

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 26-02-2021		2. REPORT TYPE Final		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Weaponizing Values: Reimagining U.S. Cyber Strategy				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) MAJ Emille Prosko Advisor: Dr. Timothy Schultz				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Ethics and Emerging Military Technology (EEMT) Program U.S. Naval War College 686 Cushing Road, Newport, RI 02841				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution Statement A: Approved for public release; Distribution is unlimited. Reference: DOD Directive 5230.24					
13. SUPPLEMENTARY NOTES A paper submitted to the Faculty of the U.S. Naval War College in partial satisfaction of the requirements of the Ethics and Emerging Military Technology Graduate Certificate Program. The contents of this paper reflect my personal views and are not necessarily endorsed by the U.S. Naval War College or Department of Defense.					
14. ABSTRACT: In a strategic environment of gray zone conflict, the current USCYBERCOM Strategy advantages Washington's values-agnostic adversaries, China and Russia. America has a unique set of values which differentiate it from its authoritarian competitors in Great Power Competition. U.S. values are a source of strength that promote trust and confidence for allies. Yet, the U.S. does not play to this strength by opting for an action-oriented, aggressive strategy; the current "Defend Forward" approach puts it at odds with some global cyber norms and cedes the moral high ground to autocratic competitors who exploit the gray zone. These same adversaries subvert norms and advocate for a closed, controlled internet order, but Washington's current cyber strategy fails to effectively challenge their influence by providing a viable way to maintain an open, interconnected cyberspace. This paper reimagines cyber strategy development. It focuses first on the values at stake and the ethical considerations inherent in cyber competition and then explores the optimal way to protect the American way of life in cyberspace. After establishing an understanding of who and what America is defending online and acknowledging adversary advantages in gray zone conflict, the author presents an analytical framework for cyber strategy based on norms-alignment and a strategic emphasis on either offense versus defense. Using scenario forecasting, this paper advocates a defense-oriented, norms-aligned cyber strategy that favors teamwork with allies, is commercially viable, economically sustainable, and achieves U.S. aims without conceding American values. This new approach – deciding the values at stake, before deciding how to compete – ensures the U.S. does not lose who it is as a nation as America adapts to modern threats.					
15. SUBJECT TERMS (Key words) Cyber Strategy, Values, Ethics, Great Power Competition, Gray Zone Conflict, Norms					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT N/A	18. NUMBER OF PAGES 82	19a. NAME OF RESPONSIBLE PERSON Ass. Dean-Electives &
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			19b. TELEPHONE NUMBER (include area code) 401-841-3556

NAVAL WAR COLLEGE
Newport, RI



Weaponizing Values: Reimagining U.S. Cyber Strategy

Emille K. Prosko, MAJ, USA

A paper submitted to the Faculty of the U.S Naval War College in partial satisfaction of the requirements of the Ethics and Emerging Military Technology Graduate Certificate Program.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Defense.

26 February 2021

Contents

Abstract	2
Acknowledgements	3
I. Thesis and Introduction: Strategizing for Cyber Conflict	4
IIA. The Competitive Environment	8
IIB. Unique Values Reinforce Friction among Great Power Competitors	13
IIIA. Competing Online: How Cyberspace Became a Competition Space	17
IIIB. On Cyberspace: A Unique Conflict Domain?	22
IIIC. On Cyberspace: Mental Frameworks for the Operating Environment	27
IIID. Ethics in the Cyber Domain: A Closer Look at How We Compete	31
IVA. Already Competing Online: Current Cyber Strategies	33
IVB. The Current Stalemate: On Cyber Norms	37
IVC. Change in U.S. Policy: Offense vs. Defense	39
V. The Cyber Quadrant: Possible Future Scenarios	47
VI. The Road Ahead: Necessary Revisions to Defense and Diplomacy	56
Appendix A: Global Internet Map	69
Appendix B: Nested U.S. Cyber Strategies	70
Bibliography	

Abstract

In a strategic environment of gray zone conflict, the current USCYBERCOM Strategy advantages Washington's values-agnostic adversaries, China and Russia. America has a unique set of values which differentiate it from its authoritarian competitors in Great Power Competition. U.S. values are a source of strength that promote trust and confidence for allies. Yet, the U.S. does not play to this strength by opting for an action-oriented, aggressive strategy; the current "Defend Forward" approach puts it at odds with some global cyber norms and cedes the moral high ground to autocratic competitors who exploit the gray zone. These same adversaries subvert norms and advocate for a closed, controlled internet order, but Washington's current cyber strategy fails to effectively challenge their influence by providing a viable way to maintain an open, interconnected cyberspace.

This paper reimagines cyber strategy development. It focuses first on the values at stake and the ethical considerations inherent in cyber competition and then explores the optimal way to protect the American way of life in cyberspace. After establishing an understanding of who and what America is defending online and acknowledging adversary advantages in gray zone conflict, the author presents an analytical framework for cyber strategy based on norms-alignment and a strategic emphasis on either offense versus defense. Using scenario forecasting, this paper advocates a defense-oriented, norms-aligned cyber strategy that favors teamwork with allies, is commercially viable, economically sustainable, and achieves U.S. aims without conceding American values. This new approach – deciding the values at stake, before deciding how to compete – ensures the U.S. does not lose who it is as a nation as America adapts to modern threats.

Acknowledgements

I am deeply indebted to many professors, practitioners, and colleagues who informed and influenced my research. My advisor, Dr. Tim Schultz, offered helpful guidance, encouragement, and patience throughout the year-long research effort. A project of this scope would not have been possible without his careful balance of patience and constructive critique. Dr. Chris Demchak's decades of work on cybersecurity policy greatly influenced the analysis and strategy recommendations put forth in this paper. Participating in her cybersecurity course at the outset of this endeavor provided an excellent foundation for my research. I appreciate the graciousness of the following technical experts in allowing me to interview them for this work: George Lucas, Brian Broene, Andrew Eich, Dave Hyde, Joseph Lane, and Matthew Shellem. Correspondence with cyber policy expert Beau Woods significantly enhanced the scenario analysis presented and cybersecurity sector research recommendations. As a China expert, Dr. Kristin Mulready-Stone provided a thoughtful review which strengthened my arguments about cyber competition among Great Powers. Isabel Lopes and Eamon McKeever were a tremendous help with research and formatting. My talented EEMT colleagues consistently inspired me and challenged me through their valuable insights in discussion. I would be remiss if I did not offer a heartfelt thank you to my family, especially my mother and my son, who afforded me countless quiet hours to devote to this project.

Finally, I am grateful to Dr. Schultz and Dr. Tom Creely for their continued time and leadership investment in the Naval War College's EEMT Program. As instruments of warfare become more complex, thank you for reminding today's military leaders that ethics emphasis in education remains critical because it is people, not things, who decide war's outcome.

Strategizing for Cyber Conflict: How to Think about the Problem

In the cyber domain, the U.S. is competing in a way that is inconsistent with its values and therefore, undermines its strengths while advantaging authoritarian competitors. America has a unique set of values, a source of strength that promotes trust and confidence for allies. While a military preference for an action-oriented approach is understandable, the U.S. does not play to its strengths by opting for an aggressive “Defend Forward” strategy which puts it at odds with some global cyber norms and cedes the moral high ground to autocratic competitors who exploit the gray zone. These same adversaries subvert norms and advocate for a closed, controlled internet order, yet Washington’s current cyber strategy fails to effectively challenge their influence by providing a viable strategy to maintain an open, interconnected cyberspace. This paper advocates a team-centric, norms-aligned, defense-oriented approach to protecting American interests online and competing with other Great Powers in the cyber domain.

Much literature exists on cyber conflict, analyzing its effect on warfare and its potential to lead to war. Just in the past two years, the USCYBERCOM Commander announced a new, “defend forward” approach to cyber competition, the Congressionally chartered Cyber Solarium Commission published a groundbreaking report with recommendations for the U.S. Cyber Strategy, and the *Texas National Security Review* (TSNR) dedicated a special issue to cyber competition.¹ The re-emergence of Great Power Competition (GPC), and its emphasis in the

¹ USCYBERCOM Commander General Nakasone’s describes the command’s new “defend forward” approach to cyber competition in this 2019 Joint Forces Quarterly Article:

<https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf>. The Cyber Solarium Commission was established “to develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences.” It published recommendations in early 2020 for a strategy of layered cyber deterrence. They are available as an executive summary and full report here: https://icitech.org/2020-us-cyberspace-solarium-commission-report/?gclid=Cj0KCQiAifz-BRDjARIsAEElyGLa_Xcu1-sNI_m5DmSngc2rLYr7E328hPP6FcPpUo-2rIIdbP2OLzsaAm0DEALw_wcB.

According to *Texas National Security Review* editors Robert Chesney and Max Smeets, its Cyber Competition issue is an “intervention” to address some of the shortfalls in existing studies on cyber attacks and cyber competition. Links to all articles in the issue are found here: <https://tnsr.org/category/special-issue-cyber-competitio>

U.S. 2018 National Defense Strategy, reinforces the need to consider cyber conflict through the specific lens of strategic competition and in the context of gray zone conflict, more commonly known as competition below the level of armed conflict.² Introducing the *TNSR* cyber competition series, editors Robert Chesney and Max Smeets point out the current volume of research on the topic does not amount to a clear narrative on either effects created in the cyber domain or how fluid conceptual frameworks for cyber issues should influence the United States' Cyber Strategy as it competes with starkly different peers.³ There is one important point of disagreement among experts: despite an increase in cyber incidents in the past decade, no consensus exists on whether cyber conflict is likely to escalate into an armed force engagement or deescalate tensions between nations. Cyber experts Brandon Valeriano, Ryan Maness, and Benjamin Jensen chronicle cyber competition in the international system from 2001 to 2014 and provide compelling evidence cyber conflict has not been escalatory.⁴ I agree with their optimistic conclusion but heed Jason Healey and Robert Jervis's warning that changing geopolitical circumstances could render it untrue, making the intersection of Great Power Competition and the cyber domain worthy of continued study.⁵

²U.S. Department of Defense, *Summary of the 2018 National Defense Strategy: Sharpening the American Military's Competitive Edge* (Washington, DC: Government Printing Office, 2018), 2, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

³ Robert Chesney and Max Smeets, "The Dynamics of Cyber Conflict and Competition," *Texas National Security Review Special Issue: Cyber Competition* (October 2020): 2-3, <https://repositories.lib.utexas.edu/handle/2152/83971>.

⁴ Benjamin Jensen, Ryan Maness, and Brandon Valeriano, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018), 70.

⁵ Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review Special Issue: Cyber Competition* (September 2020): 2, <http://dx.doi.org/10.26153/tsw/10962>. Currently a senior fellow at the Atlantic Council, Jason Healey was its founding director for cyber issues. Healey is also a cyber-specialist and senior research scholar at Columbia University's School for International and Public Affairs. Robert Jervis is the Adlai E. Stevenson professor of international politics at Columbia University. In this paper, these authors present findings on situational cyber stability based on cross-domain relationships and conditions between states.

This project contributes to the discussion regarding cyber conflict in a different way. Much of the current research concentrates on policy implications of certain actions and strategies in the cyber domain, especially focusing on an offensive versus defensive posture and an adherence to emerging global norms. But that focus is too far down the logic chain that should be underpinning strategies. Rather than asking, “What should the U.S. do to compete effectively in the cyber domain?” I ask, “What are the values at stake?” U.S. policymakers must be clear about who and what America is defending. In particular, a number of drivers influence the way the U.S. competes in cyberspace. Certainly, USCYBERCOM and its partners have a duty to protect the American way of life. They share a desire with the civilian leadership to endorse and help secure the most open and safe online environment for American citizens and U.S. allies. While protecting and securing, USCYBERCOM must also be bounded by American values and cognizant of how its actions in cyberspace message those values to the world. Determining which of these drivers should most significantly influence the U.S. Cyber Strategy must precede a debate about which cyber strategy is appropriate in this moment of Great Power Competition in gray zone conflict.⁶

This analysis is particularly critical because neglecting these unanswered questions directly harms the U.S. comparative advantage in strategic competition. The country must play to its strengths in Great Power Competition and American values are a foundational component of that strength. The U.S. maintains its position in the liberal world order because its partners trust Washington to use its power to protect a free and open way of life – values these partners expect

⁶ Brandon Valeriano, “Article 83 Review on ‘What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment,’” *H-Diplo/ISSF*, July 26, 2017. A Senior Fellow at the Cato Institute and Bren Chair of Military Innovation at the Marine Corps University, Valeriano recognized the importance of understanding *why* states engage in cyber conflict, here: <https://issforum.org/articlereviews/83-cyber>. He poses these three, important questions: 1) Just what issues drive [states to fight in] international cyber conflicts? 2) What, if not costs [of cyber operations], are they [leaders] focused on? 3) What role do resolve, interest, and capability play [in driving cyber conflict]?

to shape Washington's actions. Therefore, a competitive approach that deviates from those values undermines America's position relative to values-agnostic authoritarian regimes. How should America effectively act in accordance with its values in cybered Great Power Competition? Can it weaponize honesty and transparency in the gray zone? These questions are not simply for lofty idealists. These are questions for realists who appreciate the nature of twenty-first century Great Power Competition, best described as gray zone conflict. To compete in a way that is both effective and consistent with U.S. values requires an acknowledgement of the defining aspect of the competition space. As Carl von Clausewitz counsels,

The first, the supreme, the most far-reaching act of judgment that the statesman and commander have to make is to establish by that test the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature.⁷

In this paper, I disaggregate those two overarching questions into analytical components. First I ask: What is the nature of the competitive environment? What values distinguish the U.S. from its competitors? What does the U.S. hope to achieve in cyberspace? Then, how should strategists think about the cyber domain (what makes it unique) and what are the ethical considerations inherent in cyber competition? Finally, I explain the implications of this analysis for U.S. Cyber Strategy. Imagine a different world where U.S. strategic cyber thinkers early on consider more broadly the way America competes with other global powers as they design the role that norms and offensive (vs. defensive) mindsets should play in their strategic approach. This new approach – deciding the values at stake, before deciding how to compete – ensures that the U.S. does not lose who it is as a nation as America adapts to modern threats.

⁷ Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 88.

The Competitive Environment

The nature of the competitive environment is gray zone conflict, which National Defense University (NDU) Distinguished Scholar Francis Hoffman describes as, “nonviolent coercion as a means of political competition.” Hoffman acknowledges the ambiguity inherent in the term gray zone conflict. To clarify, he classifies it as “measures short of armed conflict” with “an integrated and purposeful design” and distinguishes it from the violent methods used in other elements of the conflict continuum – irregular, hybrid, and conventional warfare.⁸

The term has gained prominence over time as kinetic exchanges between major powers have declined and scholars have challenged the stark black-and-white understanding of war and peace common in U.S. strategic culture. They warn that retaining this vision of the strategic environment could lead to a reactive and militarized foreign policy.⁹ Gray zone conflict poses unique challenges, especially to those who subscribe to the liberal international order. This is because realist-oriented, ethically agnostic participants in gray zone conflict can leverage the ill-defined borders between peace and war. They routinely exploit ambiguity concerning their identity, their objectives, whether they are actually violating international treaties and norms, and whether a military response would be justified.¹⁰ For America’s adversaries, as George Kennan noted decades ago, “The varieties of skullduggery which make up the repertoire of the

⁸ Francis G. Hoffman. *The Evolution of Hybrid Warfare and Key Challenges: Hearing before the Committee on Armed Services, House of Representatives*, 115th Cong. (2017), <https://www.govinfo.gov/content/pkg/CHRG-115hhrg25088/pdf/CHRG-115hhrg25088.pdf>. Hoffman’s 2017 testimony to the House Armed Services Committee on the Evolution of Hybrid Warfare has heavily influenced the understanding of gray zone conflict among national security professionals.

⁹ Nadia Schadlow, “Peace and War, the Space Between,” *War on the Rocks*, August 18, 2014, <http://warontherocks.com/2014/08/peace-and-war-the-space-between/>.

¹⁰ David Barno and Nora Bensahel, “Fighting and Winning in the ‘Gray Zone,’” *War on the Rocks*, May 19, 2015.

totalitarian government are just about as unlimited as human ingenuity itself, and just about as unpleasant.”¹¹

The cyber domain is a prime space for gray zone conflict to take place, enacting cyber conflict. Revisionist regimes deftly harness nontraditional elements of statecraft to undermine U.S. credibility, including cyber intrusions, corruption, and disruption.¹² The domain is, as many cyber experts admit, difficult to conceptualize. Defense leaders and analysts have developed several frameworks to help strategists think about competing in cyberspace, several of which are discussed in this paper. In terms of defining cyberspace, the Department of Defense calls it: “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.”¹³ It is a broad space that includes both the networks (physical and virtual) and the hardware necessary to craft, package, transmit, secure, reconstruct and receive information.¹⁴ In terms of the weapons and actions used in the domain, codes and keystrokes are, respectively, the unique mode of competing. The same spectrum of conflict described above – methods short of war, through hybrid warfare, to conventional war – exists in the cyber domain.

¹¹ Giles D. Harlow and George C. Maerz, eds., *Measures Short of War: The George F. Kennan Lectures at the National War College, 1946-47* (Washington, DC: National Defense University Press, 1990), 6-8.

¹² Hoffman, “The Evolution of Hybrid Warfare,” 5.

¹³ Catherine A. Theohary, *Defense Primer: Cyberspace Operations*, CRS Report No. IF10537 (Washington, DC: Congressional Research Service, 2020), 1, <https://crsreports.congress.gov/product/pdf/IF/IF10537>. Interestingly, as George Lucas points out on page 16 of his 2017 book, *Ethics and Cyber Warfare*, cyberspace is a redundant term, since, “Cyber itself is a new term, derived from an ancient Greek noun referring to a ‘space’ or a ‘domain.’”

¹⁴ George Lucas, *Ethics and Cyber War: The Quest for Responsible Security in the Age of Digital Warfare* (New York, NY: Oxford University Press, 2017), 17-19.

