainty."

individuals make decisions of risk and uncertainty in relation to potential gains and losses. However, choices made are influenced by subjective biases that accompany the decision makers probability calculus and frequency of exposure to similar instances.[195]

Kahneman and Tversky, from their earlier works, identified the three unique cognitive biases of representativeness, availability, and anchoring as underlying preconceptions that significantly influenced decisions, all of which could be considered as an individual making assumptions from different aspects of recall.[196] For example, if we look at the apprehensive state of military decision makers to incorporate cyber into an operation, the reasoning might be based on what they know a cyber effect to be attributed to or what their frame of reference might be when considering a cyber effect.[197] There frame of reference may only be the STUXNET attack on the Iranian nuclear power plant in 2010.[198] STUXNET was the name for the malicious computer code that attacked the SCADA systems, (Supervisory control and data acquisition,) of Iran's nuclear facilities, which ultimately caused substantial damage to Iran's nuclear program.[199] Due to the notary of STUXNET and actual knowledge base of an individual, this event cloud the judgement of the decision maker to not only think that using such a cyber option is not warranted to the current operation, but the ability to use such an effect is well beyond the organic capacity of his/her unit. Furthermore, a Commander must also weigh what the probability of success by using a cyber capability must be as well. Kahneman and Tversky postulate that based on an actor(s) relative knowledge or understanding of how something might be representative to something else, will influence how the actor(s) chooses to respond in similar instances.[200]

---

[195] Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* 47, no. 2 (1979): 263–91, https://doi.org/10.2307/1914185.

[196] Tversky and Kahneman, "Judgment under Uncertainty."

[197] Kaminska, "Risk Aversion Is at the Heart of the Cyber Response Dilemma."

[198] Jim Finkle, "Researchers Say Stuxnet Was Deployed against Iran in 2007," *Technology News*, February 26, 2013, https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226.

[199] William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, sec. World, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[200] Tversky and Kahneman, "Judgment under Uncertainty."

Looking at the availability heuristic bias for the DOD, the common reference point for over twenty years has been operating in a counter insurgency environment.[201] The US' current adversaries have greater resources and capabilities that a counter insurgency force will not typically have. At the small unit level, the past twenty years of experience and refinement of doctrine, have instructed them to begin priorities of work, build physical fortifications, plot out defensive fighting positions, and build mortar pits for counter battery or targeting measures. However, now the enemy has wide range offensive and defensive cyber capabilities compared to recent wars. Hypothetically, some of the U.S. service members are wearing GPS watches that are inadvertently projecting signals into cyberspace, signals that can be picked up by enemy signal analysis, and subsequently targeted from a distance.[202] The commander's decision to conduct certain activities for the force protection of his unit are well founded. Still, an extremely dangerous aspect of defense was negated because of lack of consideration or low risk associated. Decisions made from muscle memory and the recent past certainly influence the decisions me make in future situations, especially when the reference point is recent and easily retrievable. In Kahneman's "Thinking, Fast and Slow," he discusses how humans are predisposed to prioritizing bad events, news, and information.[203] The availability heuristic bias is the predisposition in action when decision makers do not expand the possibilities beyond resemblance and recall

The anchoring heuristic bias relegates actor(s) to a starting point or estimate of a given thing or things. This bias narrows the scope of thinking and inhibits movement outside the boundaries of the original point. Anchoring has been an effective tool for marketing and advertising, and many times can be traced back to the cost, amount, or value of something. However, it has other transferable attributes outside of cost such as misinformation and disinformation campaigns that have increased with intensity with the

201 Scott D. Applegate, "The Principle of Maneuver in Cyber Operations," in *International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (2012 4th International Conference on Cyber Conflict, Tallinn: NATO CCD COE Publications, 2012), 183–95.

202 Liam Collins, "Russia Gives Lessons in Electronic Warfare," Association of the United States Army, July 26, 2018, https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare.

203 Kahneman, *Thinking, Fast and Slow*.

advent of social media.[204] The anchoring of something does not necessarily have to be money, it can be a concept or idea as well. For example, the 2016 Presidential Elections of the United States was highly documented to have been tampered with by Russian troll farms with the intent of sowing discord and trust amongst the U.S. voting public and degrading U.S. democracy.[205] This ultimately played a pivotal role in perceptions from the American public towards the presidential candidates, which in turn created turmoil across the population. This Russian objective anchored sections of the American public to false narratives and manufactured truths underneath the guise of legitimate organizations and individuals.[206] Seeing or hearing about something first, regardless of factual truth, provides a base of reference to an individual(s) and this reference point puts the decision maker on a specific trajectory of thought that is difficult to divert from. This concept, now applied to a military application, can cause military leaders to be uncertain in split decision environments. The need to make quick hasty decisions is inevitable. Performing military best practices might not be the solution to the problem. Understanding what compels military leaders to decide, should not be based in a preconceived falsity due to limited insight of past experience, knowledge, or familiarity, and definitely not by basing the decision from an irrelevant point of origin.

3. Value of Insight

As discussed by Kahneman and Tversky, the value in expanding EUT to incorporate prospect theory's biases impacts on decision making, is that the decision to be made is further framed with a more accurate depiction of not only what results can be achieved through factual utility, but it eliminates factors that could contribute to poor judgment and poor outcomes through exposing an individual's prejudices.[207] Using

[204] Judith E. Rosenbaum and Jennifer Bonnet, "Looking Inward in an Era of 'Fake News': Addressing Cognitive Bias," Young Leaders of the Americas Initiative, June 10, 2019, https://ylai.state.gov/looking-inward-in-an-era-of-fake-news-addressing-cognitive-bias/.

[205] "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements," U.S. House of Representatives Permanent Select Committee on Intelligence, February 16, 2018, https://intelligence.house.gov/social-media-content/.

[206] Congress. House. Permanent Select Committee on Intelligence.

[207] Tversky and Kahneman, "Judgment under Uncertainty."

prospect theory does not provide the only solution, but it does provide a pathway through the decision making process that helps put into context the gains and losses from a specific point of reference. This point of reference can have sway over balancing of the decision process to employ approaches when allocating resources.[208] For example, in February of 2022 and the onset of the Russo Ukrainian conflict, President Biden was given a multitude of options for intervening in the conflict by implementing cyber warfare designed to disrupt Russian operations.[209] The options proposed would produce effects that fell below an act of war according to international law.[210] Yet, the U.S. government was divided in concern for escalatory retaliation for the use of cyber, regardless if the operations were veiled through covert means. As previously mentioned, Libicki considers the principle of escalation brought on by cyber operations as unfounded and without precedent.[211]

The Executive and Legislative Branch of the U.S. are making decisions from a frame of reference created by nuclear policy from the 1960s.[212] Considering that the opposition has a vote in response measures, there is the perceived bias that Vladmir Putin would also abide by the same international law and not interpret U.S. intervention as an act of war. The effects that would be achieved would certainly garner utility on behalf of Ukraine, however, the biased assumptions and frame of reference altered the way that decisions were made. Just as with military doctrine or decision-making process, provides a roadmap to frame a problem, prospect theory further defines and identifies subtle nuances that can better assist the decision maker in avoiding the pitfalls of assumptions in fact.[213] The goal of illuminating hidden prejudices or knowing the unknown may not give the decision maker the answer they are looking for, however it does support in framing uncertainty, therefore further reducing risk to unknown concepts.

---

[208] Kahneman and Tversky, "Prospect Theory."

[209] Ken Dilanian and Courtney Kube, "Biden given Options for Unprecedented Cyberattacks against Russia," NBC News, February 24, 2022, https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558.

[210] Dilanian and Kube.

[211] Libicki, "Correlations between Cyberspace Attacks and Kinetic Attacks."

[212] Libicki.

[213] Tversky and Kahneman, "Judgment under Uncertainty."

4. Human Nature

Humans as a species are characteristically drawn to the path of least resistance. This can be linked to the development of optimal survival responses fashioned through generations in to "defend against recurring and novel threats."[214] Due to sensory overload and the desire to conserve energy, the human body will form quick neurological responses that assist in the transition to surviving another day.[215] All humans are subject to these involuntary reactions as well as the consequences of error that can accompany presumptive thought. Humans prefer complete models of understanding of the world as opposed to new, incomplete, and complex concepts that require more time, energy, and resources to solve.[216] These shortcuts are a filtering process that our subconscious mind is conducting, and it summarizes available information from the past to adapt as circumstances dictate. If decision makers understand that this is happening, the ability to make informed decisions regarding a programmed "shortcut" comprehension, will increase the probability of success.[217] Despite the well documented psychological aspects of biases and quick response shortcuts affecting decision making, the U.S. military tends to err on the side of caution and avoidant behavior, as is defined by its already fundamentally bureaucratic status quo driving organization.[218] Although the process of avoidance can work to balance a bureaucratic system like the military, a reliance on intuition and shortcuts can leave gaps for adversaries to exploit.