While the terms cyber conflict and cyberwar are often used interchangeably, they are distinguished from one another in scope. While cyberwar occurs within the bounds of a network, cyber conflict transcends digital limits, including the cybered system that underpins modern social, economic, and technological systems.¹⁵ This paper is concerned, foremost, with cyber conflict because it occupies the spectrum between peace and largescale conventional war. It is endemic in a globally connected age characterized by gray zone conflict among great powers. Although it is certainly possible for cyber activity to escalate into violence in the physical domain, most nations have leveraged the space to gain asymmetric advantage without resorting to conventional war. Stated another way, cyber conflict creates a range of outcomes that could lead to the far-right end of the conflict spectrum, but largely enables measures short of war or hybrid war. Examples of this include: 1) the Stuxnet virus (gray zone), 2) the Chinese breach of the U.S. Office of Personnel Management (OPM) (gray zone), and 3) the Russian attacks on the Ukrainian power grid (hybrid war).¹⁶ One of the first documented cases of a cyberattack – the 2007 Russian-linked (but denied) Distributed Denial of Service (DDoS) attack against Estonia – disrupted service for banks, news outlets, and government agencies but caused no physical damage.¹⁷

¹⁵ Chris Demchak, “Cybered Conflict vs. Cyber War,” *Atlantic Council Blog* (blog), October 20, 2010, <https://www.atlanticcouncil.org/blogs/new-atlanticist/cybered-conflict-vs-cyber-war/>.

¹⁶ Center for Strategic & International Studies, “Significant Cyber Incidents,” *CSIS.org*, 2021 <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.

¹⁷ Lucas, *Ethics and Cyber War: The Quest for Responsible Security in the Age of Digital Warfare*, 3-7. In his discussion of various cyberattacks, Lucas explains DDoS attacks involve large networks of hijacked, compromised computers, termed ‘botnets,’ that can be ordered by hackers to generate and transmit an enormous barrage of messages or logon requests to a specific Internet address, overwhelming it and effectively shutting down whatever agency, organization, or financial service is associated with that address.” George Lucas actually describes these events as cyber war, a term first introduced by the Rand Corporation’s strategic studies expert John Aquilla in 1992. However, in my paper, I use the term cyber conflict (as defined above) for consistency. The breadth, complexity of systems, and ambiguity surrounding actors involved in cyber conflict is most critical to note, rather than the term itself, since much debate persists among scholars about what terms and analogies best capture events in cyberspace. Finally, cyberwar is not included in the DoD Dictionary of Military and Associated Terms published in 2020, but

These examples demonstrate that cyber conflict is an extension of international politics across a very wide spectrum of consequences, from measures short of war to influence another nation's defense system to hybrid conflict affecting an adversary's national infrastructure. These attacks and campaigns blur the line between military and civilian targets in cyber conflict. Corporations become attack vectors for adversaries seeking to disrupt national networks, as was the case in the 2016 Russian disinformation campaign waged on social media (Facebook and Twitter)¹⁸ and the 2020 hack against IT management company, Solar Winds.¹⁹ Cyber conflict is not only a new form of state-on-state competition, it is now the dominant form of direct contestation in the gray zone.²⁰

If gray zone conflict is the nature of modern strategic competition, what is Great Power Competition? In 2017, Francis Hoffman briefed the House Armed Services Committee: "In both Europe and in Asia, we are competing with major revisionist powers for influence and for the retention of a rules based international order."²¹ After Russia's cyber-enabled intervention in

cyberspace attacks are defined as follows: "Actions taken in cyberspace that create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or manipulation that leads to denial that appears in a physical domain and is considered a form of fires." Link to the DoD Dictionary here: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.

¹⁸ Sheera Frenkel and Julian E. Barnes, "Russians Again Targeting Americans with Disinformation," *New York Times*, September 1, 2020, <https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html>. The Solar Winds breach affected not only civilian cybersecurity companies, but also included government victims, to include U.S. Departments of State, Homeland Security, Commerce, and the Treasury, as well as the National Institutes of Health. Solar Winds was a perfect entry point for the Russians, since it has over 18,000 customers who rely on its network monitoring and other security services.

¹⁹ Brian Barrett, "Security News This Week: Russia's SolarWinds Hack Is a Historic Mess," *Wired Magazine*, December 19, 2020, <https://www.wired.com/story/russia-solarwinds-hack-roundup/>.

²⁰ Bruce Jones and Torrey Taussig, "Democracy & Disorder: The Struggle for Influence in the New Geopolitics," *Brookings Institute*, February 2019 (10), https://www.brookings.edu/wp-content/uploads/2019/02/FP_20190226_democracy_report_WEB.pdf. In their report, the authors assert, "Regions of contestation have emerged across the developing and industrialized world. It is a competition of influence that involves political, economic, and military tools—and it is increasingly digitalized."

²¹ Hoffman, "The Evolution of Hybrid Warfare," 7.

Georgia in 2008, historian Robert Kagan argued that the world was entering an era of global competition, pitting the value systems and ideas of the U.S. liberal democracy against those of Chinese and Russian autocracies.²² This outlook gained traction in Washington following Beijing's disputed land claims in the South China Sea and Moscow's annexation of Crimea. The 2017 National Security Strategy (NSS) and 2018 National Defense Strategy (NDS) formalized the term Great Power Competition in U.S. foreign policy, and it has since been used in over 6,500 security strategy articles.²³

A 2020 Report to Congress on Great Power Competition includes these features, relating to China and Russia: 1) a shift in strategic emphasis and resources from counterterrorism (CT) to grand strategy with special focus on the Indo-Pacific region, 2) an international relations transition from the post-Cold War unipolar moment to a multipolar environment, and 3) a capabilities build-up for innovation, supply chain security (including software), hybrid warfare, and gray zone conflict. While some defense experts caution against the term's ambiguity and polarizing effect on allies, its meaning is applied here as the contest between the United States, China, and Russia to assert national will and global influence, encompassing the military, economic, diplomatic, and cultural spheres.²⁴

²² Robert Kagan, "History's Back: Ambitious Autocracies, Hesitant Democracies," *Carnegie Endowment for International Peace*, August 25, 2008, 2, <https://carnegieendowment.org/2008/08/25/history-s-back-ambitious-autocracies-hesitant-democracies-pub-20401>.

²³ Uri Friedman, "The New Concept in Washington Everyone is Talking About," *The Atlantic*, August 6, 2019, 2-3, <https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/>.

²⁴ Ronald O'Rourke, *Renewed Great Power Competition: Implication for Defense – Issues for Congress*, CRS Report No. R43838 (Washington, DC: Congressional Research Service, 2020), 16-19, <https://crsreports.congress.gov/product/pdf/R/R43838/71>.

Unique Values Reinforce Friction among Great Power Competitors

Ideological competition between democratic and authoritarian governance is making a comeback. The 2018 NDS emphasizes strategic competition as the defining feature of the current operating environment.²⁵ In 2020, the Trump administration released a related counter-People's Republic of China (PRC) Strategy, acknowledging the near-peer threat posed by a rapidly rising China. While the U.S. has not produced a parallel plan to counter Moscow, implicit in Washington's strategic documents is a grudging return to a Cold-War-era rivalry, one that pits the U.S. against two uniquely skilled opponents.²⁶ Today, a democratic United States faces two revisionist competitors in economic heavyweight China and seasoned disruptor Russia. While GPC is often cast in terms of economic, technological, and information warfare, it is the struggle between U.S. democratic values and authoritarian ideals which transcends all aspects of the rivalry.

The PRC Strategy elaborates on the ideological differences which underpin the way the United States and China compete, specifically contrasting the role of the state, in either protecting or subordinating individual rights.²⁷ Disturbingly, the PRC Strategy points to evidence that the Chinese Communist Party (CCP) is exporting its authoritarian governance model,

²⁵ U.S. Department of Defense, "Summary of the National Defense Strategy of the United States of America," 6.

²⁶ Jonathan M. DiCicco and Brandon Valeriano. "International Rivalry and National Security," *The Oxford Handbook of U.S. National Security*, ed. Nikolas K. Gvosdev, Derek S. Reveron, and John A. Cloud (New York: Oxford University Press, 2018) 1, 3. Canisius College Associate Professor of Political Science Jonathan DiCicco and Niskanen Center senior fellow in cyber security Brandon Valeriano define rivalry as "protracted conflict with a hostile adversary," which is, "antagonistic enough that a militarized dispute or war might break out at any time." This definition is consistent with the current dynamic between Sino-American and Russo-American relations, although conventional war with China is more likely than Russia, which demonstrates a preference for hybrid warfare.

²⁷ The White House, *United States Strategic Approach to the People's Republic of China* (Washington, DC: The White House, 2020), 4-5, <https://china.usembassy-china.org.cn/wp-content/uploads/sites/252/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.24v1.pdf>.

heavily reliant on tech-enabled surveillance – one that censors free speech, abuses and silences political dissenters, and deceptively propagates a pro-CCP narrative that ignores these flaws. Confirming the severity of the threat to American values, Admiral Davidson, USINDOPACOM Commander, stresses that China uses coercion, corruption, and co-option for internal suppression and external aggression.²⁸ Russia, for its part, continues its cycle of disruption and denial, the attacks on Ukraine’s power grid and interference in the 2016 U.S. election offering recent examples. The modern Chinese and Russian emphasis on information operations and deception should surprise no one. Mao Zedong’s texts on insurgency and Russia’s “disinformation” doctrine are foundational to the way U.S. peers think about competition.²⁹ These twentieth-century ideas manifest in modern-day disinformation campaigns, intellectual property (IP) theft, digital authoritarianism, and cyberattacks carried out by Beijing and Moscow.

What differentiates the way the U.S. approaches competition? While a relatively young global power, America’s ideological foundation finds its roots in ancient Greece, Roman republicanism, and the Enlightenment.³⁰ Throughout its short history, a pioneering American

²⁸ Admiral Philip S. Davidson, “USINDOPACOM Commander’s Keynote Address for the 33rd Annual National Symposium,” Honolulu, Hawaii, January 12, 2021, <https://www.pacom.mil/Media/Speeches-Testimony/Article/2469844/33rd-annual-sna-national-symposium/>.

²⁹ See this reference for a compilation of Mao Zedong’s texts on insurgency: *Seeing Red: The Development of Maoist Thought on Insurgency*. In a recent review of Mao’s influence, Cato Institute’s Doug Bandow discusses Mao’s legacy and its influence on Xi Jinping: <https://www.cato.org/publications/commentary/xi-jinping-wants-become-new-mao>. Iza Ding and Jeffrey Javed explain why Mao’s influence persists in modern China in this 2019 study in the Washington Post: <https://www.washingtonpost.com/politics/2019/05/29/why-maoism-still-resonates-china-today/>. The long history of Russian disinformation is captured in journalist Adam B. Ellick’s documentary series, Operation Infektion, linked here: <https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html>.

³⁰ Carl Richard, Thomas Ricks, and Caroline Winter, “What the Founders Learned from the Greeks and the Romans,” December 8, 2020, in *Live from the National Constitution Center*, moderated by Jeffrey Rosen, produced by Jackie McDermott, podcast, <https://constitutioncenter.org/interactive-constitution/podcast/what-the-founders-learned-from-the-greeks-and-romans>; Harvard University’s Pluralism Project, “Enlightenment and Revolution,” *Pluralism.org*, last modified 2020, <https://pluralism.org/enlightenment-and-revolution>.

spirit has led to a competitive approach characterized by flexibility, innovation, resiliency, and sheer grit. Since the great U.S. democratic experiment began, Americans have demonstrated a willingness to scrap and reinvent to defend their founding ideals – liberty, equality, opportunity, and individual rights and freedoms. Contrary to authoritarian China and Russia, U.S. culture is open and optimistic, as epitomized in the American Dream; regardless of race, creed, religion, or economic background, an individual’s effort and innovative spirit define their destiny. While heightened partisanship and foreign manipulation of the free press in the United States threatens to fracture American unity behind its ideals, the ideological advantage associated with America as the land of freedom and opportunity for all is captured in the NSS’s principled realism.³¹

Fundamentally then, what is it that we compete for? The U.S. NSS frames security goals in four pillars: 1) protect the American people, homeland, and way of life; 2) promote American prosperity; 3) preserve peace through strength; and 4) advance American influence. At the most fundamental level, then, we compete with other nations to preserve the ideals described above because they enable individual liberties and freedom.³² As it manifests in the cyber domain, Great Power Competition ensures the U.S. open concept for the internet and secures the online environment for the free exchange of commerce and ideas. Today, America seeks to defend its way of life by partnering with other like-minded countries to promote democratic governance worldwide and increase global connectedness. This U.S.-conceived liberal world order relies on openness, transparency, and accountability to thrive and emphasizes intergovernmental organizations and interoperable digital networks in the modern environment. Unfortunately,

³¹ The White House, *The National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), 4.

³² Nina Evanson, “American Culture,” *IES: Cultural Profiles*, 2016, <https://culturalatlas.sbs.com.au/american-culture/american-culture-business-culture>.

global connectedness is undermined in cyberspace by exploitive adversaries who prefer a closed, surveilled cyber domain which favors government control over the digital economy and online communication.

Given competitors' blatant attempts to undermine an open, U.S.-backed liberal world order, Washington's positive competitive aims are coupled with corresponding negative aims: preventing impediments to the free and open lifestyle Americans promulgate. The United States, China, and Russia are engaged in a battle for ideological supremacy, both generally and in the cyber domain, specifically.³³ This realist appraisal is borne out with evidence that Beijing and Moscow would rather remain in the shadows.³⁴ The views from the Washington Monument and Tiananmen Square or Red Square are not the same; the first is a beacon of freedom and the latter two exemplify ruthless free speech suppression. Censorship of speech often occurs on the internet, including both mainstream and social media. Why does China get away with muzzling Muslims (and any other threats to its power) online and radical invasion of citizens' privacy?³⁵

³³ Elizabeth Economy, "China's New Revolution: The Reign of Xi Jinping," *Foreign Affairs* 97, no. 3 (2018): 65, <https://www.foreignaffairs.com/articles/china/2018-04-17/chinas-new-revolution>. Countless authors have claimed, more broadly, that global U.S.-Sino competition is ideological. Elizabeth Economy, a Starr Senior Fellow and Director for Asia Studies at the Council on Foreign Relations, explains why that is true: "Xi has eliminated the dividing line between domestic and foreign policy. But now that the country [China] is exporting its political values—in some cases, to buttress other authoritarian-leaning leaders, and in others, to undermine international law and threaten other states' sovereignty—China's governance model is front and center in its foreign policy."

³⁴ Sarah Cook, "The Globalization of China's Media Controls: Key Trends from 2019," *The Diplomat: The Debate*, 2020, 2, <https://thediplomat.com/2020/01/the-globalization-of-chinas-media-controls-key-trends-from-2019/>. Over the past decade, China has done an impressive job of keeping its exploitive tactics and disregard for human rights from the public eye. More recently, though, the CCP's global propaganda push and suppression of negative press abroad has resulted in backlash. In the referenced article, Sarah Cook points out, "China's public approval ratings declined by between 7 and 17 percentage points from 2018 to 2019 in influential developing countries with notable Muslim populations, including Indonesia, Kenya, and Tunisia." In a more recent opinion piece, from June 2020, the same author describes the growing global pushback: <https://thediplomat.com/2020/06/chinas-media-influence-has-gone-global-so-has-the-pushback/>.

³⁵ Abdi Dahir, "China Is Exporting Its Digital Surveillance Methods to African Governments," *Nextgov*, November 1, 2018, <https://www.nextgov.com/emerging-tech/2018/11/china-exporting-its-digital-surveillance-methods-african-governments/152495/>.

Why can Russia turn off the lights in Ukraine and interfere with the 2016 U.S. election with minimal reprisal? Frankly, Beijing and Moscow transgress because the U.S. and its allies offer no consolidated alternative to Chinese and Russian cyber tactics. Rare global media outcries to condemn Chinese and Russian encroachment on individual freedom and free flow of ideas are often drowned out by the disinformation and divisive influence operations prosecuted by Beijing and Moscow.³⁶ To their credit, Chinese and Russian manipulative efforts are paying off – the voice of democracy is being silenced through savvy online tactics. The U.S. is struggling with an effective way to counter online interference without mirroring its adversaries’ oppressive online censorship. Without a more concerted and consolidated campaign for an open internet environment, “all that is necessary for evil to prevail is for good men to do nothing.”³⁷

Competing Online: How Cyberspace became a Competition Space

Technology reflects human nature. This statement has been borne out consistently enough to make it worthy of inclusion among Melvin Kranzberg’s list of technology truisms.³⁸ Technology may escape the original intentions of its human creators but cannot completely elude human influence. Thus, our tools reflect the full spectrum of our humanity – the best of our brilliance, the most altruistic of our intentions, and the worst of our destructiveness. Our modern

³⁶ Economy, “China’s New Revolution: The Reign of Xi Jinping,” 73-74. In this article, Economy presents several complementary thoughts highlighting China’s hypocrisy: “China is eager to restrict opportunities for outsiders to pursue their political and economic interests within its borders, even as it advances its own such interests outside China... While Xi poses new challenges for the United States, he also offers a distinct new opportunity: the chance for Washington to hold him publicly accountable for his claim that China is prepared to assume greater global leadership... The good news is that Xi has made his revolutionary intentions clear. There is no excuse now for the United States not to respond in equally unambiguous terms.” In its messaging, the U.S. could (and should) catch Xi Jinping in his self-created dilemma – China wants respect without responsibility – and call him out in his malign actions on the world stage.

³⁷ John Stuart Mill, “Saint Andrews Inauguration Address,” 1867.

³⁸ Melvin Kranzberg, “Technology and History: ‘Kranzberg’s Laws,’” *Technology and Culture* 27, no. 3 (1986): 544-560.

communications technology and platforms exemplify this truth in many ways. The internet, specifically, is the modern highway of ideas and information. Born of noble intentions and incubated in the Defense Advanced Research Projects Agency (DARPA) lab before commercializing, the internet's founders conceived of a globally accessible tool in which "everyone could quickly access data and programs from any site."³⁹ Openness was foremost in its creators' minds. The decentralized structure of the original internet promoted efficiency and freedom of communication. The ARPANET's (later the internet) neglect of control mechanisms reflected not negligence, but optimism that the tool would bring nations and cultures together in a collaborative way. Its designers projected countless opportunities for connection but were unimaginative when it came to the internet's destructive potential when corrupt hands controlled the keyboards.⁴⁰

Today, the same internet that connects families and friends around the planet simultaneously serves as the propaganda platform for extremist organizations. The very open and equalizing internet DARPA's scientists conceived of has now become the tool of dictators to disrupt free and fair elections and repress the rights of ethnic minorities.⁴¹ The cables that carry information to inform voting publics and educate the most remote populations also spew disinformation to the same audiences, corrupted by nefarious actors manipulating the invention for their own perverse purposes. The original internet design did not account for these threats, which represent the exploitation of its open architecture for misuse.

³⁹ Barry Leiner *et al.*, "Brief History of the Internet: 1997," *Internet Society*, September 13, 2017, <https://www.internetsociety.org/resources/doc/2017/brief-history-internet/>.

⁴⁰ See this link for a description of the internet backbone and a technical explanation of how the internet infrastructure is manipulated by malign actors, especially China: <https://www.zdnet.com/article/china-has-been-hijacking-the-vital-internet-backbone-of-western-countries/>.

⁴¹ Abdi Dahir, "China is Exporting its Digital Surveillance to African Governments," 2018.

The decentralized structure of the original internet design has allowed current users to hijack the tool for their own ends. The irony is that these threats are not optimally countered by adding controls (although authoritarian leaders would have us think otherwise), as illustrated by Facebook's 2020 attempts to block political ads in U.S. elections, which resulted in bipartisan criticism for unfairly suppressing free speech without minimizing voter misinformation.⁴² Democratic governments struggle to preserve the positive potential of the open internet, minimizing controls on free exchange while protecting against threats, but the cyber domain favors the offense and disadvantages the defense.⁴³ Thus, a constant race persists in cyberspace: defensive walls, secure software, and cybersecurity practices seek to keep pace with creative malicious code, deceptive delivery mechanisms (think: social engineering, phishing, etc.) and disinformation strategies. To date, the billions of dollars in damage caused by rookie hackers and sophisticated states, alike, indicates the better angels of our human nature are not winning out. What to do about this problem is covered in recommendations provided later in the paper. But, that it is a problem should be no surprise – our tools reflect our nature and our values. And, regardless of how much internet cable and code is involved, it remains, foremost, a human problem.

The global connectivity map has become busier as more and more of the world has gained access via either cable or wireless internet. This portends a world where the power passes from states and multinational corporations (MNCs) to the people. The internet does not distribute

⁴² See the following links for more information on the negative reaction to Facebook's blocking political ads prior to the 2020 U.S. Presidential election: <https://www.google.com/amp/s/www.washingtonpost.com/technology/2020/10/27/facebook-ban-new-political-ads/%3foutputType=amp>; <https://www.technologyreview.com/2020/09/06/1008192/why-facebooks-political-ad-ban-is-taking-on-the-wrong-problem/>; <https://www.nytimes.com/2020/09/04/technology/facebooks-political-ads-block-election.html>.

⁴³ Chris Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly*, 2011.

influence (power) equitably, as its founders intended and optimists projected. However, cyberspace does diffuse power in a way that is distinct from other warfighting domains. Advancements in internet connectivity like 5G mean that connected consumers can collaborate with even more speed and efficiency. Powerhouse providers like Huawei and Ericsson not only make life more convenient and connected for developed countries, they often introduce internet and digital communication to developing countries.⁴⁴ In Africa, Huawei's 5G investment has represented not an incremental technological advancement from 4G, but an introduction of many societies to the internet.⁴⁵

The race among Information and Communications Technologies (ICT) companies to meet the widening demand for connectivity is not simply a matter of commercial competition for market share; it represents an opportunity to shape the global internet order. This is because ICT companies are either owned by or reflect values of their own state government, and authoritarian countries practice a different internet model than open, democratic societies.⁴⁶ For example, in Russia and China, individual privacy and data rights are largely ignored, and the internet is a tool to manipulate political outcomes in favor of the current regime. States that favor a liberal world

⁴⁴ Makada Henry-Nickie, Kwadwo Frimpong, and Hao Sun, "Trends in the Information Technology sector," *Brookings Institution*, March 29, 2019, 3, <https://www.brookings.edu/research/trends-in-the-information-technology-sector/>. This Brookings report describes trends in the global technological landscape, explaining that the, "move from a hardware to software-centric level of growth has been particularly pronounced in developing countries due to deeper and wider mobile-cellular networks...[T]he maturing mobile ecosystem has been fueled by greater accessibility among mobile internet users and the affordability of smartphones and portable devices."

⁴⁵ Abdi Dahir reports on China's most recent technology agreement with the African Union, which includes rolling out 5G networks, here: <https://qz.com/africa/1632111/huawei-african-union-sign-deal-to-boost-5g-ai-cloud-computing/>. Writing for Voice of America, Salem Solomon explains: "the agreement expands Huawei's foothold in a market with significant potential for growth in the years ahead; just 36% of Africans had reliable internet access as of March." The article is linked here: <https://www.voanews.com/africa/after-allegations-spying-african-union-renews-huawei-alliance>.

⁴⁶ Chinese and Russian companies operating abroad are often state-owned or state-affiliated. Huawei and Peter-Service are two, respective examples. While the American government lacks the same level of influence over its private businesses, U.S. ICT companies still reflect American values or openness, transparency, and individual rights.

order tend to view the cyber domain as the land of opportunity – a highway to create content, share ideas, and communicate freely.⁴⁷ The U.S. banning of Huawei and the campaign to convince its allies to do so highlights this ideological struggle of open vs. closed internet. China continues to export its digital authoritarianism – “the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations” – to countries along its Belt-and-Road Initiative.⁴⁸ Anywhere Huawei builds a tower, the company can facilitate intelligence collection and influence for China as it reroutes data back to Beijing.⁴⁹ When Russian companies Protei and Peter-Service provide System of Operative-Search Measure (SORM) technologies abroad, they partner with local telecom firms to enable the host government to practice Moscow’s model of digital surveillance (copying the internet traffic of independent media, private companies, and citizens).⁵⁰ In these instances of Chinese and Russian influence, the internet is a tool for control, not a means to communicate freely.

Because Chinese and Russian companies are either state-owned (China) or subject to state intimidation (Russia), the winner of the ICT market share battle gains the ability to determine how cyber technology is used in the client state and, therefore, which internet order is propagated in that region. Although there is a commercial element to the ICT competition, in

⁴⁷ Pages 24-25 of the following Freedomhouse Freedom of the Net Report show the distinct online environments among the U.S. and its great power rivals: https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf. In the global rankings based on obstacles to internet access, limits on content, and violations of user rights, the U.S. scores 77 (out of 100), while Russia earns only 30, and China scores just 10, making China the least free online environment according to Freedomhouse’s global rankings.

⁴⁸ Alina Polyakova and Chris Meserole, “Exporting digital authoritarianism: The Russian and Chinese models,” *Brookings Institute*, August 27, 2019, 1, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

⁴⁹ Democratic Staff Report for the Committee on Foreign Relations (Ranking Member: Robert Menendez), *The New Big Brother: China and Digital Authoritarianism* (Washington, DC: U.S. Senate, 2020) 27-31.

⁵⁰ Alina Polyakova and Chris Meserole, “Exporting digital authoritarianism: The Russian and Chinese models,” 8.

reality it illustrates a significant portion of Great Power Competition is taking place in the cyber domain.

On Cyberspace: A Unique Conflict Domain?

In contrast to the closed, control-oriented internet model propagated by China and Russia, openness of the internet in democratic countries both enhances modern life and creates an extremely complex problem for security strategists. Proposing how to balance the internet's opportunities and challenges requires, first, consideration of the optimal way to think about the cyber domain before suggesting strategies on how the U.S. can promote its open model in that shared space. The cyber substrate is unique among other warfighting domains in that it is manmade and increasingly ubiquitous. It transcends "boundaries of land, sea, air, institution, and medium."⁵¹ Cyberspace is akin to the air, maritime, and space domains in its role as a global commons for the exchange of business and communication.⁵² The air and maritime comparison is imperfect, however, because national waters exist and are respected in the form of national airspace (delineated by national boundaries) and exclusive economic zones (EEZs). In the cyber realm, the distinction of "national networks" is blurred by the start and end points of global cables and towers transmitting data packets. When does an intercontinental cable become domestic hardware? That question has yet to be unequivocally answered in international law.⁵³

⁵¹ Demchak, "Cybered Conflict vs. Cyber War," 2010. While cybersecurity scholar Chris Demchak uses the term cybered conflict, this paper shortens the word to cyber conflict, since cybered was not common among most literature describing actions in the cyber domain. Her understanding of cyber as a dual-use substrate linking multiple warfare domains and societal systems is helpful in capturing the complexity inherent to competing in the cyber domain. Her 2010 article is available here: <https://www.atlanticcouncil.org/blogs/new-atlanticist/cybered-conflict-vs-cyber-war/>.

⁵² As Jason Healey and Robert Jervis suggest in their recent TNSR article, "[Cyber] is existential to a growing number of states. Advanced states rely on connectivity, including the Internet of Things, not just for communication but control of the economy and industry." See full article here: <https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/>.

⁵³ Chris C. Demchak, "Cybered Conflict, Hybrid War, and Informatization Wars," In *Routledge Handbook of International Cybersecurity*, ed. Eneken Tikk and Mika Kerttunen (New York: Routledge, 2020), 36-51.

(See Figure 1 in [Appendix A](#): Global Internet Map.) Further complicating national cyber boundaries is the matter of hardware, which is often owned by foreign companies with proprietary rights to the technology underpinning the network. Also at issue is who can divert communication through pathways outside the local network, essentially enabling surveillance of another country's network.⁵⁴

Another distinct feature of the cyber domain is the invisibility cloak it offers users – criminals and states alike. Because of the way the Western internet was originally designed, message locations (internet protocol address) and senders can easily be masked through proxy servers, making attribution in cyberspace very difficult. This is especially useful for gray zone competition. Actors, including states, can conduct attacks from the shadows, hiding the identity (IP address) of the coders behind the keyboard and their link to the government. The attack victim is equally challenged to identify, hold accountable, and, crucially, justify a particular response against the perpetrator. Samuel Liles, an Associate Professor for Cyber Forensics at Purdue University, describes three layers of attribution in the cyber domain, each increasingly

⁵⁴Chris Demchak explains IP hijacking here:

<https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca>. The Federal Communication Commission's steps to remove China Telecom (and several other Chinese ICT companies) from U.S. networks in December 2020 due to the threat Demchak describes are described here: <https://www.reuters.com/article/usa-china-tech/fcc-begins-process-of-halting-china-telecom-u-s-operations-idUSKBN28K2ER>. David McCabe, "F.C.C. designates Huawei and ZTE as National Security Threats," *New York Times*, 30 June 2020, available at <https://www.nytimes.com/2020/06/30/technology/fcc-huawei-zte-national-security.html>. Huawei is #3 among vendors of submarine fiber cable market in a sample covering 2017-2021 at this link: <https://www.businesswire.com/news/home/20171030006219/en/Top-5-Vendors-in-the-Global-Submarine-Fiber-Cable-Market-from-2017-to-2021-Technavio>. Distinct from the IP hijacking, Huawei's massive share of the global submarine cable communication network is critical, as intercontinental fiberoptic cable supports 95% of internet traffic flows in an increasingly interconnected world. The submarine cable market is dominated by powerhouse multinational companies due to a high barrier to entry, and Huawei offers not only technical experience and equipment but also low prices, indicating they will likely retain a prominent role in the market for the foreseeable future.

difficult to establish: political posture, factual (technical), and legal (forensic).⁵⁵ The risk level for cyber counter measures increases as the degree of attribution decreases. Additionally, time and availability of evidence are not on the victim's side. By the time a victim can pinpoint and, requiring an even more meticulous process, provide proof of the attacker's identity, the court of international opinion (which gets a vote in gray zone competition)⁵⁶ has forgotten the fervor of its indignance at the original attack. Consequently, the victim risks more reputational damage in just retaliation than the attacker gambled with a preemptive cyber strike. This is especially true if the victim is committed to an open, connected internet. Conversely, if the victim is already viewed as a pariah state with little regard for cyber norms, it has little to lose in retaliation. Even if the victim *can* attribute the attack, what consequences is that government willing to entertain? As an example, it took the United States and Great Britain several months to publicly blame the Wannacry attack on North Korea, and even with confident attribution, President Trump's Homeland Security Advisor admitted there was little the U.S. could do in response.⁵⁷

Third, even when an actor is identified in the cyber domain, actor intent is difficult to ascertain. When states operate on foreign networks, are they conducting cyber espionage consistent with traditional, acceptable intelligence norms? Are they conducting operational

⁵⁵ Samuel Liles, "Cyber Security Defense and Attribution," Lecture by Samuel Liles, 2015-2018 Special Advisor & "Ciso in Residence," Cyber Threat Analysis, Department of Homeland Security. By Chris Demchak. US Naval War College. May 18, 2017. <http://selil.com/archives/6791>.

⁵⁶ Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law* no. 42, no. 2 (2017): 20, https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf. Regarding the lack of granularity in international law's application in cyberspace, Schmitt explains, "it will likely be left to States to address grey zones through State practice and expressions of *opinio juris*. However, because most State practice in cyberspace is classified, the bulk of the heavy lifting will likely have to be accomplished by *opinio juris*."

⁵⁷ David E. Sanger, *The Perfect Weapon: War, Fear, and Sabotage in the Cyber Age* (New York, NY: Penguin Random House LLC, 2018), 287-290.

preparation of the environment (OPE) for a planned operation? There is no easy way to resolve the “espionage-OPE distinction problem.”⁵⁸ The intent perception issue is linked to the tailored and time-sensitive nature of cyber tools.⁵⁹ Unlike a physical missile, which can be universally employed to the same damaging effect (varying solely on the caliber of the targeted defense), a cyber weapon must be customized for a precise target on a particular network. A useful example is the cyber and electronic sabotage of North Korean Musudan missile testing. Within a year of the operation’s purported success (88 percent missile failure rate), Kim Jong-Un switched to a new missile technology, making the current code obsolete.⁶⁰ The same cyber weapon could not have been repurposed against a Russian or Chinese system because of technical specificities unique to each country’s missile program and communications network. The tailored nature of cyber weapons elevates the role of OPE and incentivizes a constant presence on adversaries’ networks (as evidenced by the DoD’s “defend forward” cyber concept).⁶¹

Finally, the cyber domain is unique simply because its complexity and novelty create a sense of uncertainty and fear of the unknown among the highest level of decisionmakers.⁶² The cyber substrate is increasingly woven into the fabric of modern society, but the current cohort of

⁵⁸ Ben Buchannan and Fiona S. Cunningham, “Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis,” *Texas National Security Review Special Issue: Cyber Competition* 3, no. 4 (Fall 2020) 7.

⁵⁹ Laura Galante, Robert K. Knake, and David E. Sanger, “Cyber Conflict: The Evolution of Warfare,” *Council on Foreign Relations* Panel, Moderated by Reena Ninan (June 2018), <https://www.cfr.org/event/cyber-conflict-evolution-warfare>.

⁶⁰ Sanger, *The Perfect Weapon: War, Fear, and Sabotage in the Cyber Age*, 268-291.

⁶¹ On page five of the article cited above, Buchannan and Cunningham explain the OPE-intent link: “Much of the development and preparation for a cyber operation requires access to or occurs within adversary networks. Moreover, the accesses and payloads that make offensive cyber operations possible are often specific to a particular network: Cyber operations lack the fungibility of conventional or nuclear weapons and should be tailored to their targets in order to be effective.” Full article link here: <https://repositories.lib.utexas.edu/handle/2152/83958>.

⁶² The cyber domain is the youngest among warfighting domains and as such, the uncertainty is prevalent, even among digital natives, as there is little precedent to reference when predicting cyber operation outcomes and adversary responses in the domain.

national leaders are not digital natives.⁶³ This is not an ageist appraisal, but a practical acknowledgement that human nature influences technical solutions. Those with authority to approve cyber policy and authorize cyber operations in the U.S. government must overcome a natural aversion to unfamiliar tools. One need only observe recent Big Tech Congressional hearings to witness well-intentioned digital immigrants fumble in their attempt to govern such a pervasive, expansive, and technically based realm.⁶⁴ Such understandable discomfort among U.S. lawmakers, policymakers, strategists, and decisionmakers has potential to result in either of two types of strategic failings. On the one hand, as in Arthur C. Clarke's "Superiority," those inexperienced in technical matters can fall victim to technology worship, blind to the limits of their tools. On the other hand, leaders may be too cautious or secretive about a tool whose mechanisms and effects they do not fully understand. Either extreme is problematic. It is a mistake to view cyber weapons as a panacea, rather than a complementary tool to integrate with current capabilities because history demonstrates, most recently in the Afghanistan and Iraq wars, that technological dominance prompts an asymmetric adversary response. In cyberspace, this manifests in lawfare and gray zone tactics.⁶⁵ Leaders hesitant to wade into the ambiguity of the cyber domain may miss the significance of cyber threats short of war and fail to seize

⁶³ Chris Demchak, "Conflicting Policy Presumptions about Cybersecurity: Cyber-Prophets, -Priests, -Detectives, and -Designers, and Strategies for a Cybered World," *Atlantic Council Issue Brief* (2010): 1-2, https://www.jstor.org/stable/resrep03333?seq=3#metadata_info_tab_contents.

⁶⁴ Follow these links to coverage of Big Tech Congressional hearings over the past two years, explaining why Congressmen and women may seem out of touch or confused by the technology they seek to govern: <https://www.nytimes.com/2020/07/29/technology/congress-big-tech.html> and <https://www.cnet.com/news/some-senators-in-congress-capitol-hill-just-dont-get-facebook-and-mark-zuckerberg/> and 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.

⁶⁵ Arthur C. Clarke, "Superiority," *The Magazine of Fantasy and Science Fiction* 2, no. 4 (August 1951): 3-11, <http://nob.cs.ucdavis.edu/classes/ecs153-2019-04/readings/superiority.pdf>.

creative opportunities for U.S. influence in cyberspace.⁶⁶ The gap in leader and technical expert understanding is a temporal challenge in the cyber domain, and one gradually overcome as cybersecurity evolves into a boardroom issue and cyber tools are widely viewed as “a strategic and asymmetric force to shape geopolitics.”⁶⁷ As with all warfighting domains, competition in cyberspace is an extension of politics. The question which policymakers consistently grapple with is: what is the best way to frame competition in this complex operating environment?

On Cyberspace: Mental Frameworks for the Operating Environment

One way of framing cyber competition is as “soft war.” In his 2014 article, George Lucas describes state-sponsored hacktivism, a broad term for cyber malevolence and mischief, as a new kind of “soft war.” He explains that “soft war” has grave consequences but is usually non-kinetic and rarely results in damage to physical objects, offering the 2012 Saudi Aramco cyberattack (a computer virus) and DDoS attacks against U.S. financial institutions as examples.⁶⁸ Lucas argues that “adversaries pursuing...‘soft war’ [will be compelled to] minimize unnecessary destruction and loss of life.” Given this understanding of the domain, Lucas expresses optimism that “emergent norms” of cyber conflict as “soft war” may deter escalation

⁶⁶ Deputy Director-General for the International Institute for Strategic Studies Kori Schake provides an example from the Obama Administration of what she calls “small ball activity” to coerce adversary behavior through creative tactics. The American Ambassador in Beijing published the Beijing air quality index on the embassy website, a no-cost move risking no confrontation with Chinese leadership but holding China accountability to their own public for their poor environmental practices. (The embassy website is one of the few ways to breach the great firewall blocking Chinese internet from outside influence.) Thinking this way about Great Power Competition allows for innovative solutions which leverage American comparative advantage over authoritarian regimes. See this link for more from Kori Schake on great power competition: <https://www.csis.org/analysis/great-power-competition>.