5. Management and Regulatory Focus

Samuelson and Zeckhauser's work on "Status Quo Bias in Decision Making," suggests individuals are also susceptible to make decisions based on organizational

214 Dean Mobbs et al., "The Ecology of Human Fear: Survival Optimization and the Nervous System," *Frontiers in Neuroscience* 9 (2015): 1, https://doi.org/10.3389/fnins.2015.00055.

215 Mobbs et al., "The Ecology of Human Fear."

216 Kahneman, *Thinking, Fast and Slow*.

217 Kahneman.

218 Wilson, *Bureaucracy*.

pressures at the behest of retaining the status quo, effectively altering the outcome.[219] This brings us to a more nuanced studied aspect of prospect theory and human dynamics. Management and Regulatory Focus Theory plays to the promotion and prevention and loss/ gain of status quo regardless of logically framed, bias awareness decisions. Tory Higgins, issues that people are not just necessarily risk averse because of specific idiosyncrasies, but rather, individuals also make decisions in uncertainty juxtaposed to their relative position to the status quo within the organizations they belong.[220] Setting aside the individual biases and including a complex organizational work environment, an individual's aversion to risk comparative to their inclinations of promotion or prevention favors a trending towards the status quo.[221] Promotion here refers to individuals within an organization that view challenges and goals as opportunities to make progress. They are not as easily dissuaded from taking risks under uncertainty for higher yields of gains. These individuals are more concerned with advancement and growth.[222] Whereas prevention focused actors are predisposed to be leery of uncertainty and tend to focus on a status quo, security, and safety, therefore avoiding the backlash or repercussions of getting something wrong and not upsetting the natural order of things.[223]

With the U.S. military moving from kinetic operations to strategic competition below the level of armed conflict, leaders would make decisions based off their experience and what does not affect the status quo. In a given circumstance, how the leader perceives the information and based of his/her experience, could drastically change on the strategy implemented. For prevention focused actor(s), they are driven by advancement ideals in

219 William Samuelson and Richard Zeckhauser, "Status Quo Bias in Decision Making," *Journal of Risk and Uncertainty* 1, no. 1 (March 1988): 7–59, https://doi.org/10.1007/BF00055564.

220 James F. M. Cornwell and E. Tory Higgins, "Management and Regulatory Focus: Three New Domains of Application," *Rutgers Business Review* 2, no. 1 (Spring 2017): 142–49, https://rbr.business.rutgers.edu/sites/default/files/documents/rbr-020112.pdf.

221 Cornwell and Higgins.

222 Ellen Crowe and E. Tory Higgins, "Regulatory Focus and Strategic Inclinations: Promotion and Prevention in Decision-Making," *Organizational Behavior and Human Decision Processes* 69, no. 2 (February 1997): 117–32, https://doi.org/10.1006/obhd.1996.2675.

223 Heidi Grant, "The Hidden Danger of Being Risk-Averse," *Harvard Business Review*, July 2, 2013, https://hbr.org/2013/07/hidden-danger-of-being-risk-averse.

that wanting to progress in their careers, but this might not be possible if it does not align with the current status quo.[224]

6. Actions Speak Louder than Words

The cyber domain will eventually be integrated throughout the military regardless of the apprehension for change. The Joint Chiefs has acknowledged cyber as a domain in 2004, CYBERCOM was created in 2010, the DOD has adopted the Defend Forward and Persistent Engagement Strategy within cyber, and the world relies on digital technology for everything.[225] This era will bring with it the need for alternate ways of thinking, a different knowledge base, and a necessity for familiarity within the domain. Leaders must contend with the inevitability of this change and must not make decisions based off how they have always done it.

The expectation for all members of the military to become computer programmers or even understand the basic components of the cyber domain is an unrealistic expectation. Borghard, Montgomery, and Valeriano also suggest that merely growing the size of cyber military occupational specialties or recruiting subject matter experts within the field is insufficient as well to address the growing need of integration in the military.[226] According to the Cyberspace Solarium Commission, it is imperative for the success of future military operations to understand how this domain fits within warfare.[227]

Unfortunately, the programs that exist to provide this education are inconsistent and inadequate based on the assessed needs, but their necessity is certainly vital. The inadequacy was identified for the American public writ large within the Cyberspace Solarium Commission report, however, growth for a professional system in the military was limited to establishing Title 10 professors in cyber security and information

---

[224] Cornwell and Higgins, "Management and Regulatory Focus."

[225] Goldsmith, *The United States' Defend Forward Cyber Strategy*.

[226] Erica Borghard, Mark Montgomery, and Brandon Valeriano, "The Challenge of Educating the Military on Cyber Strategy," War on the Rocks, June 25, 2021, https://warontherocks.com/2021/06/the-challenge-of-educating-the-military-on-cyber-strategy/.

[227] Borghard, Montgomery, and Valeriano.

operations.[228] Borghard, Montgomery, and Valeriano, suggest that more is needed than just the implementation of academic professionals, and programs need to be developed to standardize military cyber educational institutions.[229] This will bridge the gaps in knowledge as a point of reference and understanding for the decision maker, which in turn will limit the potential for hidden bias. If the U.S. wishes to remain competitive within the cyber domain, specifically against the Chinese pacing threat, the U.S. is and has been failing to compete with educating its force in the technical arena by as much as ¼ that of Chinese levels as far back as 2012.[230] This should give pause for military leaders and policy makers to reflect on points of budgetary emphasis and allocation of resources.

Once the surface is scratched for providing a base of knowledge to the force, inserting this knowledge is the next step to reenforce concepts in service-centric and joint practical applications. Joint Chiefs Admiral Grady urges to move beyond the apprehensive nature and aversion to implementation, we need to be allowed to "test a little and learn a lot.[231] In theory, Grady's comments ring true for any use and implementation of systems, especially within a multidimensional atmosphere. A narrowing point of concern is that there is still a propensity to train and apply new systems in a very scoped and "stove pipe of excellence" type environment.[232] Programs and training for new systems meant to integrate and work collaboratively with others within the military have a tendency to shift to building internal infrastructures and operating procedures because those units are held responsible for their performance, pending if they are implemented at all.[233] This goes back to Grady's statement of failing a little.

---

228 King and Gallagher, *Cyberspace Solarium Commission Report*.

229 Borghard, Montgomery, and Valeriano, "The Challenge of Educating the Military on Cyber Strategy."

230 Cordesman, *Chinese Strategy and Military Forces in 2021*.

231 LaGrone, "Eliminating 'Risk Aversion' Key to Weapons Development."

232 Vergun, "Multi-Domain Battle Requires Non-Stovepipe Solutions, Say Leaders."

233 Stew Magnuson, "Stove-Piped Systems Alive and Well in the Military," *National Defense*, November 8, 2011, https://www.nationaldefensemagazine.org/articles/2011/11/8/stovepiped-systems-alive-and-well-in-the-military.

Knowledge is important but exercising the knowledge is just as important. Hoffman confers that the U.S. Army introduced Combat Training Centers (CTC) in the late 70's to address retrospective Vietnam Era operational problems in the hopes that "training as you fight" would better prepare and integrate the force for future wars.[234] In order to "train as you fight" efficiently and effectively, the DOD created training venues that would accurately depict the environment the military would operate in. Over the years, the CTCs supported and mirrored the needs of forces, and it was relatively conducive to reconstruct a kinetic environment in which to train. These environments reflected a counter insurgency area of operations for over 20 years but have failed to update with the modern needs of a technological driven battlespace. As a result, they are reducing funding and closing.[235] Yet, they issue that the CTCs reproduce an environment for Strategic Competition and Large-Scale Combat Operations.[236]

If the intent is to apply and test capabilities of war within an environment that reflects real world scenarios, providing much needed context, training, and familiarity to decision makers, the ability to fail a little and learn a lot is an impossibility if the environment doesn't truly reflect reality. There is value in developing capabilities within organizations, but if those organizations are not subjected to the replicated realities of war time integration, interdependence, and interoperability in dynamic environments, then the ability for decision makers to have points of reference and relative understanding of capabilities becomes diminished.

E. CONCLUSION

Understanding the deficiencies of current military thought and process will assist the U.S. in preparing for the wars of the future. Prospect theory and its accompanied subsidiaries of thought are just a few ways that we have discussed that can further the

234 Jon T. Hoffman, ed., *A History of Innovation: U.S. Army Adaptation in War and Peace* (Washington, DC: Center of Military History, 2009), https://history.army.mil/html/books/innovation/History_of_Innovation.pdf.