⁶⁷ Laura Galante, Robert K. Knake, and David E. Sanger, “Cyber Conflict: The Evolution of Warfare,” *Council on Foreign Relations*, June 20, 2018, <https://www.cfr.org/event/cyber-conflict-evolution-warfare>.

⁶⁸ Lucas’s description of “soft war” as non-kinetic, cyber-enabled political sabotage is very similar to Hoffman’s definition of gray zone conflict: “nonviolent coercion as a means of political competition.” According to Lucas, nations operating in this soft, gray competitive space, “substitute cleverness and ingenuity for brute strength.”

to war or physical destruction via the cyber domain.⁶⁹ However, since the publication of Lucas's article, the cyber domain has borne out an escalation in tactics leading to physical effects, including the 2017 multibillion dollar, globally shared price of the Wannacry and NotPetya attacks.⁷⁰ While China continues to fine-tune its intellectual property theft and enable its information operations in cyberspace, a brazen Russia seems more and more willing to explicitly execute cyberattacks with physical consequences. Thus, Lucas's initial assessment of cyberconflict as "soft war" should be expanded to a framework that reflects the broadening spectrum of conflict spanning the gray zone in cyberspace, short of violence but capable of effects in the physical domain.

Josh Rovner, an Associate Professor at American University, offers a second framework: intelligence operations. Lucas draws a parallel between cyber domain soft tactics and espionage which Rovner takes a step further, suggesting that cyber operations are best viewed as an intelligence contest. In 2019, Rovner asserted, "Most cyber operations among great powers are about collecting and protecting information." In the same article, he suggested that the "race to exploit that information to improve one's relative position" is underway between Washington, Beijing, and Moscow. However, he downplays "direct sabotage of adversary systems" as less visible.⁷¹ While many of Rovner's intelligence analogies prove insightful to understanding Great

⁶⁹ George Lucas, "State Sponsored Hacktivism and the Advent of 'Soft War,'" *Ethics and Armed Forces*, Issue 2014/2, (2014): 16-23.

⁷⁰ "Multibillion dollar damage cause by Notpetya and Wannacry – Learn how Forescout Visibility Platform can Help Address," *Forescout Research and Cyber Alerts*, September 12, 2018, <https://www.forescout.com/company/blog/multibillion-dollar-damage-caused-by-notpetya-and-wannacry-learn-how-forescout-visibility-platform-can-help-address/#:~:text=A%20recent%20WIRED%20Magazine%20article,on%20Danish%20shipping%20giant%20A.P.&text=NotPetya%20and%20WannaCry%20are%20equal,percent%20device%20visibility%20is%20required.>

⁷¹ Josh Rovner, "Cyber War as an Intelligence Contest," *War on the Rocks Special Series: The Brush Past*, September 16, 2019, <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/#:~:text=The%20cyberspace%20competition%20is%20an,not%20be%20our%20best%20guide..>

Power Competition in the cyber domain, not all cyber activity is intended to gain intelligence. The problem of distinguishing adversary intent proves problematic, especially in the case of covert intelligence gathering, and makes norm-building particularly challenging.

In a separate article reviewing USCYBERCOM strategy, Rovner cautions against another framework used to understand and strategize for cyber conflict: strategic deterrence. He suggests deterrence relies too heavily on norms which will never be accepted by the revisionist China or Russia described in the U.S. NSS. He applauds a more pragmatic USCYBERCOM “persistent engagement” outlook that acknowledges the U.S. should “disrupt and degrade adversaries’ capabilities” but will never induce its enemies to quit trying.⁷² Yet, deterrence is more nuanced than Rovner allows in his argument, which means it is, in fact, a useful framework when it accounts for the unique features of the cyber domain.

A genuinely applicable strategy of deterrence begs this question: deter what? In the cyber domain, is it the U.S. goal to deter all cyber intrusions? Or, perhaps more realistically, does it hope to thwart any attacks which lead to damage to physical infrastructure? A bit more ambitious, does Washington hope to thwart Russian disinformation campaigns propagated on the internet? Or Chinese intellectual property theft via the internet? Against whom – both the U.S. and its allies? What about the cyber-enabled espionage of both of these countries? In a 2017 article, Joseph Nye, former Dean of the John F. Kennedy School of Government, offers four separate mechanisms for cyber deterrence: 1) punishment, 2) denial, 3) entanglement, and 4) norms. Referring to the oft-used Cold War deterrence analogy, he concludes, “ambiguities of attribution and the diversity of adversaries do not make deterrence and dissuasion impossible in

⁷² Josh Rovner, “More Aggressive and Less Ambitious: CYBERCOM’s Evolving Approach,” *War on the Rocks Special Series: The Brush Past*, September 14, 2020, <https://warontherocks.com/2020/09/more-aggressive-and-less-ambitious-cyber-commands-evolving-approach/>.

cyberspace, but punishment occupies a lesser degree of the strategy space than in the case of nuclear weapons.”⁷³ Underscoring the challenge of cyber deterrence, he identifies that effective deterrence is a psychological process that relies on clear communication of intent, particularly problematic in the cyber domain, where there is high risk of misperception of adversary cyber activity.⁷⁴ Nye’s approach to cyber deterrence, which applies appropriate mechanisms depending on the “who” and “what” is being deterred and appreciates the unique features of cyberspace, present a more actionable understanding of cyber deterrence.

Determining whether or not states should publicize application of these deterrent mechanisms in the cyber domain requires consideration of yet another framework: covert action. Austin Carson’s “Secret Wars: Covert Conflict in International Politics” highlights the benefits states acquire by allowing attribution in cyberspace to remain ambiguous. Using a covert action framework for the cyber domain, he suggests plausible deniability may allow states to uphold the very norms they have just violated.⁷⁵ This may explain why the U.S., while largely agreeing with much of the Tallinn Manual’s application of Just War Theory to the cyber domain, has not further codified international norms based on its findings. As Lucas also acknowledged, “the one issue in the cyber domain on which the U.S., Russia, and China seem to agree” is resisting further legislation.⁷⁶ The problem with secrecy, however, is that it is a tool better suited for authoritarian regimes. While democracies are both underpinned and advantaged by transparency

⁷³ Joseph Nye, “Deterrence and Dissuasion in Cyberspace,” *International Security* 41, no. 3 (2017): 68-69, https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266.

⁷⁴ Nye, “Deterrence and Dissuasion in Cyberspace,” 53.

⁷⁵ Sam Winter-Levy, “Keeping the Adversaries’ Secrets Secret: Review of Austin Carson’s Secret Wars,” *The Lawfare Book Review*, April 17, 2019, <https://www.lawfareblog.com/keeping-adversarys-secrets-secret>. Austin Carson is an Assistant Professor of Political Science at Chicago University who focuses on the politics of secrecy in international relations.

⁷⁶ Lucas, “State Sponsored Hacktivism and the Advent of ‘Soft War,’” 21.

in the cyber domain, secrecy and loose norms leave room in the gray zone for lawfare and aggression short of war, which favors the United States' revisionist competitors.

As the discussion above highlights, there are many perspectives on how to frame operations in the cyber domain. No single framework fits perfectly but each helps to appreciate a different aspect of the domain, where espionage, influence operations, sabotage of critical civilian systems, and jockeying among Great Powers occur simultaneously. To strategize for competition in the cyber domain, one must first understand the operating space – in this case, one that is both human-created and highly complex. Nye's nuanced conception of deterrence in the cyber domain offers especially useful insight for Great Power Competition in the cyber domain and will prove a helpful framework following a review of the limits of nascent cyber norms in shaping adversary behavior.⁷⁷

Ethics in the Cyber Domain: A Closer Look at How we Compete

Notably missing from the above frameworks is a values or ethics-based perspective of the cyber domain. George Lucas's 2014 "Hacktivism" article highlights some of the ethical concerns that have emerged over the past 20 years during which the internet has evolved into a staple of modern society. The internet has long been viewed through a utilitarian lens, a technological tool to connect and share ideas efficiently and across vast distances. Communities use it to connect, businesses to broaden customer bases, and educators to enable distance learning. Yet, the internet is also used by cyber criminals to steal information and states to sabotage one another in the gray zone of conflict. Indeed, humans engage in good and evil behavior, so unsurprisingly, the cyber substrate has been used in accordance with, and in contradiction to, its creators' intent. Not only do individual users misuse the internet, but also, as Lucas points out, states engage in

⁷⁷ Nye, "Deterrence and Dissuasion in Cyberspace," 45-46.

“hacktivism” and offensive cyber operations which cause physical damage while skirting international law.⁷⁸ Because user intent drives how a technological tool is used, including the internet, the ethical implications of cyber activity cannot be ignored as the U.S. develops its strategy going forward.

As the cyber domain increasingly connects the globe, it divides the world order into two camps: 1) those favoring an open system with power in the hands of its users, versus 2) those preferring closed systems which can be more easily wielded by authoritarian states and actors to retain power. A fundamental question: Is one of these preferences for the internet’s use more ethically “right” than the other? Certainly, the diverging models for cyberspace prompt ethical concerns, which can be viewed at two levels – users and governments. First, user data and privacy rights are respected only in a free, open internet model. These must be protected from greedy commercial companies, cyber criminals, and stealthy states seeking to garner intelligence, steal intellectual property, and spread disinformation. Thus far, unfortunately, few governing bodies exist for this purpose. From a virtue ethics perspective, internet users must maintain a healthy balance of self-respect, temperance, and respect for others while operating online. Internet providers must respect the rights to privacy among their customers without granting them so much deference as to undermine important requests for information in support of national security.

The second level of ethical concerns involves the broader international system, which will be altered depending on which model for cyber use wins out. Looking through the deontological lens, governments have a duty to ensure the citizens’ data and privacy rights and must protect its domestic netizens and private businesses from foreign cyberattacks. Within the

⁷⁸ Lucas, “State Sponsored Hacktivism and the Advent of ‘Soft War,’” 16-23.

international system, governments should collaborate to shape the rules which enable free and open communication between states while minimizing hacker threats, especially since state borders matter little in the cyber domain. Governments must respect the sovereignty of others states, but this becomes very gray in the cyber realm, and must be balanced with a responsibility to protect their own citizens from exploitation by other states.

Finally, consequentialist ethics informs the debate about the actions that both individuals and states take in the cyber domain. What cyber policy creates the best outcome for the greatest number of global netizens? This paper argues it is an open, interoperable, free internet, but securing that kind of online environment is incredibly challenging, prompting some states to take unethical actions to achieve that end. To preserve an open internet order, what consequences are acceptable, or even what effects fall short of outright conflict, is a matter still up for debate. To optimally resolve this clash of ethical frameworks in the cyber domain, the U.S. requires a cyber strategy which satisfies varying ethical perspectives while remaining true to American values of individual rights and freedom.

Already Competing Online: Current U.S. Cyber Strategy

The current USCYBERCOM Commander General Paul Nakasone's answer to the best way to defend U.S. interests in cyberspace is "Persistent Engagement." He captures U.S. government aims this way: "Our strategic concept has evolved from a 'response force' to a 'persistence force.' This persistence force will contest our adversaries' efforts in cyberspace to harm Americans, American interests...and critical public and private institutions." The new U.S. military cyber strategy also seeks to achieve superiority through persistence by degrading enemy capabilities in the cyber domain and deterring adversary attack by inflicting high costs.⁷⁹ The

⁷⁹ Nakasone, "A Cyber Force for Persistent Operations," 2.

2018 USCYBERCOM Command Vision defines persistency this way: “Cyberspace persistence is the continuous ability to anticipate the adversary’s vulnerabilities, and formulate and execute cyberspace operations to contest adversary courses of action under determined conditions.”⁸⁰ Simply put, a “persistence” approach justifies a forward presence (on adversary networks) in order to anticipate and neutralize threats to a free and open internet and American safety and interests. Consistent with the DoD’s role outlined in the 2018 National Cyber Strategy – to preserve peace through strength and protect America’s networks– the current DoD approach is more aggressive than earlier, more defensively-oriented strategies.⁸¹ It emphasizes speed over caution in responding to perceived threats. (See the nested cyber strategies in Figure 2 of [Appendix B: Nested U.S. Cyber Strategies](#).) Additionally, the “defend forward” part of the USCYBERCOM concept suggests the command believes both deterrence and international norms, alone, are insufficient to prevent attacks against American values.⁸²

The U.S. is advantaged in several ways as it competes. In 2019, General (Ret.) Joseph Dunford cited the fusion of military, economic, diplomatic, and cultural elements of power with

⁸⁰ USCYBERCOM, *Achieve and Maintain Cyberspace Superiority: Command Vision* (Washington, DC: USCYBERCOM, 2018), 5-6, <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf>. This passage captures the spirit of the new command vision: “We cede our freedom of action with lengthy approval processes that delay US responses or set a very high threshold for responding to malicious cyber activities. Our adversaries maneuver deep into our networks, forcing the US government into a reactive mode after intrusions and attacks that cost us greatly and provide them high returns. This reactive posture introduces unacceptable risk to our systems, data, decision-making processes, and ultimately our mission success. [For this reason,] The Department of Defense (DOD) is building the operational expertise and capacity to meet growing cyberspace threats and stop cyber aggression before it reaches our networks and systems.”

⁸¹ Terri Moon Cronk, “White House releases First Cyber Strategy in 15 Years,” *DoD News*, September 21, 2018, <https://www.defense.gov/Explore/News/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/#:~:text=The%20first%20new%20National%20Cyber,strength%3B%20and%20advancing%20American%20influence>.

⁸² The December 2020 CRS Cyberspace Operations Defense Primer describes the nesting of the DoD’s cyber strategy within the four pillars of the broader national cyber strategy. The primer is available at: <https://crsreports.congress.gov/product/pdf/IF/IF10537>.

a spirit of innovation as well as a strong alliance network of like-minded democracies as the U.S. comparative advantage in strategic competition (a term frequently substituted for Great Power Competition).⁸³ Importantly, America can leverage this strength in the cyber domain if it retains its status as the preferred partner of choice, a title it has enjoyed based on its ideology and willingness to live up to its purported values.

While China and Russia may choose to partner in specific areas, neither has committed to a broad, Sino-Russian autocratic alliance, nor boasts the healthy and global alliance system cultivated by the United States.⁸⁴ Still, China's economic rise and Russia's formidable information warfare capability pose a threat to the U.S. and its allies in cyberspace because their authoritarian regimes and revisionist goals would be limited by the post-World War II, Washington-led order if they chose to follow it.⁸⁵ China seeks respect among the global community without having to conform to democratic norms respecting free speech, individual privacy (especially online), and intellectual property rights. Russia's strong-man tactics and sneaky online manipulation are disadvantaged in a rules-based order which condemns its corruption and opportunism. Both oppressive regimes bristle at human rights standards which infringe on their harsh tactics to control political dissidents and ethnic minorities. Beijing and Moscow ignore UN calls for increased transparency and excel in the gray zone because they hope to overturn the current rules-based international order and only selectively adhere to the

⁸³ Jim Garamone, "Dunford Describes U.S. Great Power Competition with Russia, China," *Defense.gov*, March 21, 2019, <https://www.defense.gov/Explore/News/Article/Article/1791811/dunford-describes-us-great-power-competition-with-russia-china/>.

⁸⁴ Bruno Macaes, "Russia to China: Together we can rule the world," *Politico*, February 21, 2019, <https://www.politico.eu/blogs/the-coming-wars/2019/02/russia-china-alliance-rule-the-world/>.

⁸⁵ Michael Mazarr, Oriana Mastro, Christopher Preble, and Kori Shake. "Great Power Competition," *Defense 2020*, podcast audio, moderated by Kathleen Hicks, January 15, 2020, <https://www.csis.org/analysis/great-power-competition>.

norms that underpin it as it suits their needs. This demonstrated willingness to subvert global norms – especially cyber norms – which do not align with their interests advantages China and Russia in Great Power Competition because the U.S. is bound by the norms which undergird the American-led liberal world order.

Reviewing a parallel moment in history offers a final, cautionary reflection on modern Great Power Competition in the cyber domain. A century ago, Germany found itself in the same position as China and Russia. Britain led a Euro-centric order at the time, and Berlin sought to upset the global balance through war, which ultimately transpired in 1914. In recent years, U.S. leaders have repeatedly asserted they do not wish for Great Power Competition to become Great Power War,⁸⁶ and how we choose to compete in the pervasive cyber domain, where much of gray zone conflict occurs, is a significant factor in reducing the likelihood of either Russia or China escalating to violence to change the current balance of power.⁸⁷ Norms can sometimes be effective in restraining state behavior, but as the next section highlights, emerging cyber norms have thus far failed to do so, prompting the U.S. to develop its current, more aggressive cyber strategy.

⁸⁶ Defense Forum Washington. “Remarks from GEN Mark A. Milley, USA, Chairman of the Joint Chiefs of Staff,” U.S. Naval War Institute, December 14, 2020, video, 24:08, <https://www.youtube.com/watch?v=CVU9CY4PKvI>.

⁸⁷ Before leaving this section, it is worth noting that many defense experts disagree with the conflation of competition with Russia and China in the NSS, since Russia is a declining power (albeit one with nuclear weapons and United Nations’ veto power), and China is a rising power. I agree with this concern and appreciate the DoD’s recent distinction of China as the number one threat to U.S. national security. However, for the purpose of this paper, I focus more on unique aspects of each country’s competitive approach, especially its cyber strategy, rather than identifying the top overall competitor. For more on Great Power Competition and the need to distinguish the Chinese and Russian threat, see Vice President for Defense and Foreign Policy Studies at the Cato Institute, Chris Preble’s comments at this link: <https://www.csis.org/analysis/great-power-competition>.

The Current Stalemate: Existing Cyber Norms

Because most competition in the cyber domain takes place in the gray zone short of armed conflict, coercion via the cyber domain is becoming an increasingly popular tool for states. It is especially problematic, then, that incomplete norms govern competition in this domain, especially for offensive actions. The Tallinn Manuals offer an expert application of international law to cyber activities. The second volume, specifically, addresses cyber operations conducted in the gray zone outside of armed conflict. These documents provide a valuable reference and important launch point for future discussion. However, the evolution of cyber conflict over the past ten years, from Stuxnet to Wannacry to NotPetya to Solar Winds, indicates that the areas of non-consensus among experts and states will continue to be exploited at the expense of billions of dollars in global chaos and destruction. Until acceptable norms can be established, agreed upon by influential global actors, and incentivized for all major cyber powers, this trend may escalate. Separately, if states' disruptive behavior in the cyber domain is left unchecked by the Liberal World Order, the internet will remain an effective tool for authoritarian regimes with no regard for Western norms of open internet to prosecute effects with little backlash and minimal resources invested.

Relatedly, the recent US shift to a more aggressive cyber strategy has fueled a rigorous debate over the value of norms in mediating adversary behavior in cyberspace.⁸⁸ In its comprehensive 2020 report, the Cyberspace Solarium Commission highlights the insufficiency of the status quo in cyberspace and identifies the need to strengthen and enforce international norms. While admirable in its scope, detail, and call to action, the report implementation

⁸⁸ Michael P. Fischerkeller and Richard J. Harknett, "Persistent Engagement and Tacit Bargaining: A Path toward Constructing Norms in Cyberspace," *Lawfare*, November 9, 2018, <https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace>.

mistakenly assumes “the U.S. and others have agreed on norms of responsible behavior in cyberspace.”⁸⁹ This assumption is disproved by the areas of Tallinn Manual non-consensus which have left a gray zone that states have exploited in cyber conflict over the past decade.⁹⁰ In 2013 a Group of Governmental Experts at the United Nations (UNGGE) agreed that international law, including the UN Charter, applied to Information and Communications Technologies (ICTs) and was “essential” to maintaining peace and stability, and an “open, secure, peaceful and accessible ICT environment.” In 2015, this group, which included representatives from the United States, China, and Russia, explicitly directed states to respect national sovereignty in cyberspace and agreed that peacetime norms prohibited attacks on critical infrastructure.⁹¹ Yet, these agreements have had little effect on states’ ability to bully weaker states, spread disinformation, and steal intellectual property in the cyber domain, all with minimal consequence outside of hollow condemnation.⁹² Undermining the UNGGE’s

⁸⁹ Sang Lee, Ainsley Katz, Karrie Jefferson, Val Cofield, and Laura Bate, “The Cyberspace Solarium Commission on Norms,” *Council on Foreign Relations Blog*, April 16, 2020, <https://www.cfr.org/blog/cyberspace-solarium-commission-norms>. See a complete list of the UNGGE’s eleven non-binding norms on pages 7-8 of this UN Report: <https://undocs.org/A/70/174>.

⁹⁰ Michael Schmitt’s description of gray zones in cyber law highlights areas of non-consensus which leave room for “asymmetrical lawfare,” advantaging states who do not conform to the rule of law. Schmitt is the lead author of both Tallinn Manuals and an expert on cyber law. His article is linked here: https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf.

⁹¹ Microsoft. “Protecting People in Cyberspace: The Vital Role of the United Nations in 2020” (2019): 3, <https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf>.

⁹² As Jason Healey and Robert Jervis point out, “Many destabilizing, brazen, and reckless attacks have not violated the letter of U.S. norms [because these norms are not] specific, binding, and global.” They also highlight the challenge ill-defined norms pose to clear communication, an important feature of effective deterrence: “It is particularly difficult in the cyber arena to signal resolve, intent, or displeasure because there are few accepted rules and no clear escalation ladders. Their research is available here: <https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/>; Jacquelyn Schneider, “A Strategic Cyber No-first-use Policy? Addressing the U.S. Cyber Strategy Problem,” *The Washington Quarterly* 43, no. 2, 170-172. Hoover Institute Fellow Jacquelyn Schneider provides these examples of how efforts at establishing norms have largely failed to stop coercive behavior in cyberspace: “Despite the efforts of the Obama administration [to establish a norm forbidding attacks against critical infrastructure], cyberattacks and operations against critical infrastructure grew more sophisticated and normalized tools of state coercion. The 2016 Russian cyber-enabled operation to influence the US elections, Russian attacks on Ukrainian power grids later that year, and North Korean and Iranian attempts to extort

credibility, the 2015 ostensible celebration of cyber norms among UN members preceded the Russian NotPetya attack, U.S. Persistent Engagement/Defend Forward Strategy (in which the U.S. disregards others' network sovereignty), and a massive Chinese cyber spying campaign.⁹³

Additionally, current norms do nothing to govern the contest taking place to influence the nature of the modern internet – the open, interconnected system for the free expression of ideas and exchange of commerce endorsed by the United States versus the closed, authoritarian system where cyber borders are distinct, which is exported globally by China and Russia. In any case, blatant disregard for professed norms suggests that international cyberspace norms may be critical to stability in the domain, but are amorphous – certainly, unenforceable. This research explores the degree to which the United States Government should promote cyberspace norms, not strictly from the legal perspective so thoroughly explored in the Tallinn Manuals, but through a holistic application of traditional ethical frameworks and U.S. values.

Change in U.S. Policy: Offense vs. Defense

Since states have thus far failed to agree on global cyber norms with enough granularity to reduce the gray zone,⁹⁴ the U.S. must find a way to win in that nuanced competition space. Successful competition, as defined in the NSS and NDS, means protecting, sustaining, and propagating the U.S. free and open internet. As described above, under the Trump

money from the US financial sector dating back to 2014 all demonstrated the increasingly front-line role of critical infrastructure in state-led cyberattacks.” While I disagree with her assessment that a no-first-use cyber policy would be any more successful in mediating adversary behavior in cyberspace, given their preference for a closed, controlled internet, her concerns regarding the U.S.’ hypocrisy in professing but not adhering to norms are valid. Schneider’s work is linked here: <https://doi.org/10.1080/0163660X.2020.1770970>.

⁹³ The Chinese cyber spy campaign included open source collection by a private Chinese firm Zhehua (on behalf of China's Ministry of State Security and the People's Liberation Army) on 2.4 million individuals and 650,000 organizations from around the world. The story broke in September 2020 and is covered in detail at this link: <https://www.dw.com/en/zhenhua-data-leak-exposes-chinas-new-hybrid-warfare/a-55083540>.

⁹⁴ Schmitt, “Grey Zones in the International Law of Cyberspace,” 20.

administration, the U.S. opted to achieve these ends by adopting a more aggressive, offensive posture, rather than just shore up cyber defenses in anticipation of more gray zone hacks. A persistent engagement approach, operating forward on adversary networks, is intended to increase responsiveness given the frequency of cyberattacks over the past decade (recall the tailored nature of cyber tools for each network). To enable a more aggressive strategy through policy, President Trump signed National Security Presidential Memorandum 13 (NSPM-13), which streamlined decision-making authority for executing offensive cyber operations, including offensive countermeasures. Some scholars have expressed concerns about this approach, which departs from the Obama administration's more consensus-based and deliberate decision-making process.⁹⁵ While the Biden administration may choose to dial back the offense, or at least reinstate a more robust approval process, it is worth considering what logic supports a more forward, aggressive cyber posture.

In addition to the advantages of defending forward – OPE tailored to specific networks to increase responsiveness and freedom of action for a preemptive strike – Naval War College Cybersecurity Professor Chris Demchak describes five advantages for the offense in the cyber

⁹⁵ Sydney J. Freedberg, Jr., "Trump Eases Cyber Ops but Safeguards Remain," *Breaking Defense*, September 17, 2018, <https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/>. This 2018 Breaking Defense report describes the effects of NSPM-13 on U.S. offensive cyber operations: "It delegates to the secretary of defense certain cyberspace authorities to do cyber effects operations for a particular mission." NSPM-13 remains classified, so the exact mechanism for streamlining decisions is unclear. However, cybersecurity specialist Dustin Volz reported the following in 2018, when the memorandum was signed by President Trump: "John Bolton, President Trump's national security adviser, confirmed during a press briefing that the old rules [regarding cyber weaponry approval] had been replaced by new classified guidance intended to empower the Defense Department with more flexibility to launch offensive cyber strikes without first needing to vet those decisions through an elaborate interagency process." President Trump's National Security Advisor at the time justified the action this way: "Our presidential directive effectively reversed those restraints, effectively enabling offensive cyber operations through the relevant departments," Mr. Bolton said. "Our hands are not tied as they were in the Obama administration." The full Wall Street Journal article is available at: <https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729>. An important clarification: Current at this paper's publication, POTUS still retains final strike authority for major U.S. offensive cyber strikes.

substrate. First, it is easy to scale organizations and operations through global communications. Just as robots are a tool in land warfare, cyber bots can expand an attacker's force in cyberspace. Second, physical proximity can easily be overcome as attackers quickly reach across thousands of miles with high-speed internet access. Third, targeting in cyberspace is precise, and, since physical distance is not a factor, attackers can strike multiple targets simultaneously. Fourth, attackers can choose when and where to reveal their tools and techniques, which are usually kept masked, so the code cannot be either exploited (like Mimikatz) or defended against. Finally, opaqueness in attack origin makes deniability easier for the attacker.⁹⁶ The 2018 NotPetya attack exemplifies many of these advantages. The Russian worm was inserted through a backdoor Ukrainian company, Linkos Group. The malware rapidly propagated across two thousand targets worldwide, destroying hard drives in sixty-five countries,⁹⁷ including the U.S., and causing over \$10 billion in corporate loss. Against this malware, "distance was no defense."⁹⁸ The attack leveraged two hacker exploits: EternalBlue, leaked from the NSA, and Mimikatz, open-source code from a French security researcher. These two, together, were a lethal combination of code which could bypass Microsoft patches. Despite NotPetya's global reach, Russia has yet to face severe consequence for the gross damages inflicted in the attack, which cost its victims ten times what the attackers paid to launch, reinforcing the benefits of the offense.

⁹⁶ Chris Demchak. "Three Futures for a Post-Western Cybered World." *Military Cyber Affairs* 3, no. 1:6 (2018): 2.

⁹⁷ Sanger, *The Perfect Weapon*, 291.

⁹⁸ Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired Magazine*, August 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>. Although cybersecurity experts still argue over the mysteries of NotPetya, including whether or not the billions in dollars of damage was collateral damage for a Russian political message targeting Ukraine, they agree it could occur again on a larger scale. This suggests that the benefits of the offense in cyberspace, at least for authoritarian regimes with little regard for the current international order, persist today.

Organizational culture also plays a role in strategy development; the predisposition for an offensive posture is baked into the military psyche. Generations of military leaders have clamored for action, sometimes leading to the militarization of foreign policy.⁹⁹ Even America's most celebrated general, George Washington, struggled to exercise restraint with his smaller Colonial force, failing to stay true to a Fabian strategy of war in his eagerness to take the fight to the enemy.¹⁰⁰ Military will to win and superior planning capability often push leaders toward action, even when restraint is more prudent. In America, this aggressive mindset is not simply a historic trend, but also grounded in doctrine.¹⁰¹ While Carl von Clausewitz describes the defense as the stronger form of warfare,¹⁰² Army Doctrinal Publication (ADP) 3-90 describes the offense as "the ultimate means commanders have to impose their will on the enemy force," and, "the decisive form of war."¹⁰³ The translation into the cyber domain is rather vague. In Joint Publication (JP) 3-12 offensive cyber operations are "missions intended to project power in and through cyberspace."¹⁰⁴ While the offensive characteristic of "audacity" does not appear in JP 3-

⁹⁹ Avner Offer, *The First World War: An Agrarian Interpretation* (Oxford: Clarendon Press, 1991), 364. In his analysis of the failure of the German U-Boat campaign to achieve decisive strategic effects in World War I, Offer explains the military bias for action, regardless of the nature of the problem. Kori Schake, in the linked CFR podcast, also suggests that military planning prowess often puts defense leaders out ahead of other government departments in strategy development. Great Power Competition Podcast, here: <https://www.csis.org/analysis/great-power-competition>; Garamone, 2020. In the modern counter-terrorism fight, the propensity of both U.S. Presidential administrations to use drones represented an urge to take military action, even if efficacy was questionable. Larry Lewis and Diane Vivrichek offer a more robust discussion on drone war in their 2016 book, available here: <https://www.hsdl.org/?abstract&did=798675>.

¹⁰⁰ John Ferling, *Whirlwind: The American Revolution and the War That Won It* (New York: Bloomsbury Press, 2015), 172.

¹⁰¹ Laura Galante, Robert K. Knake, and David E. Sanger, "Cyber Conflict: The Evolution of Warfare," <https://www.cfr.org/event/cyber-conflict-evolution-warfare>.

¹⁰² Clausewitz, *On War*, 358.

¹⁰³ U.S. Army, *Offense and Defense*, Army Doctrinal Publication 3-90, (Washington DC: Headquarters, U.S. Army, 2019), 3-1.

¹⁰⁴ Department of Defense, *DoD Dictionary of Military and Associated Terms*, (Washington DC: Headquarters, Department of Defense, 2020), 158.

12, the cyber publication leads with a charge from General Nakasone to “aggressively defend our networks.”¹⁰⁵ Additionally, the architects of the new strategy suggest it “reorient[s] U.S. cyber strategy around continuous action”¹⁰⁶ indicating a spirit of action permeates all branches of service and all domains through a U.S. military culture which rewards initiative.

Not only is the offense advantaged in the cyber domain, and the DoD biased toward an action-oriented approach, but the defense is disadvantaged in many ways in modern democratic societies. An open internet is home to interconnected socio-technological-economic systems (STEs) and it is tough to deny an attacker – criminal or state-affiliated – access when there are so many points of entry. Additionally, the explosion of largely unregulated digital media outlets, including social media, are prime targets for adversaries wishing to undermine the foundations of democracy: tolerance among different societal groups and rigorous debate of differing ideas based on a common set of facts. Vulnerabilities also increase with the complexity of the computer system, suggesting that more technologically developed countries like the U.S. and many of its allies will be at greater risk for attack than developing countries lacking robust digital infrastructure. The fast pace of innovation keeps the defense guessing as to which paths an attacker will take to attain technical surprise.¹⁰⁷ Cornell University Associate Professor of Science and Technology Rebecca Slayton explains that with so many vulnerabilities, “it is unlikely that the defense will be able to find and patch every vulnerability before the offense

¹⁰⁵ Department of Defense, *Cyberspace Operations*, Joint Publication 3-12, (Washington DC: Headquarters, Department of Defense, 2018), II-1; Audacity is described in ADP 3-90 as “dispelling uncertainty by acting decisively.” The publication encourages acting, “aggressively to seize the initiative” and “continuously engaging” the enemy. While the term, audacity, is not used in JP 3-12, it is a characteristic reflected in the DoD’s current “Persistent Engagement” cyber strategy.

¹⁰⁶ Fischerkeller and Harknett, “Persistent Engagement and Tacit Bargaining: A Path toward Constructing Norms in Cyberspace,” 1.

¹⁰⁷ Healey and Jervis, “The Escalation Inversion and Other Oddities of Situational Cyber Stability,” 19.

finds and exploits it.”¹⁰⁸ Exacerbating these network liabilities is the role of human error in cybersecurity, which has been the cause of nearly every instance of intrusion on U.S. networks.

Certainly defense is not futile, but as Joseph Nye indicates, with such a large attack surface where vulnerabilities can be exploited, entanglement is a critical complement to norms and strict denial in preventing attacks.¹⁰⁹ In other words, potential attackers will be deterred not only by international expectations and robust and resilient cyber defense, but also because their interests are enmeshed with those of their potential victims in an interdependent global internet system. Thus, even though an open internet system creates vulnerabilities, an interconnected online environment increases the tools democracies have to deter malign behavior in cyberspace, an important consideration for Washington strategists grappling with the cyber offense-defense-norms balance.

Democratic preference for an interconnected international network stands in stark contrast with nondemocratic nations who “close their cyber borders” (think: Chinese firewall) and “extract technology and concessions for access”¹¹⁰ (think: Chinese coercive diplomacy).¹¹¹

¹⁰⁸ Rebecca Slayton, “What is the Cyber Offense-Defense Balance?” *International Security* 41, no. 3 (2017): 88.

¹⁰⁹ Nye, “Deterrence and Dissuasion in Cyberspace,” 50, 56-57. Concerning *why* denial does not work against major states, even if it can achieve relative success against nonstate actors and cybercriminals, “[state] intelligence services can formulate an advanced persistent threat. With time and effort, a major military or intelligence agency is likely to penetrate most defenses.” Related, Nye offers this important assessment of the consequences of the interdependence between private cybersecurity companies and government networks: “There is a huge hole in deterrence theory if we are going to depend on denial to save us. While hardened military networks seem safe, there are points of entry across the system because of the proliferation of third-party contractors and simple human error.” The recent Russian Solar Winds hack provides an excellent example of the risks inherent in private-government integration in cyberspace. Read more about that cyber espionage attack here: <https://www.wired.com/story/russia-solarwinds-hack-roundup/>.

¹¹⁰ Demchak, “Three Futures for a Post-Western Cybered World,” 14-15.

¹¹¹ The White House, *United States Strategic Approach to the People’s Republic of China*, 4-5. The counter-PRC strategy provides specific examples of scenarios when Chinese cyber espionage leads to intellectual property theft. These include when the PRC: “(1) requires or pressures United States companies to transfer their technology to Chinese entities; (2) places substantial restrictions on United States companies’ ability to license their technology on market terms; (3) directs and unfairly facilitates acquisition of United States companies and assets by domestic firms to obtain cutting edge technologies; and (4) conducts and supports unauthorized cyber intrusions into United States

The advantages of the offense and disadvantages of the defense are not equally enjoyed by democratic and authoritarian regimes. This is because the nature of the government plays a key role in determining its internet model of open or closed networks, globally connected vs. strict cyber borders. China, especially, has a small number of national gateways, minimizing its cyberattack surface.¹¹² In his recent book, *New York Times* Correspondent David Sanger argues that cyberweapons are, in fact, tailor made for authoritarian regimes. Dissatisfied with the western-centric world order, they have far less to lose by ignoring cyber norms by targeting civilian infrastructure. Furthermore, he offers: “There’s a low cost of entry [in cyberspace], it’s largely asymmetrical, there’s some degree of anonymity and stealth in its use. It can hold large swaths of nation-state infrastructure and private-sector infrastructure at risk. It’s a source of income.”¹¹³ This makes it a prime weapon for authoritarian adversaries to wield against open, highly digital cyber systems whose democratic governments cannot easily retaliate against its own closed-off networks. In any case, these democratic countries presumably adhere to international laws which limit the proportionality and target distinction of the response.

companies’ networks to access sensitive information and trade secrets.” General (Ret.) Dunford captures the Chinese intellectual property theft this way: “If a U.S. company does business in China, they will automatically be required to have a cell of the Communist Party,” the chairman said. “That is going to lead to [that company’s] intellectual property going to the Chinese military.” Link to article here: <https://www.defense.gov/Explore/News/Article/Article/1791811/dunford-describes-us-great-power-competition-with-russia-china/>. The Australian Strategic Policy Institute provides an excellent review of Chinese coercive diplomacy tactics against U.S.-allied Western democracies and private companies, including in-depth case studies, here: <https://www.aspi.org.au/report/chinese-communist-partys-coercive-diplomacy>. The authors highlight, the CCP doesn’t make the link explicit and tends to deny responsibility,” which is particularly suited to the cyber domain, where actors can easily mask identity and state affiliation.