235 Thomas Spoehr, "Biden's First Defense Budget Batters the Army," Heritage Foundation Defense, June 7, 2021, https://www.heritage.org/defense/commentary/bidens-first-defense-budget-batters-the-army.

236 Elgin, "How the Army Is (NOT) Preparing for the Next War."

efforts of U.S. decision makers while attempting to construct new ways of implementing and adapting to cyber in warfare. There is value in introspectively looking at decision making which can directly affect an individual's apprehension or confidence towards making decisions under uncertainty. The chapter briefly scratched the surface as to how organizations can have detrimental impacts on these decisions despite consequences to keep the status quo. Finally, the chapter addressed the training venues that should be promoting integrative aspects for real world implementation. The following chapter will conclude the thesis with discussing how the U.S. can operate within these limitations and provide some recommendations on the changes that can be made in order to maintain a competitive edge against adversaries.

VI. HOW DO WE COMPETE WITHIN THE LIMITATIONS?

A typical U.S. response to any form of problem is to respond in kind with the appropriate component of the DIMEFL construct. However, as the systems dynamic model attempts to show, throwing more money at the problem is and cannot be the answer. If the current projections remain true of, the Chinese economy surpassing the U.S. economy by 2030 or 2033, and the goal of the PRC is to surpass the U.S. military by 2035, then money cannot be the answer. There needs to be another change in order to compete effectively and efficiently against the PRC threats.

In 2015, the PLA's SSF achieved operational status, and fused both space, cyber, and civilian technologies, as shown in the task organization. This reorganization of capabilities under one command is an attempt to streamline processes and allow for faster actions within the space and cyber domain. As discussed in Chapter 3, the United States may currently be the number 1 authority in cyber, but the PRC are close at number 2, and not only are they close, but they potentially have a much larger capacity capability just due to sheer numbers of personnel.

Within the DOD, and the U.S. Government at large, there are bureaucratic and cultural limitations. To potentially conduct a cyber-operation, a request needs to be made multiple months in advance and be screened at every decision maker level, and then sent to other agencies to ensure there are no operations or intelligence gathering that they made be doing that would be affected by an action. This process is not quick, fast, or conducive to operating in strategic competition against the pacing threat and if continued, then China will obtain domain supremacy. However, this does not have to be the case. As discussed within the Bureaucratic Limitations chapter, the DOD does possess the authority to conduct a wealth of cyber activities. However, the decisions to use these authorities or request capabilities are typically clouded within a cultural limitation of risk aversion or due to a lack of education and clarity on the behalf of the planners.

A. RECOMMENDATIONS

This thesis seeks to provide recommendations to the following question: "How can the Department of Defense adjust its positions on Cyber Titles, Authorities, Permissions, and risk aversion in leadership to maintain a competitive edge against the threat of the People's Republic of China's Strategic Support Force in the cyber domain?" Based off the research, and analyzing the problem, this thesis makes the recommendations in the following three areas for continued competition with China within the cyber domain:

1. Education—provide and create education on the capabilities, effects, and planning processes for cyber operations to Task Force Commanders' staffs and above. This will facilitate the staffs being able to present effective and dynamic courses of actions to the decision makers based off the requisite knowledge of cyber capabilities and the effects looking to be achieved.
2. ROEs—push permissions along with the approval to conduct cyber operations down to Task Force Commanders to operate more dynamically and at a faster operation tempo, which will put the adversary on the defensive rather than the offensive.
3. Training—provide training exercises, evolutions that will allow cyber tactical teams to practice their Mission Essential Tasks Lists either offensive or defensive cyber in a closed network directly tied to a larger exercise for a future supported commander.

These recommendations will be discussed in more detail in the following sections.

1. Education

Operations officers, primary staff officers, and detachment leads, are typically the individuals who are creating, designing, and developing the courses of actions prior to execution. These planning team "should establish a team of experts to support the planning process."[237] Within the JP 5-0 Joint Planning publication, it states that "commanders own the planning process and must continuously participate in planning to provide guidance

[237] Joint Chiefs of Staff, *Joint Planning*, III–1.

and expertise. The planner develops viable solutions to a problem presented in strategic or commander guidance."[238] It is the responsibility of the planner to develop a course of action, within the commander's planning guidance and their overall operational approach to solving the problem and ultimately present that course of action to the commander for approval or further guidance. If the planners and the commanders, do not fully understand the capabilities and effects that cyber can have at the tactical/operational level, then they cannot plan for it accordingly.

As professional warfighters, it is mandatory that all military officers and senior enlisted educate themselves to meet the challenges of future threats and challenges. Looking at the mission statements of the Marine Corps University and the Army War College, both educational entities state within their mission statements that their purpose is to "prepare leaders to meet current and future security challenges," and to "educate and develop leaders for service at the strategic level."[239] With these mission statements, it is imperative that in order to understand and meet future security challenges, the future planners, and ultimately commanders, need to understand the capabilities and effects that the military possess, in this case cyber. This thesis recommends that at least one of two courses of action be implemented:

1. Create an additional week or two at the resident schools that revolves specifically around cyber planning, cyber capabilities, cyber effects at least at the secret level. This should be provided by the services' cyber commands under mobile training teams. For example, Marine Forces Cyber develops, creates, and delivers a week or two long period of instruction to Marine Corps University students on these areas.

2. Send O-6 staffs on temporary additional duty to service component cyber command, or Naval Postgraduate School, for TS/S education on cyber that

238 Joint Chiefs of Staff, III–1.

239 Marine Corps University, "Mission and Vision Statement," accessed November 14, 2022, https://www.usmcu.edu/About-MCU/Mission-and-Vision-Statement/; Army War College, "About the U.S. Army War College," U.S. Army War College, accessed November 14, 2022, https://www.armywarcollege.edu/overview.cfm.

again consists of planning, capabilities, and effects so they can properly educate and advise their commanders and decision-makers.

2. Rules of Engagement

Doctrine is the backbone of U.S. military operations, providing guidance through historical accounts, knowledge, and application. Army ADP 1–01 Doctrine Primer states that doctrine are "fundamental principles, with supporting tactics, techniques, procedures, and terms and symbols, used for the conduct of operations and as a guide for actions of operating forces, and elements of the institutional force that directly support operations in support of national objectives."[240] These professional bodies of work provide the foundation for the military to fight and win our nations battles. On the other hand, rules of engagement dictate the who, what, when, where, and how U.S. force will be used to win those battles. As suggested throughout this paper, the cyber domain presents a unique environment where the surface of experience is just being scratched in obtaining precedence of operations. Authorities, permissions, and potential legal ramifications stand as barriers for those decision makers that are unfamiliar with implementation and integration for effects to be generated. Although doctrine is continually being updated and revised for this domain, the history, knowledge, and understanding is relatively new territory for a large percentage of the services and policy makers.[241] To better assist the services at large, defining left and right limits for rules of engagement in this domain will be paramount to the successful usage and efficient application of U.S. resources.

To increase the operational tempo and response within the INDO-PACOM AOR, this thesis recommends the following for training changes:

1. Develop ROEs along with affiliated delegation of permissions for TF commanders fixated around the three levels of war within their AO.

[240] Department of the Army, *Doctrine Primer*, ADP 1–01 (Washington, DC: Department of the Army, 2019), Glossary-1, https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18138_ADP%201-01%20FINAL%20WEB.pdf.

[241] Defranco et al., "Emerging Technologies for Disruptive Effects."

Continued development and creation of echelon level effects for rules of engagement will help bridge the gap in slow acceptance as well as building the reflexive responses that are incumbent in warfare. The complexity that exists for making decision regarding the use of cyber enabled information operations lends to the apprehension of decision makers exploring options. Further defined boundaries that are distinctive to the 3 levels of warfare will also help engrain guiding principles that assist commanders and

As U.S. services continue to develop tactical cyber units to help fill the gap between CYBERCOM strategic level cyber operations and tactical implementation, further scoped ROEs will help assist military commanders in units outside of the direct chain of control of CYBERCOM to identify what assets they have at their organic disposal that can be applied to given circumstance. Just like kinetic ROEs have historical usage in training and in conflict, defined guidelines will provide commanders the ability to recognize, incorporate, and evaluate effects, which in turn matures familiarity and comfortability. The lack of education, experience, or understanding prevents effective and efficient operations.

While there is no significant cost associated with developing ROEs, ROEs themselves can help in outlining where funding could be better allocated. Once military commanders become more acquainted with the effects achievable at their level, demand will increase due to reduced risk assessments associated with understanding the boundaries of application and repetition. Therefore, you are making decisions regarding effects to achieve on the enemy, not the broad interpretation of a cyber action itself. Understanding the effects and capabilities of cyber tactics, will facilitate a better management of the capability and allow for commanders and staff to plan for them effectively and efficiently. With this knowledge base, theatre commanders will be able to delegate the ROEs down to task force commanders, because they understand the full spectrum of the capability that they request.