¹¹² Chris Demchak and Yuval Shavitt. "China’s Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom’s BGP Hijacking." *Military Cyber Affairs* 3, no. 1:7 (2018): 1-9. <https://doi.org/10.5038/2378-0789.3.1.1050>.

¹¹³ Sanger, *The Perfect Weapon*, 2018, 286.

Considering the two options, and the sliding scale in between, the DoD's USCYBERCOM asserts that a strong offense is the best defense,¹¹⁴ while Columbia University's Healey and Jervis argue exactly the opposite – “a strong defense is the best defense.”¹¹⁵ Before determining which approach is right – Washington's previous, more defensive posture, or more recent, offensive “superiority through persistence” – it is necessary to examine the tough tradeoffs involved with either strategy. Healey and Jervis acknowledge the compromise in their most recent publication, “The Escalation Inversion and other Oddities of Situational Cyber Stability.”

If the United States wants a universal order, accepted by friends and rivals alike, it will have to make very serious compromises. U.S. decision-makers may decide...that they are unwilling to make such compromises, so that for the duration of the digital age, the United States will have to enforce its preferences through power... But if cyberspace encourages positive feedback it is unlikely to survive the conflict in anything like its form today. At the very least, the United States should acknowledge that adversaries see U.S. actions and preferences as destabilizing (at least to their own domestic orders). U.S. policy should aim not to combat adversaries but rather destabilization itself.¹¹⁶

The assumption underlying their conclusion is critical: stability is more important than ensuring the Western model for the internet is propagated globally. Chairman of the Joint Chiefs of Staff (CJCS), General Mark A. Milley, underscores the importance of stability, counseling against allowing Great Power Competition to escalate into Great Power War.”¹¹⁷ However, the DoD's aggressive “persistent engagement” strategy professes to contest our adversaries' efforts in cyberspace to harm Americans and American interests and hack our most critical public and

¹¹⁴ USCYBERCOM, *Achieve and Maintain Cyberspace Superiority: Command Vision*, 7.

¹¹⁵ Healey and Jervis, “The Escalation Inversion and Other Oddities of Situational Cyber Stability,” 25.

¹¹⁶ Healey and Jervis, “The Escalation Inversion and Other Oddities of Situational Cyber Stability,” 27.

¹¹⁷ Defense Forum Washington: Remarks from GEN Mark A. Milley, USA, Chairman of the Joint Chiefs of Staff,” 14 December 2020, U.S. Naval War Institute, video, 24:08, <https://www.youtube.com/watch?v=CVU9CY4PKvI>.

private institutions. Through this policy, the DoD is prioritizing taking the fight to the enemy over promoting global stability.

I disagree with this implied tradeoff: either the U.S. must remain aggressive, risking (legitimate) accusations of its hypocrisy and destabilizing behavior, or the U.S. must renounce its commitment to defending a free and open internet order. A creative combination of exquisite defense and determined diplomacy offers a third, unexplored alternative. This alternative is best illustrated through scenario forecasts.

The Cyber Quadrant: Possible Future Scenarios

Is offense the best defense in the cyber domain? The graphic below considers four future scenarios – The Avengers, Captain America, Gotham City, and Roadrunner – varying based on commitment to cyberspace norms and an offensive versus defensive posture. Each scenario leads the U.S. either closer to or further from its values and its desired outcome – a free, open internet. Also important, each outcome depends, in part, on the decisions of both allies and adversaries. For example, cyber norms are valuable only to the extent they shape state behavior. That includes the actions of our partners, revisionist peer powers, and third-world countries recently joining the digitally connected world. As referenced above, current espoused norms have not yet produced a decisive effect on state behavior.¹¹⁸ In this graphic, cyber norms refer to global norms as outlined by the United Nations Group of Government Experts (UNGGE), acknowledging that while these are universally backed they are not yet globally accepted. These include: protecting human rights and free expression on the internet, ensuring the integrity of

¹¹⁸ The first-ever, 2019 “global meeting on peace and stability in cyberspace” (OEWG – Open Ended Working Group), paradoxically proposed by a Russian resolution November 2018 “to establish, alongside the GGE, a ‘more democratic, inclusive, and transparent’ body for studying responsible state behavior and cooperative measures in cyberspace” was deemed “historic” in the linked *Council on Foreign Relations* blog, but was it productive? Certainly, it was well-attended, with over 80 delegations. However, given the recent Russian Solar Winds hack, it represents another ruse by authoritarian regimes to deflect from their regular, blatant violation of the UNGGE’s 2015 norms. The event is described here: <https://www.cfr.org/blog/first-global-meeting-cyber-norms>.

supply chains, and “state responsibility to prevent malicious use of ICTs in their territory.”¹¹⁹

Additionally, “high norms” (far right side of the chart) indicates these norms are binding for the U.S., regardless of whether they are universally accepted, a concept addressed in the final recommendations section.

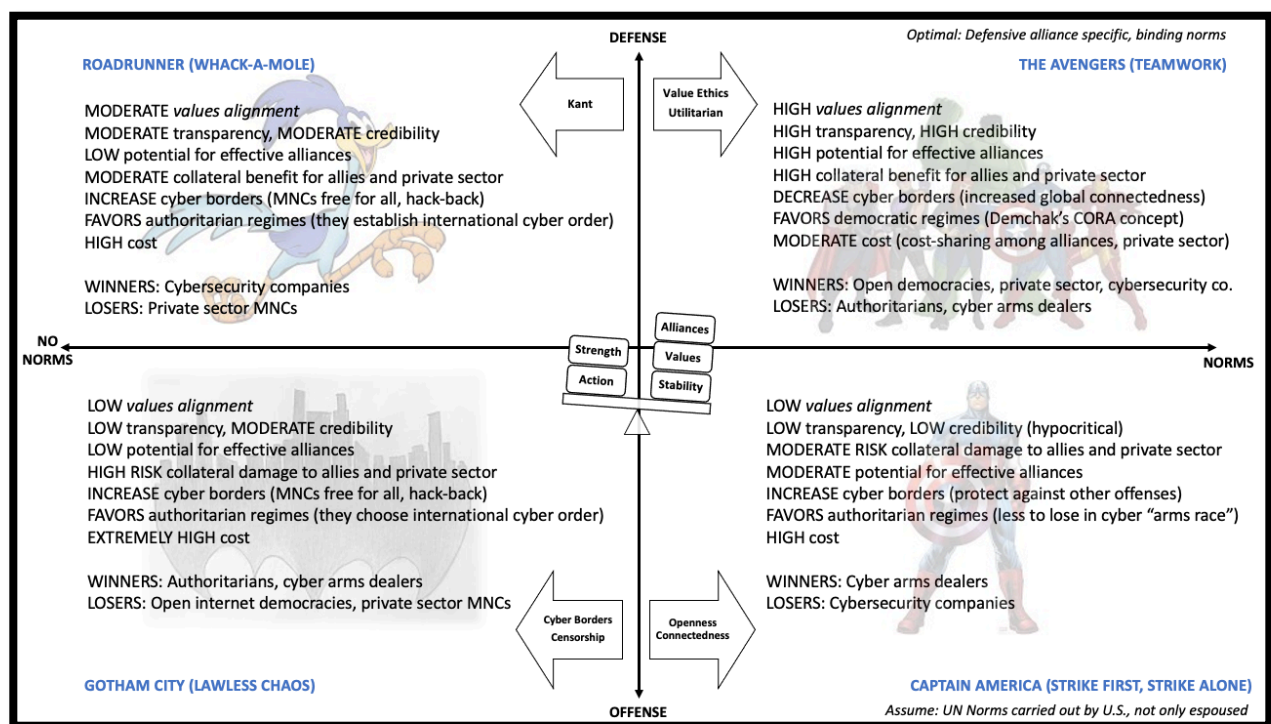


Figure 3. Cyber Forecast: Four Potential Future Scenarios

The future scenarios illustrate tradeoffs. A move toward norms risks a scenario where the U.S. respects cyber sovereignty while its adversaries disregard it. In this scenario, adversaries continue interfering on U.S. networks, disadvantaging the U.S. Yet, U.S. global leadership on norms adherence is consistent with its values: liberty, equality, opportunity, and individual rights and freedoms. U.S. strong norms sponsorship in international bodies like the UN and support for the independence of the International Telecommunications Union (ITU) and Internet Corporation

¹¹⁹ United Nations General Assembly, 70th Session, Developments in the field of information and telecommunications in the context of international security,” A/RES/70/237 (New York: UN, 2015), <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf>.

for Assigned Names and Numbers (ICANN) positions the country on the moral high ground, which makes its leadership of a Liberal World Order and open internet order more credible.¹²⁰ Also, strengthening norms favors Washington's democratic partners because it reduces gray areas in international law, undermining authoritarian regimes' ability to claim their actions are legitimate in the eyes of the international community.

By holding itself accountable to specific, binding cyber norms, the U.S. can condemn without duplicity Chinese and Russian efforts to subvert the very educational, economic, and political institutions on which democracies depend. Unambiguous norms undercut authoritarian regimes' gray zone tactics to undermine trust, transparency, and citizens' tolerance for one another and these very same institutions.¹²¹ Through higher adherence to norms, U.S. behavior in cyberspace is not only more predictable to adversaries (demonstrates restraint), but also consistent for its allies and exemplary for new (state) entrants to the cyber domain. Predictable, norms-aligned state behavior creates the stability necessary for an open and connected global cyber domain in which commerce and ideas are freely exchanged.

There is an argument to be made that moving away from norms undermines effective alliances, in which partners must know what to expect of the U.S. This side of the chart relies more on independent American strength and action to intimidate adversaries and deter cyberattacks and less on teamwork for the same purpose. Still, if the U.S. publicly admits that norms have failed to achieve results – that is, failed to deter aggression by revisionist powers in the cyber domain – then, it appears less hypocritical in preemptively striking against adversaries

¹²⁰ Anthony Craig and Brandon Valeriano, "Realism and Cyber Conflict: Security in the Digital Age," *E-International Relations Collection*, February 3, 2018, <https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/>.

¹²¹ Demchak, "Three Futures for a Post-Western Cybered World," 2.

or conducting OPE on sovereign networks, as is consistent with the current USCYBERCOM strategy and NSPM-13. Decreased norms commitment by the U.S. will likely be mirrored by adversaries, increasing risk for cyberattacks. In the same fashion, decreasing norms alignment increases the threat of damage to allies and the private sector, consistent with the WannaCry, Notpetya, and Mirai attacks which inflicted damage – intentional and collateral – at home (in the U.S.) and abroad.¹²² Additionally, a more anarchic (less norms-aligned) cyberspace prompts states to reinforce distinct cyber borders to protect cyber sovereignty. This is a win for authoritarian regimes who already seek to segment the internet (reduce openness) for better online control of their domestic populations.

Movement along the Y-axis in the chart, emphasizing either defense or offense in U.S. cyber strategy, demonstrates similar tradeoffs. For instance, a defensive posture promotes more collaboration among allies. That is, defensive techniques, practices, and programs are more shareable than offensive tools, which are more useful as state secrets.¹²³ Zero-day exploits, for example, are only valuable for their ability to capitalize on exclusive awareness of a system's weaknesses.¹²⁴ Share that code or expose that network vulnerability, and the offensive advantage is lost. On the contrary, the effects of secure software, cybersecurity software and other defensive tools are only enhanced when provided to allies and private sector partners because a broad, integrated, well-defended network raises the cost for adversary attack by minimizing

¹²² John Snow, "Top 5 most notorious cyberattacks," *Kaspersky Daily Blog*, November 6, 2018, <https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/>.

¹²³ Technological virality is the tendency of tech solutions, from nuclear weapons to cyber weapons, to spread from the nation of origin to other states. Defense-oriented cyber solutions like secure software and cybersecurity tools provide increased promise when they are shared. Like a vaccine, they offer a neutral resilience against common bad actors.

¹²⁴ Zero-day vulnerabilities are defined by Cybersecurity company FireEye here: <https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html>.

backdoor vulnerabilities and hardening targets to make adversary system access and OPE more difficult.¹²⁵ Not only does defense increase adversary costs, it is also commercially viable, doubly advantaging America. A movement toward a defense-focused strategy increases a willingness for transparency and is complemented by a high norms environment (Avengers Scenario in the chart). In a low-norms environment, a defensive posture becomes more costly, as the threat risk for adversary cyberattack is much higher and more likely to come without warning (Roadrunner Scenario).¹²⁶ Especially in a low-norms environment, a defensive posture may be perceived as passive, reactionary, or weak. A challenge in this environment, a defensive posture calls for restraint among a military cohort accustomed to action.

Shifting toward a more offensive strategy reduces constraints on U.S. actions, a point highlighted in both USCYBERCOM Command Vision and NSPM-13.¹²⁷ A more offensive posture signals strength to adversaries in that it demonstrates a willingness to act and decreases an adversary's ability to predict when and where the U.S. will strike. The emphasis on offense comes at high cost, particularly in a low norms environment where risk of escalation is more likely (Gotham City Scenario). When coupled with low norms adherence, an offensive posture also justifies the authoritarian push for stricter cyber borders to protect state interests amidst the lawless cyber chaos. While the phrase "state sovereignty in cyberspace" seems reasonable, it

¹²⁵ Brandon Valeriano and Benjamin Jensen, *The Myth of the Cyber Offense: The Case for Restraint* (Washington, DC: Cato Institute, 2019), 8, <https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint>.

¹²⁶ In a low norms environment, the threat and scope of cyberattack increases (nothing is considered taboo in cyberspace). A U.S. defensive posture in this environment means the USCYBERCOM is not operating forward on adversary networks and has less intelligence regarding these likely, impending attacks. This Roadrunner scenario leads to a fruitless game of whack-a-mole in which the U.S. is striking at enemy intrusions on its own network and paying large sums to respond to breaches when they do occur.

¹²⁷ The USCYBERCOM vision is available here: <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010>. A description of NSPM-13 is available here: <https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/>.

portends a more closed ICT environment and usually signifies a tradeoff with user privacy.¹²⁸

Some even go so far as to describe cyber sovereignty as “the beginning of cyber fascism.”¹²⁹

While the U.S. government spends billions on defensive cybersecurity,¹³⁰ many experts assess offensive weapons as more expensive, in part because they must be tailored to each adversary network.¹³¹ For instance, the U.S. invested tens of millions in Stuxnet, and its follow-on Nitro Zeus, which targeted infrastructure in a single country.¹³² Aside from monetary costs, an offensive strategy also risks more collateral damage (money, lives) to both allies and the private sector. Another consideration associated with an offensive cyber strategy is U.S. credibility. This is nuanced. The U.S. risks appearing weak or feckless if it does not project

¹²⁸ Emily O. Goldman, “From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy,” *Texas National Security Review: The Strategist*, 3:4, (Fall 2020): 85, <http://dx.doi.org/10.26153/tsw/10950>.

USCYBERCOM and NSA cyber strategist, Emily Goldman, describes cyber sovereignty as a means for states “to censor and regulate the internet to prevent exposing their citizens to ideas and opinions deemed harmful by the regime.” She explains that cyber sovereignty puts a premium on regime security at the expense of individual liberty and creates an internet model that favors state regulation over multi-stakeholder governance (for the latter, businesses, civil society, research institutions, and NGOs contribute to dialogue and solutions).

¹²⁹ Andrea Limbago, “The global push for cyber sovereignty is the beginning of cyber fascism,” *The Hill*, December 14, 2016), <https://thehill.com/blogs/congress-blog/technology/310382-the-global-push-for-cyber-sovereignty-is-the-beginning-of>. Prompted by China’s oppressive Cybersecurity Law in 2016, Andrea Limbago discusses her concerns over the 6-year decline in Freedom House internet freedom ratings. She warns that Russia and China are taking their cyber censorship tactics abroad and cautions, “Absent a major push by the U.S. government and corporations, internet freedom is at risk of being superseded by censorship and control.” The human rights and privacy abuses in the 2016 Chinese Cybersecurity Law are detailed in a Human Rights Watch report here: <https://www.hrw.org/news/2016/11/06/china-abusive-cybersecurity-law-set-be-passed>.

¹³⁰ A U.S. 2021 cybersecurity budget projection is linked here: <https://www.hstoday.us/subject-matter-areas/cybersecurity/u-s-government-to-spend-over-18-billion-on-cybersecurity/>.

¹³¹ Craig and Valeriano, “Realism and Cyber Conflict: Security in the Digital Age,” 5; Ryan Maness and Brandon Valeriano, “The dynamics of cyber conflict between rival antagonists, 2001-11,” *Journal of Peace Research* 51, no. 3 (2014): 347, <https://doi.org/10.1177/0022343313518940>. If the offense is advantaged in cyberspace, then it is surprising that, “between 2001 and 2011, only 20 out of 126 rival pairs of states engaged in cyber conflict which has mostly occurred at low levels of severity.” It is likely the high cost and sophistication of offensive tools explains their rare use.

¹³² Scott Malcomson, “The New Cyber Normal,” *Carnegie Corporation*, June 7, 2018, <https://medium.com/carnegie-reporter/the-new-cyber-normal-8cd50fb17ea0>.

strength in the cyber domain, which seems most easily demonstrated through a show of force, that is to say, offensive action. Yet, cyber “show of force” is unlike physical domain show of force. First, the offensive tool is usually tailored to a select target. Second, the tool cannot be displayed until used, limiting the ability to intimidate through strength without wasting a valuable exploit.¹³³ Additionally, to avoid hypocrisy, the U.S. can only operate on adversary networks and attack their infrastructure in a low norms environment. In a high norms environment (Captain America Scenario), the same actions violate the very norms the U.S. promotes for others.