3. Training

The DOD issues pre-deployment and theater entry requirements for deploying units to ensure individual, staff, and collective training is managed, confirming both lethality

and capability of conducting their job in support of national defense.[242] Training venues supporting validation or certification of U.S. forces need to reflect real world circumstances to support readiness and developing ROEs for cyber enabled effects within joint operations. If sites cannot reproduce the environment needed, then further developing rules of engagement could be considered just another doctrinal document in a sea of documents that U.S. military services must traverse to operate effectively together. This separation will generate little to no hands-on operational experience and most certainly would not exemplify the train as you fight mentality. Antiquated, poorly emulated, and stove piped training facilities will only stagnate the transitional integration of technologies, along with insufficiently preparing forces of adversarial cyber enabled effects on the battlespace.

To increase the state of readiness for deploying units, this thesis recommends the following for training changes:

1. Increase the pace that U.S. training venues reflect real world peer competitor environments and fully integrate cyber enabled capabilities to evaluate and improve interoperability of U.S. resources.

Venues must provide the capacity to apply cyber enabled effects within joint operations and outside of domain specific seclusion. Hands on experience and lessons learned from fully integrated facilities will increase familiarity and understanding of cyber enabled effects, which will encourage decision makers to expand comfort zones in addition to options. The reflection of a peer environment will also allow for practitioners to identify bottle necks of operations in addition to negotiating the layered legal aspects of emerging technological capabilities as they apply to rules of engagement.[243]

Linked to the increased pace would be the need to address and review current programs of record. As Admiral Grady stated in his 2021 confirmation hearing, "test a little, learn a lot," can only be accomplished if leaders push the boundaries of

[242] Department of Defense, *Emerging Technologies for Disruptive Effects*, DOD Instruction 1322.32 (Washington, DC: Department of Defense, 2021), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/132232p.PDF?ver=2J-BNK7wsId2ecJgCKtlHw%3D%3D.

[243] C. Robert Kehler, Herbert Lin, and Michael Sulmeyer, "Rules of Engagement for Cyberspace Operations: A View from the USA," *Journal of Cybersecurity* 3, no. 1 (2017): 69–80, https://doi.org/10.1093/cybsec/tyx003.

comfortability and the comfortability will be put to the test when challenging programs and systems that the services have relied on for quite some time.[244] Increasing the pace of change for training facilities should also incorporate reviewing programs of record to expedite the real world reflection needed to not only test new weapon systems, but also reflect how the services integrate their use.

B. CONCLUSION

It is no easy task to change organizational culture. Though risk averse mindsets will likely continue to impact decision-makers, these recommendations focus on concrete behavioral changes that may help address this indirectly. But first and foremost, they are designed to help quicken the operational tempo of fleet forces and put the PRC and other competitors back on the defensive. To accomplish this, permissions should fall to Task Force Commanders.

Failure to address these self-imposed bureaucratic and cultural obstacles hinder a whole joint force response in deterring the PRC. In a planning cell, two personnel may not be able to plan properly because of clearances and read ins into certain classifications. However, with the proper reallocation of funding, into education, resources and training, the U.S. can still maintain the edge over the adversary.

1. Areas for Further Research

This thesis has provided recommendations to DOD leadership for potential areas that the U.S. may be able to pick up operational tempo against the PRC within cyberspace. The topics listed below require further research and development in order to continue to build upon this discussion:

- Develop a cyber specific curriculum for Task Force staffs covering the following areas: planning, capabilities, targeting process, and effects.

[244] LaGrone, "Eliminating 'Risk Aversion' Key to Weapons Development."

- Analyze O4/O5 grade professional military education curriculum for feasibility of supporting CYBERCOM mobile training teams to instruct on cyber specific curriculum.
- Research the feasibility of developing closed secure networks utilizing virtual machines to allow offensive and defensive cyber operations integrated within either a joint exercise or in a deployment certification exercise.

APPENDIX: SYSTEM DYNAMICS VARIABLE TABLES

Table 6. Description of the Model's United States Elements

Element	Description	Formula
Converter "US GDP Growth Rate"	US GDP growth rate as of 2020. This rate will be held constant and applied into flow of the U.S. Growing Economy.	
Converter "US Defense Spending Rate"	Percentage of the GDP that is applied directly to the Defense Budget.	
Converter "US Defense Budget"	The amount the United States is spending towards defense.	"US GDP" * "US Defense Spending Rate"
Converter "US Cyber Baseline %"	The percentage that the U.S. is taking from the U.S. Defense Budget and applying it directly to Cyber.	
Converter "% of U.S. Defense Budget for Cyber"	Calculation of the final percentage of the defense spending percentage and how the impact of PRC successful signaling from cyber-attacks.	"US Cyber Baseline %" * "Impact of PRC Success"
Converter "Annual # of U.S. Attacks"	Sets the distribution of annual cyber-attacks in random variation along a bell curve.	Normal distribution with a mean of 1000 and a standard deviation of 500: NORMAL (1000,500)
Converter "Cost of Cyber Attack"	Sets the cost of building a cyber capability during a given time step at random.	Random distribution with a minimum of $10,000 U.S. dollars and a maximum of $500,000 U.S. dollars: RANDOM (10000,500000)
Converter "US Intent Score"	A score calculated utilizing the Harvard Kennedy Political Studies School (Harvard Belfer National Cyber Power Index of 2020 (HBNCPI),) This score determines the countries intentions on utilizing a cyber capability.	
Converter "US	A score calculated utilizing the Harvard Kennedy Political Studies School (Harvard	

Element	Description	Formula
Capability Score"	Belfer National Cyber Power Index of 2020 (HBNCPI),) This score determines the countries capability in cyber.	
Converter "US Cyber Power Index"	A score calculated utilizing Harvard Kennedy Political Studies School (Harvard Belfer National Cyber Power Index of 2020 (HBNCPI),) This is the overall score given to a country determining its cyber strength.	
Converter "US Prob of Success"	Sets the probability that a cyber-attack will be successful in a binomial distribution. Rationale for using the Cyber Power Index as the percentage for success is the higher the cyber power index is for a given country, it can be inferred that they will have more success in attacking another country.	Binomial distribution using the U.S. initiated attacks as the trials and using the Cyber Power Index as the probability of success: BINOMIAL ("US Initiated Attacks, "US Cyber Power Index")
Converter "US Annual Successful Attacks"	Captures the total number of successful attacks in a time step (one year) based off the initiated attacks and probability of success.	
Converter "US Signaling Input"	Determines the percentage of influence that after a certain number of successful attacks, what the strength of that action will "signal" to its adversary.	This is a graphical interface with a min of 100 attacks up to 1000 attacks. As the number approaches 1000 or surpasses, the signal input increases.
Converter "US Signaling / Deterrence / Coercion"	Captures the output of the graphical interface of the "US Signaling Input" converter in each time step.	
Converter "US Spending"	Captures in each time step what the United States is spending on cyber-attacks based off the random distribution of the cost of cyber-attack and the number of annual attacks.	"Cost of Cyber Attack" * "Annual # of U.S. Attacks"
Flow "US Growing Economy"	Calculates the annual Gross Domestic Product and flows to the U.S. GDP stock.	"US GDP" * (1 + "US GDP Growth Rate")

Element	Description	Formula
Flow "US Annual GDP"	Captures the annual Gross Domestic Product for the United States, this is the outflow of the U.S. GDP Stock.	
Flow "Annual U.S. Cyber Expenditure"	Captures the amount of money U.S. spends on cyber from the defense budget. This flows into the U.S. capacity stock.	PULSE ("% of U.S. Defense Budget for Cyber" * "US Defense Budget"
Flow "US Expenditure"	Captures the total expenditure of the U.S. This outflow is affected by the annual number of U.S. attacks, the cost of conducting a cyber-attack, and the PRC signaling.	("Annual # of U.S. Attacks" + "Annual # of U.S. Attacks" * "PRC Signaling / Deterrence / Coercion)) * "Cost of Cyber Attack"
Flow "US Cyber Action"	Captures the total number of Cyber activities. This flows into the U.S. Cyber Attack stock. This flow is affected by the annual number of U.S. attacks, and the PRC signaling.	("Annual # of U.S. Attacks" + "Annual # of U.S. Attacks" * "PRC Signaling / Deterrence / Coercion))
Flow "US Initiated Attacks"	This outflow captures the total number of U.S. initiated attacks and flows into the stock U.S. total attacks. The total number of attacks is affected by the Converters of the U.S. intent score and the U.S. capability score.	HISTORY ("US Cyber-attack, TIME) * "US capability score" * "US intent"
Stock "US GDP"	Captures the U.S. Gross Domestic Product. Inflow: U.S. GDP Outflow: U.S. Annual GDP	
Stock "US Capacity"	Captures the U.S. Capacity for cyber based off the amount of money spent on cyber. Inflow: Annual U.S. Cyber Expenditure Outflow: U.S. Expenditure	
Stock "US Cyber Action Spending Over Time"	Captures the amount of money spent in total on cyber actions. Inflow: U.S. Expenditure Outflow: N/a	
Stock "US Cyber Attacks"	Captures the number of cyber-attacks in a given time step Inflow: U.S. Cyber Action Outflow: U.S. Initiated Attacks	
Stock "US Total Attacks"	Captures the total amount of attacks over the given time period. Inflow: U.S. Initiated Attacks	

Element	Description	Formula
	Outflow: N/a	
Stock "US Total Successful Attacks (Over Time Period)"	Captures the total amount of successful attacks over the simulation or total time covered. Inflow: Flows from Converter U.S. Annual Successful Attack Outflow: N/a	

Table 7. Description of the Model's PRC Elements

Element	Description	Formula
Converter "PRC GDP Growth Rate"	PRC GDP growth rate as of 2020. This rate will be held constant and applied into flow of the PRC Growing Economy.	
Converter "PRC Defense Spending Rate"	Percentage of the GDP that is applied directly to the Defense Budget.	
Converter "PRC Defense Budget"	The amount the PRC is spending towards defense.	"PRC GDP" * "PRC Defense Spending Rate"
Converter "PRC Cyber Baseline %"	The percentage that the PRC is taking from the PRC Defense Budget and applying it directly to Cyber.	
Converter "% of PRC Defense Budget for Cyber"	Calculation of the final percentage of the defense spending percentage and how the impact of PRC successful signaling from cyber-attacks.	"PRC Cyber Baseline %" * "Impact of U.S. Success"
Converter "Annual # of PRC Attacks"	Sets the distribution of annual cyber-attacks in random variation along a bell curve.	Normal distribution with a mean of 1000 and a standard deviation of 500: NORMAL (1000,500)
Converter "Cost of Cyber Attack"	Sets the cost of building a cyber capability during a given time step at random.	Random distribution with a minimum of $10,000 U.S. dollars and a maximum of $500,000 U.S. dollars: RANDOM (10000,500000)

Element	Description	Formula
Converter "PRC Intent Score"	A score calculated utilizing the Harvard Kennedy Political Studies School (Harvard Belfer National Cyber Power Index of 2020 (HBNCPI),) This score determines the countries intentions on utilizing a cyber capability.	
Converter "PRC Capability Score"	A score calculated utilizing the Harvard Kennedy Political Studies School (Harvard Belfer National Cyber Power Index of 2020 (HBNCPI),) This score determines the countries capability in cyber.	
Converter "PRC Cyber Power Index"	A score calculated utilizing the Harvard Kennedy Political Studies School (Harvard Belfer National Cyber Power Index of 2020 (HBNCPI),) This is the overall score given to a country determining its cyber strength.	
Converter "PRC Prob of Success"	Sets the probability that a cyber-attack will be successful in a binomial distribution. Rationale for using the Cyber Power Index as the percentage for success is the higher the cyber power index is for a given country, it can be inferred that they will have more success in attacking another country.	Binomial distribution using the PRC initiated attacks as the trials and using the Cyber Power Index as the probability of success: BINOMIAL ("PRC Initiated Attacks, "PRC Cyber Power Index")
Converter "PRC Annual Successful Attacks"	Captures the total number of successful attacks in a time step (one year) based off of the initiated attacks and probability of success.	
Converter "PRC Signaling Input"	Determines the percentage of influence that after a certain number of successful attacks, what the strength of that action will "signal" to its adversary.	This is a graphical interface with a min of 100 attacks up to 1000 attacks. As the number approaches 1000 or surpasses, the signal input increases.
Converter "PRC Signaling /	Captures the output of the graphical interface of the "PRC Signaling Input" converter in each time step.	

Element	Description	Formula
Deterrence / Coercion"		
Converter "PRC Spending"	Captures in each time step what the PRC is spending on cyber-attacks based off the random distribution of the cost of cyber-attack and the number of annual attacks.	"Cost of Cyber Attack" * "Annual # of PRC Attacks"
Flow "PRC Growing Economy"	Calculates the annual Gross Domestic Product and flows to the PRC GDP stock.	"PRC GDP" * (1 + "PRC GDP Growth Rate")
Flow "PRC Annual GDP"	Captures the annual Gross Domestic Product for the PRC, this is the outflow of the PRC GDP Stock.	
Flow "Annual PRC Cyber Expenditure"	Captures the amount of money PRC spends on cyber from the defense budget. This flows into the PRC capacity stock.	PULSE ("% of PRC Defense Budget for Cyber" * "PRC Defense Budget"
Flow "PRC Expenditure"	Captures the total expenditure of the PRC. This outflow is affected by the annual number of PRC attacks, the cost of conducting a cyber-attack, and the U.S. signaling.	("Annual # of PRC Attacks" + "Annual # of PRC Attacks" * "US Signaling / Deterrence / Coercion)) * "Cost of Cyber Attack"
Flow PRC Cyber Action"	Captures the total number of Cyber activities. This flows into the PRC Cyber Attack stock. This flow is affected by the annual number of PRC attacks, and the U.S. signaling.	("Annual # of PRC Attacks" + "Annual # of PRC Attacks" * "US Signaling / Deterrence / Coercion))
Flow "PRC Initiated Attacks"	This outflow captures the total number of PRC initiated attacks and flows into the stock PRC total attacks. The total number of attacks is affected by the Converters of the PRC intent score and the PRC capability score.	HISTORY ("PRC Cyber attack, TIME) * "PRC capability score" * "PRC intent"
Stock "PRC GDP"	Captures the PRC Gross Domestic Product. Inflow: PRC GDP Outflow: PRC Annual GDP	
Stock "PRC Capacity"	Captures the PRC Capacity for cyber based off the amount of money spent on cyber. Inflow: Annual PRC Cyber Expenditure Outflow: PRC Expenditure	
Stock	Captures the amount of money spent in total on cyber actions.	

Element	Description	Formula
"PRC Cyber Action Spending Over Time"	Inflow: PRC Expenditure Outflow: N/a	
Stock "PRC Cyber Attacks"	Captures the number of cyber-attacks in each time step Inflow: PRC Cyber Action Outflow: PRC Initiated Attacks	
Stock "PRC Total Attacks"	Captures the total amount of attacks over the given time period. Inflow: PRC Initiated Attacks Outflow: N/a	
Stock "PRC Total Successful Attacks (Over Time Period)"	Captures the total amount of successful attacks over the simulation or total time covered. Inflow: Flows from Converter PRC Annual Successful Attack Outflow: N/a	

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Applegate, Scott D. "The Principle of Maneuver in Cyber Operations." In *International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, and K. Ziolkowski, 183–95. Tallinn: NATO CCD COE Publications, 2012.

Army War College. "About the U.S. Army War College." U.S. Army War College. Accessed November 14, 2022. https://www.armywarcollege.edu/overview.cfm.

Arquilla, John. *Bitskrieg: The New Challenge of Cyberwarfare*. Cambridge, UK: Polity Press, 2021.

Atsmon, Yuval, David Chinn, and Sven Smit. "Lessons from the Generals: Decisive Action amid the Chaos of Crisis." Our Insights, May 18, 2020. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/lessons-from-the-generals-decisive-action-amid-the-chaos-of-crisis.

Australian Strategic Policy Institute. "Information Engineering University." Chinese Defence Universities Tracker, May 13, 2021. https://unitracker.aspi.org.au/universities/information-engineering-university-2.

Barno, David, and Nora Bensahel. "Falling into the Adaptation Gap." War on the Rocks, September 29, 2020. https://warontherocks.com/2020/09/falling-into-the-adaptation-gap/.

Bell, William. "Risk Aversion in the U.S. Army Officer Corps." In *Joint Services Conference on Professional Ethics: The Impact of Policies on Organizational Values and Culture*, 1999. http://isme.tamu.edu/JSCOPE99/Bell99-2.html.

Biden, Jr., Joseph R. *Interim National Security Strategic Guidance*. Washington, DC: White House, 2021. https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.

———. *National Security Strategy*. Washington, DC: White House, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

Bing, Chris. "How China's Cyber Command Is Being Built to Supersede Its U.S. Military Counterpart." CyberScoop, June 22, 2017. https://www.cyberscoop.com/china-ssf-cyber-command-strategic-support-force-pla-nsa-dod/.

Borghard, Erica, Mark Montgomery, and Brandon Valeriano. "The Challenge of Educating the Military on Cyber Strategy." War on the Rocks, June 25, 2021. https://warontherocks.com/2021/06/the-challenge-of-educating-the-military-on-cyber-strategy/.