Finally, the cyber forecasts highlight the oft-overlooked ethical component to strategy selection. A U.S. commitment to global leadership in upholding cyber norms (right side of the chart) aligns with virtue ethics. According to Aristotle’s teaching, this ethical perspective emphasizes seeking the mean “in all things relative to us” as is determined “through reason as the prudent man would define [the mean].”¹³⁴ Human rights and privacy are protected by current UNGGE norms and balanced with security, which is upheld by protecting infrastructure and supply chains and guarding against malicious use of a state’s ICT. If norms are followed, individual free speech and communication online is moderated appropriately without jeopardizing state cybersecurity; specifically, norms require cyberspace is not manipulated for malign purposes, like disinformation. Movement away from norms (left side of the chart) gives authoritarian regimes an excuse to smother user liberties online and violate user privacy. Democratic regimes have to grapple with how to support free speech in the face of subversive

¹³³ Martin Libicki, “Why Cyberdeterrence is Different,” In *Cyberdeterrence and Cyberwar* (2009): 52-56.

¹³⁴ Lawrence M. Hinman, *Ethics: A Pluralistic Approach to Moral Theory* (Boston: Wadsworth, Cengage Learning, 2018), 257-259.

online attacks when global cyber norms are ignored.¹³⁵ And so, a norms-aligned U.S. Cyber Strategy provides a better environment to achieve Aristotelian balance online and virtuous use of the internet, satisfying one of the ethical frameworks.

In terms of consequence versus moral ethics, the Y-Axis represents tradeoff between Utilitarian and Kantian ethics. Utilitarian ethics, which “demands that we consider the consequences of everyone affected by the matter under consideration,” is optimized in a high norms environment.¹³⁶ Strategic support for norms, especially paired with a defense-oriented strategy, offers the greatest benefit for the greatest number of stakeholders, including American allies and businesses. The upper right-hand quadrant (Avengers Scenario) especially benefits U.S. companies providing secure software and cybersecurity services, who profit when the U.S. and its allies focus on developing a strong and resilient cyber defense. Secure software and software-driven products is a multi-trillion-dollar business, of which the U.S. and our allies have the vast majority of products used globally. Cybersecurity software, while a more fractured industry, still represents a multi-billion-dollar business. More broadly, the beneficiaries include those for whom norms reduce threat risk and who are protected by a robust defense. Netizens of the global internet order benefit from norms which promote a free, open, and connected cyberspace. Strategic norms-alignment, then, upholds two ethical perspectives: virtue and utilitarian.

On the other hand, Kantian ethics focuses on intentions and puts a premium on duty as a moral motive. The U.S. government has the duty to preserve an open and secure online

¹³⁵ For a very recent discussion of the challenges of balancing liberty and security in the U.S. online environment, see this Washington Post piece discussing Big Tech’s counterproductive attempt to stifle free speech following the 6 January 2021 raid on the U.S. Capitol: https://www.washingtonpost.com/opinions/why-big-techs-attempt-to-stifle-free-speech-could-be-futile--or-worse/2021/01/11/e912acac-5432-11eb-a931-5b162d0d033d_story.html.

¹³⁶ Hinman, *Ethics: A Pluralistic Approach to Moral Theory*, 124.

environment for its citizens. It could be argued that agreeing to constrain U.S. offensive capabilities by adhering to global norms – including its ability to target adversary infrastructure and intrude on foreign networks for intelligence collection and OPE – violates the U.S. government’s duty to act on behalf of its citizens’ security. The current U.S. Strategy asserts that the USCYBERCOM must operate forward to preempt strikes on American networks. This is consistent with Kantian ethics insofar as it is an act of good will carried out for the sake of duty to protect and secure America’s netizens and online infrastructure, regardless of the consequences it has on other states’ sovereignty. If the noble intent to protect justifies any means in U.S. strategy, then one could argue a norms-agnostic approach is more consistent with a moral ethics perspective, especially Kantian ethics.

However, there is a flaw in the application of deontology to justify an abandonment of cyber norms. In a low-norms environment (left-hand side of the chart), the U.S. is faced with either cyber chaos (Gotham City) or a game of cyber intruder whack-a-mole (Roadrunner). In either case, the U.S. cannot condemn without hypocrisy the very intrusions of its own networks which it is defending against because Washington, itself, has thwarted norms in its forward posture. Kant insists that the maxims on which one acts should be capable of being willed by rational agents as a universal law.¹³⁷ Yet, there is little universality in allowing the U.S. to target other nations’ infrastructure because the U.S. does not want its adversaries to do the same. Thus, the Kantian argument against norms is weak, as it fulfills only Kant’s requirement to act for the sake of duty but not his philosophy that “moral acts can be willed as universal law.”¹³⁸

¹³⁷ Kant’s philosophy represents a deontological moral theory and is summarized in the Stanford Encyclopedia of Philosophy here: <https://plato.stanford.edu/entries/ethics-deontological/#DeoTheKan>.

¹³⁸ Hinman, *Ethics: A Pluralistic Approach to Moral Theory*, 2018, 124.

The Road Ahead: Necessary Revisions and Implementation Challenges

Considering all tradeoffs and ethical perspectives reveals that “defense is the best defense” against cyberattacks, and even though Russia and China will continue to violate norms and resist further norms refinement, the U.S. pursue a norms-aligned strategy. The forecasting analysis also demonstrates that the creative combination of exquisite defense and determined diplomacy offers a strategic alternative that plays to U.S. strengths – including its strong allies – and is an ethical approach consistent with American values. Importantly, this approach does not fall victim to the myth that action is always more prudent than inaction. In this strategic environment, an appreciation for nuance and complexity hedges against the tendency to employ USCYBERCOM’s offensive assets or offensive countermeasures which risks devolving into hybrid warfare or even conventional war. Yet, an “Avengers” approach does not ignore efficacy. In fact, while an offensive posture is proposed as a deterrent, little empirical evidence suggests it dissuades adversaries from assuming and executing similarly aggressive strategies.¹³⁹ Using the U.S. Defend Forward Strategy as an example, USCYBERCOM’s offensively oriented approach did thwart adversary attacks. Iranian state election intimidation, the Chinese hacks to conduct espionage against the U.S. industrial base, and the Russian Solar Winds hack all occurred since October 2020, well after 2018, when the U.S. adopted a more aggressive strategy and delegated some “strike back” capabilities in NSPM-13.¹⁴⁰ Thus, focusing on defense is not simply a wise

¹³⁹ Jensen and Valeriano, “The Myth of Cyber Offense: The Case for Restraint,” 4. In their study of 272 cyber operations between rival states, the authors find that, “Offense, whether disruption, espionage, or degradation, does not produce lasting results sufficient to change the behavior of a target state. Only 11 operations (4 percent) appear to have produced even a temporary political concession, with the majority associated with sustained, multiyear counterespionage operations by U.S. operatives usually targeting China or Russia. Furthermore, each of these operations involved not just cyber actions, but other instruments of national power, such as diplomatic negotiations, economic sanctions, and military threats.”

¹⁴⁰ The Center for Strategic International Studies chronicles cyberattacks since 2006 here: <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.

moral choice, it is a decision for effectiveness rather than the myth of the efficacy of the cyber offense.

Finally, the “Avengers” team-oriented, norms-aligned, defense-centric strategy avoids the incomplete fit of traditional deterrence framework in cyberspace, and its limits are best understood through Nye’s concept of multi-faceted deterrence. Entanglement relies on interdependencies among states to impose costs on cyber aggressors, causing states to converge on norms out of shared interests. In this case, entanglement shows the limits of norms to affect state behavior. Competing with China and Russia in a very interconnected global economy offers some interest overlap, but those areas are rare and require creativity for the U.S. to leverage, suggesting Beijing and Moscow are unlikely to accept (in practice) most norms which favor a U.S.-led Liberal World Order.¹⁴¹ This reality makes a strong, resilient defense critical, as it protects against the likelihood and severity of their gray zone cyberattacks.

This paper suggests an “Avengers” team-centric, defense-oriented strategy as the best way to compete against Great Power Competitors who exploit the gray zone in the unique cyber domain. This approach requires a shift from the current “Defend Forward” DoD Strategy to a “Defense Forward.” While this might seem like semantics, the distinction signifies different norms-alignment and resource allocation. In an “Avengers” scenario, what the U.S. can project forward is not a cyber force operating uninvited on foreign networks, but rather, its leadership

¹⁴¹ Nye, “Deterrence and Dissuasion in Cyberspace,” 58-60. Joseph Nye explains, “Entanglement refers to the existence of various interdependences that make a successful attack simultaneously impose serious costs on the attacker as well as the victim Goldman, “From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy,” 2020 (88). Entanglement will require significant creativity when it comes to norms alignment with Russia and China. While Russia seems to be content to continue its practice of “double speak,” as Emily Goldman points out, “China, in particular, wants to be accepted as a member of international society but as a norm-maker, not a norm taker. It does not wish to yield to the self-interested standards of liberal states. China is currently acting on the belief that it can shape norms to serve its specific interests. America’s approach to building”

for countries who will commit to norms, not simply espouse them. It requires the courage and consistency to call out and alienate states who would subvert an open internet order (China, Russia, Iran). Since means should match ends in strategy, adopting the “Avengers” approach would require a reallocation of government funds for cybersecurity, particularly, awarding a larger portion for the Department of Homeland Security’s defensive operational element, the National Cybersecurity and Communications Integration Center.¹⁴² One positive use of U.S. strength forward is coaching and training partners in developing countries to curb Chinese and Russian influence and authoritarian internet models with a positive alternative. This effort serves multiple stakeholders, promoting U.S. cybersecurity companies globally to counter the negative and widespread presence of Huawei-supported networks. Fortunately, a complete strategy overhaul is not required. The Cyber Solarium Commission’s recommended layered defense is not exactly aligned with the “Avengers” concept and its support for persistent engagement and norms is contradictory. However, its “deny benefits” approach (Defensive Layer 2), which includes securing civilian infrastructure, offers a starting point for discussions on how to translate a defense-oriented, norms-aligned strategy into organizational orientation and action.¹⁴³

¹⁴² Jason Healy, “The Cyber Budget Shows what the U.S. Values – It isn’t Defense,” *Lawfare Blog: Cyber & Technology*, June 1, 2020, <https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense>. Cyber expert Jason Healy argues that, “The White House and National Cyber Strategy emphasize the need to protect the American people and our way of life, yet the budget does not reflect those values. Rather, the budget clearly shows that the Defense Department [whose offense/defense budget split is classified] is the government’s main priority. If the focus were defensive, rather than offensive, then law enforcement and Homeland Security funding—especially for federal cybersecurity—would be at least comparable.” As evidence, he cites, “The NCCIC, which is supposed to be the ‘nation’s flagship cyber defense, incident response, and operational integration center,’ gets just one dollar for every 10 that goes to military offensive and defensive operations.”

¹⁴³ Cyber Solarium Commission recommendations for a strategy of layered cyber deterrence, described on pages 1-2 of the Executive Summary, are available here: https://icitech.org/2020-us-cyberspace-solarium-commission-report/?gclid=Cj0KCQiAifz-BRDjARIsAEElyGLa_Xcu1-sNI_m5DmSngc2rLYr7E328hPP6FcPpUo-2rllDbP2OLzsaAm0DEALw_wcB.

Several challenges to operationalizing this strategy should prompt further research so the U.S. can compete efficiently without abandoning its values. Each issue is described below with associated research recommendations.

1) Nuanced Norms

Norms promotion is consistent with the 2018 U.S. Cyber Strategy, so why has it failed to create effects? The first issue is the nature of the UNGGE's norms – global, but not specific or binding. In the *TNSR* series, cyber experts Jason Healy and Robert Jervis explain the difficulty in achieving norms which satisfy all three criteria.¹⁴⁴ If true, the U.S. should advocate binding and specific norms, which eliminate the gray space exploited in the cyber domain by authoritarian adversaries. By unambiguously calling out malign behavior via specific norms, Washington wisely abandons the notion that norms will be globally accepted (even if they are espoused) by authoritarian regimes who envision a completely antithetical, control-oriented cyber order. The 2018 National Cyber Strategy assumes, “increased public affirmation by the United States and other governments will lead to accepted expectations of state behavior and thus contribute to greater predictability and stability in cyberspace.”¹⁴⁵ The question is: accepted by whom? This effect – greater predictability and stability – is achieved only for like-minded states; China and Russia have demonstrated their willingness to thwart nonbinding UNGGE norms when it suits their interest in subverting democracy. Josh Rovner reinforces the futility of global norms in the current environment of competition, but this leaves room for specific norms which are binding

¹⁴⁴ Healy and Jervis, “The Escalation Inversion and Other Oddities of Situational Cyber Stability,” 22.

¹⁴⁵ Goldman, “From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy,” 89; The White House, *National Cyber Strategy of the United States of America*, (Washington, DC: The White House) 2018, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

for a select group of democracies who share the U.S. interest in an open and free internet.

Establishing this team is discussed below, but there is still another challenge to promoting norms.

The second reason current cyber norms are ineffective is America's own failure to live up to them. For espoused norms to have meaning, the U.S. must commit to them in deed, not just with hollow words. USCYBERCOM's Persistent Engagement approach describes operating forward on adversary networks as the only way to get ahead of an enemy strike and explicitly rejects deterrence.¹⁴⁶ But, that forward presence undermines U.S. credibility in publicly affirming norms as the America's cyber strategy directs. Few options follow to reverse Washington's current hypocrisy regarding norms: change the norms or change U.S. behavior. For the former, it is more realistic to assume that *all states* will practice cyber espionage in "foreign territory" just as they do in the physical (land) domain. Framing the cyber domain as primarily a space for intelligence operations could help reshape specific norms about cyber sovereignty that no Great Powers currently follow. Alternatively, if the U.S. focused resources on a broad (including corporate networks) and resilient defense, perhaps a forward presence on adversary networks becomes unnecessary. Cyber experts Brandon Valeriano and Benjamin Jensen suggest application of a Corbettian concept: "stepping back from preemption and focusing on sharing intelligence and

¹⁴⁶ Josh Rovner, "Did the Cyber Solarium Commission live up to its Name," *War on the Rocks Special Series: The Brush Pass*, March 19, 2020, <https://warontherocks.com/2020/03/did-the-cyberspace-solarium-commission-live-up-to-its-name/>; Nakasone, "A Persistent Force for Cyber Operations," 12-13. General Nakasone justifies persistent engagement this way: "To defend critical military and national interests, our forces must operate against our enemies on their virtual territory as well. We cannot afford to let adversaries breach our networks, systems, and data (intellectual property and personally identifiable information). If we are only defending in 'blue space,' we have failed. We must instead maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries." Despite the legal justification provided by the DoD General Counsel, unless these are NSA cyber operatives acting under Title 50 authorities, or, unless cyber sovereignty is a futile concept, this is the equivalent of sending Title 10 land forces onto foreign soil uninvited. The U.S. tacitly approves the adversary's decision to mirror this behavior by setting this dangerous standard defending forward on enemy national networks. General Counsel remarks are linked here: <https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>.

hardening targets (that is, updating systems to repair existing vulnerabilities).” They caution, “defending forward risks undermining the ability to isolate adversary capabilities and, if need be, degrade them through targeted counter attacks designed to limit escalation risks.”¹⁴⁷ Certainly, the U.S. could direct resources spent on Cyber Mission Teams’ operations defending forward toward its “Hunt Forward” Teams, collective attribution capacity, and private sector cybersecurity partners advising allies how to best shore up defenses against network intrusions and responding to them when they occur.¹⁴⁸

Further research is necessary to resolve this particularly sticky point in cyber norms – what to do about cyber espionage¹⁴⁹ – and what that entails for USCYBERCOM resource allocation. Two things are certain: resources are finite and credibility requires disciplined adherence to principles. Thus, the Cyber Solarium Commission’s “do everything” recommended approach requires a relook, especially because the past year of investing domestic resources for battling COVID-19 has led for calls to slash defense spending (which includes USCYBERCOM funding). This would lead to a scenario in which USCYBERCOM is called to do more with

¹⁴⁷ Jensen and Valeriano, “The Myth of the Offense,” 2, 8.

¹⁴⁸ Mark Pomerleau, “How ‘hunt forward’ teams can help defend networks,” *Fifth Domain*, February 12, 2020, <https://www.fifthdomain.com/dod/2020/02/12/how-hunt-forward-teams-can-help-defend-networks/>.

¹⁴⁹ A relevant legal consideration regarding appropriate cyber norms about cyber espionage is the classification of cyber clandestine activity as traditional military activity (TMA). The CRS Cyber Operations Primer published in December 2020 explains, “Section 1632 of the FY 2019 NDAA affirms that DOD may conduct operations in cyberspace, including clandestine operations, short of hostilities or in areas in which hostilities are not occurring; it also states that a clandestine military activity or operation in cyberspace shall be considered a traditional military activity (TMA).” Since TMAs are granted Congressional reporting exceptions in Title 50, there are few mechanisms in place to check Executive Power to act outside UNGE norms in cyberspace. The CRS Primer is linked here: <https://crsreports.congress.gov/product/pdf/IF/IF10537>. Importantly, the USCYBERCOM dual-hats command of the military cyberspace operations (DoD Command) and the NSA’s intelligence-related operations, which creates challenges discussed in *War on the Rocks* here: <https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/>. Further discussion of U.S. domestic legal framework governing cyberspace is covered by Robert Chesney for the *Hoover Institute* here: <https://www.hoover.org/research/domestic-legal-framework-us-military-cyber-operations>.

less.¹⁵⁰ Foremost, its strategy recommendations need revisiting because we cannot persist in forward engagement *and* promote current cyber norms without being inconsistent.

2) Imperfect Partner Definitions: Like-Minded Democracies

If norms are specific and binding for like-minded democracies, who will we consider a part of the “Avengers” team? That is, who are the like-minded democracies we expect to join us in countering the rise in internet control? Defining that group will be challenging because the U.S. does not even agree with its European partners on all aspects of cyber governance.¹⁵¹ Certainly, partners like the United Kingdom have demonstrated troubling disregard for user privacy in their national cyber policy that does not align with the UNGGE’s 2015 norms.¹⁵² Also, the concept of “Western democracies” is dated. Eastern democracies like Japan, India, Taiwan, and South Korea (whose elections China recently disrupted) will be critical to include to avoid regressing to pitting “the East vs. the West” in cyberspace.¹⁵³ Additionally, once specific norms are established and the team is built, what kind of institution is appropriate to ensure binding norms

¹⁵⁰ Rovner, “Did the Cyber Solarium Commission live up to its Name;” A *Defense News* article describing bipartisan calls to slash defense spending for FY22 and their potential effects is linked here: <https://www.defensenews.com/smr/transition/2021/01/19/bidens-post-covid-defense-budget-choice-a-resurgence-or-a-decline/>. The FY21 defense budget request breakdown, includes allocations for cyber activities, is linked here: https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Budget_Request_Overview_Book.pdf.