Briggs, R. A. "Normative Theories of Rational Choice: Expected Utility." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Fall 2019. Stanford, CA: Metaphysics Research Lab, Stanford University, 2019. https://plato.stanford.edu/archives/fall2019/entries/rationality-normative-utility/.

Broad, William J., John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *New York Times*, January 15, 2011, sec. World. https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Busch, May. "Why Being with Like-Minded People Is Dangerous." May Busch, December 6, 2015. https://maybusch.com/why-being-with-like-minded-people-is-dangerous/.

Chatzk, Andrew, and James McBride. "China's Massive Belt and Road Initiative." Council on Foreign Relations Backgrounder, January 28, 2020. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

Chayes, Abram, William Fisher, Morton Horwitz, Frank Michelman, Martha Minow, Charles Nesson, and Todd Rakoff. "Law and Economics: Risk." The Bridge. Accessed August 5, 2022. https://cyber.harvard.edu/bridge/LawEconomics/risk.htm.

Cherry, Kendra. "The 6 Stages of Behavior Change." Verywell Mind, July 28, 2021. https://www.verywellmind.com/the-stages-of-change-2794868.

Collins, Liam. "Russia Gives Lessons in Electronic Warfare." Association of the United States Army, July 26, 2018. https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare.

Congress. House. Permanent Select Committee on Intelligence. "Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and Advertisements." U.S. House of Representatives Permanent Select Committee on Intelligence, February 16, 2018. https://intelligence.house.gov/social-media-content/.

Cooper, Zack. "Bad Idea: 'Great Power Competition' Terminology." Defense360, December 1, 2020. https://defense360.csis.org/bad-idea-great-power-competition-terminology/.

Cordesman, Anthony H. *Chinese Strategy and Military Forces in 2021*. Washington, DC: Center for Strategic & International Studies, 2021. https://www.csis.org/analysis/updated-report-chinese-strategy-and-military-forces-2021.

———. *Making America Great? Global Perceptions of China, Russia, and the United States: The International Scorecard*. Washington, DC: Center for Strategic & International Studies, 2021. https://www.csis.org/analysis/making-america-great-global-perceptions-china-russia-and-united-states-international.

Cornwell, James F. M., and E. Tory Higgins. "Management and Regulatory Focus: Three New Domains of Application." *Rutgers Business Review* 2, no. 1 (Spring 2017): 142–49. https://rbr.business.rutgers.edu/sites/default/files/documents/rbr-020112.pdf.

Costello, John, and Joe McReynolds. *China's Strategic Support Force: A Force for a New Era*. China Strategic Perspectives, No. 13. Washington, DC: National Defense University, 2018. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf.

Crowe, Ellen, and E. Tory Higgins. "Regulatory Focus and Strategic Inclinations: Promotion and Prevention in Decision-Making." *Organizational Behavior and Human Decision Processes* 69, no. 2 (February 1997): 117–32. https://doi.org/10.1006/obhd.1996.2675.

Defranco, Joseph, Diane Dieuliis, L.R. Bremseth, J.J. Snow, and James Giordano. "Emerging Technologies for Disruptive Effects in Non-Kinetic Engagements." *Homeland Defense & Security Information Analysis Center* 6, no. 2 (Summer 2019). https://hdiac.org/articles/emerging-technologies-for-disruptive-effects-in-non-kinetic-engagements/.

Department of Defense. *Emerging Technologies for Disruptive Effects*. DOD Instruction 1322.32. Washington, DC: Department of Defense, 2021. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/132232p.PDF?ver=2J-BNK7wsId2ecJgCKtlHw%3D%3D.

———. *Quadrennial Defense Review Report*. Washington, DC: Department of Defense, 2001. https://dod.defense.gov/Portals/1/features/defenseReviews/QDR/qdr2001.pdf.

———. *Summary: Department of Defense Cyber Strategy 2018*. Washington, DC: Department of Defense, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Department of the Army. *Doctrine Primer*. ADP 1–01. Washington, DC: Department of the Army, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18138_ADP%201-01%20FINAL%20WEB.pdf.

———. *Mission Command: Command and Control of Army Forces*. ADP 6–0. Washington, DC: Department of the Army, 2019. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN18314-ADP_6-0-000-WEB-3.pdf.

DeVine, Michael E. *Covert Action and Clandestine Activities of the Intelligence Community: Selected Congressional Notification Requirements in Brief*. CRS Report No. R45191. Washington, DC: Congressional Research Service, 2019. https://sgp.fas.org/crs/intel/R45191.pdf.

DeWees, Bradley, Terry C. Pierce, Ervin J. Rokke, and Anthony Tingle. "Toward a Unified Metric of Kinetic and Nonkinetic Actions: Meaning Fields and the Arc of E." *Joint Force Quarterly, JFQ*, no. 85 (2017): 16–21. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-85/jfq-85_16-21_DeWees-et-al.pdf.

Dilanian, Ken, and Courtney Kube. "Biden given Options for Unprecedented Cyberattacks against Russia." NBC News, February 24, 2022. https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558.

Dobbins, James, Howard J. Shatz, and Ali Wyne. *Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue: Different Challenges, Different Responses*. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/perspectives/PE310.html.

Donnelly, John, and Gopal Ratnam. "US Is Woefully Unprepared for Cyber-Warfare." S&P Global Market Intelligence, June 26, 2019. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/us-is-woefully-unprepared-for-cyber-warfare-52560026.

Dou, Eva. "Documents Link Huawei to China's Surveillance Programs." *Washington Post*, December 14, 2021, sec. Asia. https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.

Doyle, David, and Aaron Coombs. "How Has the Joint Readiness Training Center Changed to Adapt to Large-Scale Combat Operations?" *Military Review* 98, no. 5 (September 2018): 72–79. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2018/Doyle-and-Coombs/.

Elgin, Katherine Kjellström. "How the Army Is (NOT) Preparing for the Next War." *War Room* (blog), September 25, 2019. https://warroom.armywarcollege.edu/articles/the-next-war/.

Finkle, Jim. "Researchers Say Stuxnet Was Deployed against Iran in 2007." *Technology News*, February 26, 2013. https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226.

Freedberg, Jr, Sydney J. "Let Leaders Off the Electronic Leash: CSA Milley." Breaking Defense, May 5, 2017. https://breakingdefense.com/2017/05/let-leaders-off-the-electronic-leash-csa-milley/.

Gilbert, David. "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog." *International Business Times*, February 6, 2014, sec. CyberSecurity. https://www.ibtimes.co.uk/cost-developing-cyber-weapons-drops-100m-stuxnet-10k-icefrog-1435451.

Giocoli, Nicola. "The 'True' Hypothesis of Daniel Bernoulli: What Did the Marginalists Really Know?" *History of Economic Ideas* 6, no. 2 (1998): 7–43. https://www.jstor.org/stable/23722513.

Goldsmith, Jack. *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*. New York: Oxford University Press, 2022.

Grant, Heidi. "The Hidden Danger of Being Risk-Averse." *Harvard Business Review*, July 2, 2013. https://hbr.org/2013/07/hidden-danger-of-being-risk-averse.

Griffiths, Zachary. "In Defense of the Military Bureaucrat." American Politics. Modern War Institute, April 4, 2018. https://mwi.usma.edu/defense-military-bureaucrat/.

Hartley, Jean F. "Ideology and Organizational Behavior." *International Studies of Management & Organization* 13, no. 3 (1983): 7–34. https://www.jstor.org/stable/40396913.

Heath, Timothy R., Kristen Gunness, and Cortez A. Cooper, III. *The PLA and China's Rejuvenation: National Security and Military Strategies, Deterrence Concepts, and Combat Capabilities*. Santa Monica, CA: RAND Corporation, 2016. https://www.rand.org/pubs/research_reports/RR1402.html.

Hoffman, Jon T., ed. *A History of Innovation: U.S. Army Adaptation in War and Peace*. Washington, DC: Center of Military History, 2009. https://history.army.mil/html/books/innovation/History_of_Innovation.pdf.

Holstein, William J. *The New Art of War: China's Deep Strategy Inside the United States*. New York: Brick Tower Press, 2019.

H.R. *Operating in the Digital Domain: Organizing the Military Departments for Cyber Operation: Hearing Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the Committee on Armed Services House of Representatives*, House of Representatives, 111th Cong. 2, 2009. https://www.govinfo.gov/content/pkg/CHRG-111hhrg62398/pdf/CHRG-111hhrg62398.pdf.

Huxley, Tim, and William Choong, eds. "China's Cyber Power in a New Era." In *Asia-Pacific Regional Security Assessment 2019: Key Developments and Trends*, 77–90. London: International Institute for Strategic Studies, 2019. https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5.

Janis, Irving L. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*. 2nd ed. Boston: Houghton Mifflin, 1982. http://archive.org/details/groupthinkpsycho00jani.

Jennings, Ralph. "China's Economy Could Overtake U.S. Economy by 2030." VOA, January 4, 2022. https://www.voanews.com/a/chinas-economy-could-overtake-us-economy-by-2030/6380892.html.

Joint Chiefs of Staff. *Information in Joint Operations*. Joint Publication 3-04. Washington, DC: Joint Chiefs of Staff, 2022.

———. *Joint Planning*. Joint Publication 5-0. Washington, DC: Joint Chiefs of Staff, 2020. https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/5-0-Planning-Series/.

———. *Joint Targeting*. Joint Publication 3-60. Washington, DC: Joint Chiefs of Staff, 2013. https://www.justsecurity.org/wp-content/uploads/2015/06/Joint_Chiefs-Joint_Targeting_20130131.pdf.

———. *Legal Support*. Joint Publication 3-84. Washington, DC: Joint Chiefs of Staff, 2016. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_84.pdf.

———. *Legal Support to Military Operations*. Joint Publication 1-04. Washington, DC: Joint Chiefs of Staff, 2016. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_04.pdf.

Joint Committee on the Organization of Congress. "Congressional Precedents and Powers." Organization of the Congress: Final Report of the Joint Committee on the Organization of Congress, December 1993. https://archives-democrats-rules.house.gov/Archives/jcoc2ar.htm.

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Kahneman, Daniel, and Amos Tversky. "Prospect Theory: An Analysis of Decision under Risk." *Econometrica* 47, no. 2 (1979): 263–91. https://doi.org/10.2307/1914185.

Kaminska, Monica. "Risk Aversion Is at the Heart of the Cyber Response Dilemma." *Net Politics* (blog), March 31, 2021. https://www.cfr.org/blog/risk-aversion-heart-cyber-response-dilemma.

Kandrík, Matej. "The Case against the Concept of Great Power Competition." The Strategy Bridge, June 30, 2021. https://thestrategybridge.org/the-bridge/2021/6/30/the-case-against-the-concept-of-great-power-competition.

Kane, J. Robert. "Covert Action, Military Operations and the DOD–CIA Debate." *Real Clear Defense*, August 9, 2018. https://www.realcleardefense.com/articles/2018/08/09/covert_action_military_operations_and_the_dodcia_debate_113701.html.

Kania, Elsa B., and John K. Costello. "The Strategic Support Force and the Future of Chinese Information Operations." *Cyber Defense Review* 3, no. 1 (Spring 2018): 105–21. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1589125/the-strategic-support-force-and-the-future-of-chinese-information-operations/.

Kerner, Sean Michael. "What Is the Great Firewall of China?" Internet technologies, June 2022. https://www.techtarget.com/whatis/definition/Great-Firewall-of-China.

Kibbe, Jennifer D. "CIA/SOF Convergence and Congressional Oversight." *Intelligence and National Security* 0, no. 0 (August 7, 2022): 1–17. https://doi.org/10.1080/02684527.2022.2104015.

Kim, Woosang, and Scott Gates. "Power Transition Theory and the Rise of China." *International Area Studies Review* 18, no. 3 (2015): 219–26. https://doi.org/10.1177/2233865915598545.

King, Angus, and Mike Gallagher. *Cyberspace Solarium Commission Report*. Washington, DC: Cyberspace Solarium Commission, 2020. https://www.solarium.gov/report.

LaGrone, Sam. "Eliminating 'Risk Aversion' Key to Weapons Development, Says Vice Chair Nominee Grady." USNI News, December 9, 2021. https://news.usni.org/2021/12/08/eliminating-risk-aversion-key-to-weapons-development-says-vice-chair-nominee-grady.

Lewis, James Andrew. "Toward a More Coercive Cyber Strategy: Remarks to U.S. Cyber Command Legal Conference, March 4, 2021." Center for Strategic & International Studies, March 10, 2021. https://www.csis.org/analysis/toward-more-coercive-cyber-strategy.

Liang, Qiao, and Wang Xiangsui. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

Libicki, Martin C. "Correlations between Cyberspace Attacks and Kinetic Attacks." In *2020 12th International Conference on Cyber Conflict (CyCon)*, 199–213. Estonia: IEEE, 2020. https://doi.org/10.23919/CyCon49761.2020.9131731.

Lindsay, Jon R. "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem." *Intelligence and National Security* 36, no. 2 (2021): 260–78. https://doi.org/10.1080/02684527.2020.1840746.

Livieratos, Cole. "Bombs, Not Broadcasts: U.S. Preference for Kinetic Strategy in Asymmetric Conflict." *Joint Force Quarterly, JFQ*, no. 90 (2018): 60–67. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1567411/bombs-not-broadcasts-us-preference-for-kinetic-strategy-in-asymmetric-conflict/.

Lopez, C. Todd. "Defense Secretary Says 'Integrated Deterrence' Is Cornerstone of U.S. Defense." U.S. Indo-Pacific Command, May 3, 2021. https://www.pacom.mil/Media/News/News-Article-View/Article/2593958/defense-secretary-says-integrated-deterrence-is-cornerstone-of-us-defense/.

———. "Low-Level Commanders Need Authority to Counter Information Operations, Northcom Leader Says." DOD News, September 22, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2785305/low-level-commanders-need-authority-to-counter-information-operations-northcom/.

Lotrionte, Catherine. "Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations under International Law." *Cyber Defense Review* 3, no. 2 (2018): 73–114. https://www.jstor.org/stable/26491225.

Lydia. "'If You Always Do What You've Always Done, You'll Always Get What You've Always Got.' ~ Henry Ford." *Hidden Gem* (blog), November 8, 2021. https://hiddengemprofiles.com/2021/11/if-you-always-do-what-youve-always-done-youll-always-get-what-youve-always-got-henry-ford/.

Lythgoe, Trent. "Our Risk-Averse Army: How We Got Here and How to Overcome It." Modern War Institute, May 9, 2019. https://mwi.usma.edu/risk-averse-army-got-overcome/.

Magnuson, Stew. "Stove-Piped Systems Alive and Well in the Military." *National Defense*, November 8, 2011. https://www.nationaldefensemagazine.org/articles/2011/11/8/stovepiped-systems-alive-and-well-in-the-military.

Maness, Ryan C., Brandon Valeriano, Benjamin Jensen, Kathryn Hedgecock, and Jose Macias. "The Dyadic Cyber Incident and Campaign Data (DCID), Versions 1, 1.1, 1.5, and 2.0." Cyber Conflict Database. Accessed November 2, 2022. https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset.

March, James G. *A Primer on Decision Making: How Decisions Happen*. New York: Free Press, 1994.

Marczak, Bill, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert, and Vern Paxson. *China's Great Cannon*. Toronto: University of Toronto, 2015. https://citizenlab.ca/2015/04/chinas-great-cannon/.

Marine Corps University. "Mission and Vision Statement." Accessed November 14, 2022. https://www.usmcu.edu/About-MCU/Mission-and-Vision-Statement/.

Mobbs, Dean, Cindy C. Hagan, Tim Dalgleish, Brian Silston, and Charlotte Prévost. "The Ecology of Human Fear: Survival Optimization and the Nervous System." *Frontiers in Neuroscience* 9 (2015): 1–22. https://doi.org/10.3389/fnins.2015.00055.

Myers, Meghann. "Risk Aversion and Secrecy Are Costing U.S. Its Military Advantage, No. 2 General Says." *Military Times*, October 28, 2021, sec. Pentagon & Congress. https://www.militarytimes.com/news/pentagon-congress/2021/10/28/risk-aversion-and-secrecy-are-costing-us-its-military-advantage-no-2-general-says/.

Naegele, Tobias. "16th Air Force Is Fully Up and Running." *Air & Space Forces Magazine*, July 16, 2020. https://www.airandspaceforces.com/16th-air-force-is-fully-up-and-running/.

Nakashima, Ellen. "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms." *Washington Post*, February 27, 2019. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

Ni, Adam, and Bates Gill. "The People's Liberation Army Strategic Support Force: Update 2019." *China Brief* 19, no. 10 (May 29, 2019). https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/.

Nickerson, Charlotte. "What Is the Mere Exposure Effect?" Simply Psychology, March 8, 2022. https://www.simplypsychology.org/mere-exposure-effect.html.

Office of the Secretary of Defense. *Military and Security Developments Involving the People's Republic of China, 2021*. Washington, DC: Office of the Secretary of Defense, 2021. https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

Pomerleau, Mark. "New U.S. Army Cyber Unit Is Building Concepts for Tactical Cyber Operations." C4ISRNet, December 29, 2021. https://www.c4isrnet.com/cyber/2021/12/29/new-us-army-cyber-unit-is-building-concepts-for-tactical-cyber-operations/.

Richard Nixon Presidential Library and Museum. "War Powers Resolution of 1973." Richard Nixon Presidential Library and Museum, July 27, 2021. https://www.nixonlibrary.gov/news/war-powers-resolution-1973.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux, 2020.

Robert Kehler, C., Herbert Lin, and Michael Sulmeyer. "Rules of Engagement for Cyberspace Operations: A View from the USA." *Journal of Cybersecurity* 3, no. 1 (2017): 69–80. https://doi.org/10.1093/cybsec/tyx003.

Robertson, Corey. "Train as We Fight." U.S. Army, May 7, 2015. https://www.army.mil/article/148095/train_as_we_fight.

Rosenbaum, Judith E., and Jennifer Bonnet. "Looking Inward in an Era of 'Fake News': Addressing Cognitive Bias." Young Leaders of the Americas Initiative, June 10, 2019. https://ylai.state.gov/looking-inward-in-an-era-of-fake-news-addressing-cognitive-bias/.

Rovner, Joshua. "The Intelligence Contest in Cyberspace." *Lawfare* (blog), March 26, 2020. https://www.lawfareblog.com/intelligence-contest-cyberspace.

Samuelson, William, and Richard Zeckhauser. "Status Quo Bias in Decision Making." *Journal of Risk and Uncertainty* 1, no. 1 (March 1988): 7–59. https://doi.org/10.1007/BF00055564.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 1966.

Scobell, Andrew, Edmund J. Burke, Cortez A. Cooper, III, Sale Lilly, Chad J. R. Ohlandt, Eric Warner, and J. D. Williams. *China's Grand Strategy: Trends, Trajectories, and Long-Term Competition*. Santa Monica, CA: RAND Corporation, 2020. https://doi.org/10.7249/RR2798.

Selk, Avi. "'There's so Many Different Things!': How Technology Baffled an Elderly Congress in 2018." *Washington Post*, January 2, 2019. https://www.washingtonpost.com/lifestyle/style/theres-so-many-different-things-how-technology-baffled-an-elderly-congress-in-2018/2019/01/02/f583f368-ffe0-11e8-83c0-b06139e540e5_story.html.

SHRM. "Understanding and Developing Organizational Culture." SHRM, July 21, 2022. https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/understandinganddevelopingorganizationalculture.aspx.

Simon, Herbert A. "A Behavioral Model of Rational Choice." *Quarterly Journal of Economics* 69, no. 1 (February 1955): 99–118. https://doi.org/10.2307/1884852.

Southerland, Matthew. *U.S. Freedom of Navigation Patrol in the South China Sea: What Happened, What It Means, and What's Next*. Washington, DC: U.S.-China Economic and Security Review Commission, 2015. https://www.uscc.gov/research/us-freedom-navigation-patrol-south-china-sea.

Special Inspector for Afghanistan Reconstruction. *What We Need to Learn: Lessons from Twenty Years of Afghanistan Reconstruction*. Arlington, VA: Special inspector for Afghanistan Reconstruction, 2021.

Spoehr, Thomas. "Biden's First Defense Budget Batters the Army." Heritage Foundation Defense, June 7, 2021. https://www.heritage.org/defense/commentary/bidens-first-defense-budget-batters-the-army.

Statista Research Department. "U.S. Military Force Numbers, by Service Branch and Reserve Component 2020." Statista. Accessed November 16, 2022. https://www.statista.com/statistics/232330/us-military-force-numbers-by-service-branch-and-reserve-component/.

Sterman, John D. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Boston: McGraw-Hill, 2010.

Stewart, Darren M. "New Technology and the Law of Armed Conflict." *International Law Studies* 87 (2011): 271–98. https://digital-commons.usnwc.edu/ils/vol87/iss1/12/.

Timothy B. Lee. "In the 1970s, Congress Investigated Intelligence Abuses. Time to Do It Again?" *Washington Post*, June 27, 2013, sec. Economic Policy. https://www.washingtonpost.com/news/wonk/wp/2013/06/27/in-the-1970s-congress-investigated-intelligence-abuses-time-to-do-it-again/.

Tversky, Amos, and Daniel Kahneman. "Judgment under Uncertainty: Heuristics and Biases." *Science* 185, no. 4157 (September 27, 1974): 1124–31. https://doi.org/10.1126/science.185.4157.11.

U.S. Army Cyber Command. "About Army Cyber." U.S. Army Cyber Command. Accessed October 5, 2022. https://www.arcyber.army.mil/About/About-Army-Cyber/.

U.S. Cyber Command. "Command History." U.S. Cyber Command. Accessed October 28, 2022. https://www.cybercom.mil/About/History/.

U.S. Cyber Command Public Affairs. "DOD's Largest Multinational Cyber Exercise Focuses on Collective Defense." U.S. Department of Defense, December 6, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2863303/dods-largest-multinational-cyber-exercise-focuses-on-collective-defense/.

U.S. Fleet Cyber Command. "Command Description." U.S. Fleet Cyber Command/U.S. 10th Fleet. Accessed October 5, 2022. https://www.fcc.navy.mil/.

Valeriano, Brandon. "Cost Imposition Is the Point: Understanding U.S. Cyber Operations and the Strategy Behind Achieving Effects." *Lawfare* (blog), March 27, 2020. https://www.lawfareblog.com/cost-imposition-point-understanding-us-cyber-operations-and-strategy-behind-achieving-effects.

Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press, 2018.

Valeriano, Brandon, Ryan C. Maness, and Benjamin Jensen. "What Do We Know about Cyber War?" Working paper. Accessed August 5, 2022. http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/valeriano_maness_jensen_cyber_what_do_we_know_v2_.pdf.

Vergun, David. "Multi-Domain Battle Requires Non-Stovepipe Solutions, Say Leaders." U.S. Army, May 25, 2017. https://www.army.mil/article/188282/multi_domain_battle_requires_non_stovepipe_solutions_say_leaders.

Von Mises, Ludwig. *Bureaucracy*. New Haven, CT: Yale University Press, 1945.

Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, and Anina Schwarzenbach. *National Cyber Power Index 2020: Methodology and Analytical Considerations*. Cambridge, MA: Belfer Center for Science and International Affairs, 2020. https://www.belfercenter.org/publication/national-cyber-power-index-2020.

Wall, Andru E. "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action." *Harvard National Security Journal* 3 (2011): 85–142. https://www.soc.mil/528th/PDFs/Title10Title50.pdf.

West, Laura B. "The Rise of the 'Fifth Fight' in Cyberspace: A New Legal Framework and Implications for Great Power Competition." *Military Law Review* 229, no. 3 (2021). https://tjaglcs.army.mil/mlr/the-rise-of-the-fifth-fight-in-cyberspace-a-new-legal-framework-and-implications-for-great-power-competition.

White House. *Executive Order 12333- United States Intelligence Activities*, 1981. https://dodsioo.defense.gov/Library/EO-12333/.

———. "FACT SHEET: President Xi Jinping's State Visit to the United States." The White House—President Barack Obama, September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Wilson, GI. "Careerism and Psychopathy in the U.S. Military." Fabius Maximus website, June 23, 2019. https://fabiusmaximus.com/2019/06/23/generals-careerism-and-psychopathy/.

Wilson, James Q. *Bureaucracy: What Government Agencies Do and Why They Do It*. New York: Basic Books, 1989.

Wong, Edward, and Damien Cave. "U.S. Seeks to Reassure Asian Allies as China's Military Grows Bolder." *New York Times*, August 5, 2022, sec. World. https://www.nytimes.com/2022/08/05/world/asia/taiwan-china-united-states-allies.html.

World Bank. "GDP (Current US$)—United States." World Bank. Accessed November 1, 2022. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US.

World Population Review. "Military Size by Country 2022." World Population Review. Accessed November 16, 2022. https://worldpopulationreview.com/country-rankings/military-size-by-country.

Xie, John. "Will China Surpass the U.S. in Military Air Superiority?" VOA, October 13, 2021. https://www.voanews.com/a/when-will-china-surpass-the-us-in-military-air-superiority-/6270069.html.

Xie, Stella Yifan. "China's Economy Won't Overtake the U.S., Some Now Predict." *Wall Street Journal*, September 2, 2022, sec. World. https://www.wsj.com/articles/will-chinas-economy-surpass-the-u-s-s-some-now-doubt-it-11662123945.

Zhang, Ruixun, Thomas J. Brennan, and Andrew W. Lo. "The Origin of Risk Aversion." *Proceedings of the National Academy of Sciences* 111, no. 50 (December 16, 2014): 17777–82. https://doi.org/10.1073/pnas.1406755111.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California