¹⁵¹ EU-US coordination on internet governance is described by Emily Taylor and Stacie Hoffman for *Chatham House* here: <https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-14-EU-US-Relations-Internet-Governance2.pdf>.

¹⁵² UK Amnesty International, “Mass Surveillance: Why we’re taking the UK to court over massing spying,” Amnesty International UK, May 18, 2020, <https://www.amnesty.org.uk/why-taking-government-court-mass-spying-gchq-nsa-tempora-prism-edward-snowden>. Additionally, Goldman highlights Britain’s disregard for cyber sovereignty: “the United Kingdom...has publicly declared that remote cyber operations below the non-intervention threshold are not prohibited by international law and do not require consent.” Her article is linked here: <https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/>.

¹⁵³ Maiko Ichihara, “The Changing Role of Democracy in Asian Geopolitics,” *Carnegie Endowment for International Peace*, September 14, 2017, <https://carnegieendowment.org/2017/09/14/changing-role-of-democracy-in-asian-geopolitics-pub-73110>.

among that group of states? Currently, various cybersecurity partnerships which exclude authoritarian regimes exist, including: the NATO Computer Incident Response Capability and Rapid Reaction Teams as part of its Cyber Defense Policy,¹⁵⁴ the Blue Dot Network with Japan and Australia, the Clean Network program, and the State Department's Indo-Pacific Digital Connectivity and Cybersecurity Partnership.¹⁵⁵ Are these disparate efforts, led by various government departments, sufficient? Chris Demchak proposes a sweeping 'Cyber Operational Resilience Alliance' (CORA), "a collective whole-of-nations integrated response across integrated allied democratic civil societies" to counter authoritarian influence in the digital ecosystem.¹⁵⁶ Determining the right team and organizational model to govern an open, connected cyber domain requires further research, but finding answers to the above questions is important if norms are to play a role in shaping the future actions in the cyber domain.

3) Imperfect Partner Definitions: Whole of Nation Effort and Private Sector Stakeholders

Often when the term "partner" is used in national security, it refers to a member of an international coalition.¹⁵⁷ However, cyberspace is a multi-use domain, serving stakeholders

¹⁵⁴ The NATO Cyber Defense Policy is described here:

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

¹⁵⁵ Goldman, "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy," 98. One of the promising initiatives, the Clean Network Program is, "a comprehensive effort by a coalition of like-minded countries and companies to secure their critical telecommunications, cloud, data analytics, mobile apps, Internet of Things, and 5G technologies from malign actors... More than 30 countries and territories are now Clean Countries, and many of the world's biggest telecommunications companies are Clean Telcos."

¹⁵⁶ Demchak, "Three Futures for a Post-Western Cybered World," 3, 12-20. In the article, Chris Demchak asserts, "today no single democracy has the scale and sufficient resources to alone match the foreknowledge and strategic coherence of the newly confident and assertive China... To change current global trends, the small group of consolidated democratic civil societies needs a collective approach to counter China's growing dominance across all fields of cyberspace."

¹⁵⁷ Rovner, "Did the Cyberspace Solarium Commission Live up to its Name," 8. Rovner refers to the cyber domain as: "the public internet... a constellation of overlapping networks maintained by a mish-mash of states, firms, individuals and private sector groups."

across a broad spectrum of social, technological, economic, and political systems. Therefore, partners in cybersecurity should also include: 1) the State Department, critical for promoting norms and building alliances, and 2) the private sector, which provides tools for and benefits from cyber defense.¹⁵⁸ As the Solar Winds breach proves, especially in cybersecurity supply chains, the line between government and corporate systems quickly blurs. Civilian infrastructure, particularly Supervisory Control and Data Acquisition Systems (SCADA) and Industrial Control Systems (ICS), remain vulnerable to malign manipulation.¹⁵⁹ What is the best means to integrate efforts for a strong cyber defense? The Cyber Solarium Commission (CSC) proposed a National Cyber Director (President's principal advisor to coordinate cyber actions), a position adopted in the FY21 National Defense Authorization Act (NDAA).¹⁶⁰ Yet, as Josh Rovner points out, this organizational change, alone, is likely to fall short of the mark considering the incredible scope of all online activity.¹⁶¹ While "military-civilian" partnerships are encouraged in the 2018

¹⁵⁸ Goldman, "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy," 97; David Vergun, "Great Power Competition can Involve Conflict Below Threshold of War," 2 October 2020, <https://www.defense.gov/Explore/News/Article/Article/2364137/great-power-competition-can-involve-conflict-below-threshold-of-war/>. At the 2020 Special Operations/Low Intensity Conflict Conference, Acting Assistance Secretary of Defense for SO/LIC, Ezra Cohen, stressed a whole of nation approach in the cyber domain: "[to counter] adversaries [who] embrace the anonymity of social media platforms and the viral nature of information flow as they employ information statecraft as an integral element of their approach to competition... requires a whole-of-government approach that integrates technical capabilities and institutional knowledge across civilian agencies, foreign partners and other entities."

¹⁵⁹ Scott Weed, "US Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure," *Air Force Research Institute*, (Maxwell AFB: Air University Press, 2017), 4-7, https://media.defense.gov/2017/Nov/20/2001846609/-1/-1/0/CPP0007_WEED_SCADA.PDF.

¹⁶⁰ CSC Chair, Senator Angus King, details all CSC recommendations adopted in the FY21 NDAA here: <https://www.king.senate.gov/newsroom/press-releases/ndaa-enacts-25-recommendations-from-the-bipartisan-cyberspace-solarium-commission>. The Senate-confirmed National Security Director is provision 1752 in the NDAA.

¹⁶¹ Rovner, "Did the Cyberspace Solarium Commission Live up to its Name," 8. The author notes, "The commission correctly notes that government and society are deeply immersed in cyberspace. Oversight and policy will remain complicated and difficult as long as that remains the case. Efforts to streamline cyberspace policy are likely to disappoint for the same reason."

National Defense Strategy, few venues exist for sharing best practices in cyber defense.¹⁶² When a civilian firm is hacked by foreign actors, what does the government support to the corporation look like? Cybersecurity scholars Robert Knake and David Sanger describe it as still largely a “Home Depot model – you can do it, we can help.” That is, the DHS can provide technical advice but another private sector company will come in for clean-up and restoration efforts.¹⁶³ A more mutually symbiotic relationship, where companies provide information for the government to monitor defense readiness in cyberspace while receiving better access to incident prevention and response tools, will require a deliberate government effort to operationalize. Integration of cyber National Guard Forces is just one example of how this can be achieved. National online safety standards, as is paralleled in the U.S. automobile industry (NHTSA’s FMVSS), or even an international safety-oriented body, similar to the ICAO for aviation, represent another way the government can ensure private companies are equipped with adequate network security tools.¹⁶⁴ More creative avenues for collaboration exist and will be illuminated through further research.

Regarding individual actors in cyberspace, what does cybersecurity education for the public look like? After all, individuals also interact in the cyber domain and play a key role in cybersecurity. The good news is that CSC does offer several recommendations for public-private partnership in cybersecurity, and Congress adopted six as provisions in the FY21 NDAA.¹⁶⁵

¹⁶² Mattis, “Summary of the National Defense Strategy of the United States of America,” 8, 11.

¹⁶³ Laura Galante, Robert K. Knake, and David E. Sanger, “Cyber Conflict: The Evolution of Warfare,” <https://www.cfr.org/event/cyber-conflict-evolution-warfare>.

¹⁶⁴ The National Highway Traffic Safety Administration’s Federal Motor Vehicle Safety Standards are codified in U.S. Code and are described here: <https://www.nhtsa.gov/laws-regulations/fmvss>. The International Civil Aviation Organization (ICAO) is a 93-member UN group formed after WWII to serve as a foundation for the standards and procedures for peaceful global air navigation. Further information can be found at the organizational site here: <https://www.icao.int/about-icao/Pages/default.aspx>.

¹⁶⁵ FY21 NDAA Provisions available here: <https://www.king.senate.gov/newsroom/press-releases/ndaa-enacts-25-recommendations-from-the-bipartisan-cyberspace-solarium-commission>. They include: 1719 (Cybersecurity Education and Training Assistance K-12 Program), 1728 (Assessing Private-Public Collaboration in Cybersecurity),

These represent a promising start to better integration. Further research, directed by Provisions 1728 and 1739, is necessary to optimize support of private sector partners in cyber defense and educate public netizens to maintain cybersecurity as they navigate the web.

4) Cybersecurity Sector Incentives: Profit over Patriotism

A final hurdle in reaching an “Avengers” future is the cybersecurity sector itself. The military and corporate sector benefit from the hardware, software, and services provided by cybersecurity firms. Mordor Intelligence reports, “The cybersecurity market was valued at USD 156.24 billion in 2020, and it is expected to reach USD 352.25 billion by 2026,” driven by increased online connectedness and a growing rate of attacks.¹⁶⁶ It is worth considering: does a defense-focused strategy truly reduce the cost for competing in cyberspace if cybersecurity companies are incentivized to create short-term, proprietary solutions which ensure their consistent market growth, but would not necessarily be interoperable in a collective cybersecurity alliance (described above)? If an open and connected internet future is the objective, a segmented defense is not desirable. Still, the financial incentives to do so exist under current conditions in the cyber domain, especially since cybersecurity firms are not held accountable for breaches, as was illustrated during Solar Winds.¹⁶⁷ Indeed, the cybersecurity industry is highly fractured and despite a hefty price tag, does not always deliver on its security

1739 (Defense Industrial Base Cybersecurity Threat Hunting and Sensing, Discovery, and Mitigation), 1744 (Creation of a Biennial WoG/State/Private Sector Cyber Exercise), 9002 (Codify Sector Critical Infrastructure Risk Management Agencies), 9603 (Continuity of the Economy Plan).

¹⁶⁶ Mordor Intelligence provides a cybersecurity market overview covering the study period 2018-2026 here: <https://www.mordorintelligence.com/industry-reports/cyber-security-market>.

¹⁶⁷ Reporting on the Solar Winds hack is available here: <https://www.forbes.com/sites/jodywestby/2020/12/16/solarwinds-cyber-attacks-raise-questions-about-the-companys-security-practices-and-liability/?sh=4c80f174711d>. As Forbes contributor Jody Westby explains, “The recently discovered cyber attacks against numerous U.S. government departments and thousands of public and private sector entities around the world, via a compromise of SolarWinds software, underscore the risks associated with third party vendors and raise questions about liability.”

promise to clients.¹⁶⁸ Moreover, if recent Senate hearings are any indication, American-based Multinational Corporations (MNCs) feel less loyalty to their country than to profit and shareholders.¹⁶⁹ There are no idle resources, so these cyberattacks and hacks represent significant cost for cybersecurity consumers.¹⁷⁰ What can be done to incentivize efficiency in this sector? Are significant changes in the cybersecurity industry or its governance required to improve long-term cyber defense? Would a greater emphasis on secure software create a more enduring impact on cyber defense by reducing requirements for expensive cybersecurity software/services? This is the least explored challenge to implementing a defense-oriented, norms-aligned strategy for cyber competition in the gray zone. Therefore, it merits the most research to determine what changes in the cybersecurity industry would improve efficiency and effectiveness in a long-term cyber defense. The nature of Great Power Competition is, after all, protracted gray zone conflict, making economy of resources over time particularly crucial for strategic success.

If these challenges can be overcome, a future that looks more like the “Avengers” than “Gotham, Roadrunner, or a solo Captain America” offers the U.S. the best chance to compete and win in a way consistent with its values. The U.S. can succeed if it fights the hype about escalation in cyberspace and resists the military predisposition for action that pervades the modern cyber competition dialogue. As Victoria University Wellington Public Policy Professor Joe Burton warns:

¹⁶⁸ Tony Bradley, “The Standard Cybersecurity Model is Fundamentally Broken,” *Forbes*, October 7, 2019, <https://www.forbes.com/sites/tonybradley/2019/10/07/the-standard-cybersecurity-model-is-fundamentally-broken/?sh=7ccc8a271189>.

¹⁶⁹ Scott Malcomson, “The New Cyber Normal 2018, 8.

¹⁷⁰ “According to the Center for Strategic and International Studies (CSIS) and McAfee, “cybercrimes, which include damage and destruction of data, stolen money, lost property, intellectual property theft, and other areas, currently cost the world almost USD 600 billion each year, or 0.8% of the global GDP.” This is reported in the Mordor Intelligence cybersecurity market overview here: <https://www.mordorintelligence.com/industry-reports/cyber-security-market>.

Certainly there appears to be a massive industry built up around cyber security, which is looking to profit from people's fears about cyber intrusions....[There are] billions of dollars being awarded by the U.S. government for the safeguarding of digital infrastructure and the intrusive role that agencies like the National Security Agency have taken in cyberspace. Just as with the threat from terrorism in the post-9/11 environment, an excessively military response to cyberattacks, combined with a failure to develop a wide range of civil and criminal mechanisms, may lead to less effective policy.¹⁷¹

An emphasis on teamwork, norms, and resilient defense among like-minded allies and corporate partners prevents an overly militarized, aggressive cyber strategy. An “Avengers” approach plays to the strength of U.S. values and avoids playing into the hands of authoritarian regimes seeking to manipulate us into denying our own values to counter their malign behavior. Washington cannot be bullied into an unethical way to win because America will lose the trust of its allies along the way. The U.S. can win in the cyber competition without abandoning the values which make it the respected leader of the Liberal World Order.

¹⁷¹ Joe Burton, “Review: *Cyber War versus Cyber Realities*,” *H-Net: Humanities and Health Sciences Online*, (April 2016), <https://networks.h-net.org/node/28443/reviews/118703/burton-valeriano-and-maness-cyber-war-versus-cyber-realities-cyber>.

Appendix A: Global Internet Map

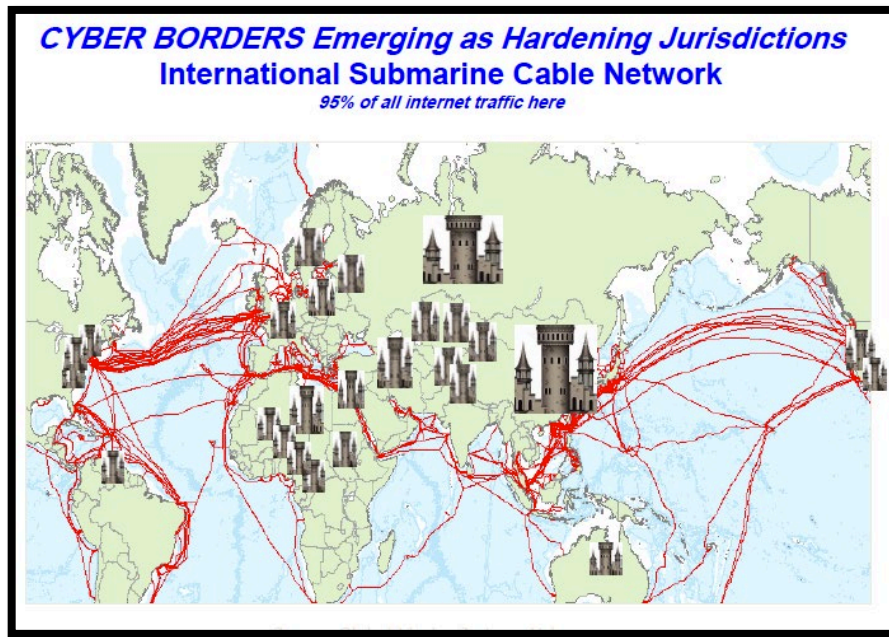
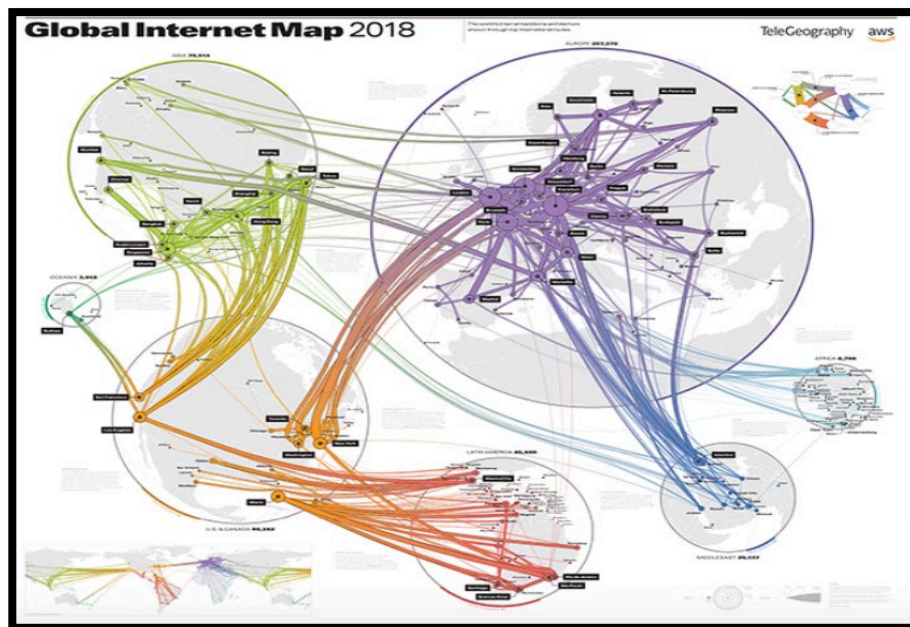


Figure 1. Chris Demchak, RDML Grace M. Hopper Professor of Cyber Security at the U.S. Naval War College, uses this graphic to explain the importance of cyber borders in determining a new cyber world order and, thus, a key part of cyber conflict. The global internet map, shown below, is also useful in visualizing the interconnected, global nature of the cyber substrate, closely linked to the idea of cyber borders. Importantly, the image shows the internet is heavily weighted in the Western work (American and Euro-centric). Link to the interactive map, here: <https://global-internet-map-2018.telegeography.com/>.



Appendix B: Nested U.S. Cyber Strategies

<u>National Strategy</u>		<u>DoD Strategy</u>	
NSS	Cyber Pillars	LOEs	Op Concepts
Protect the American people, homeland, and way of life	Protect the American people, homeland, and way of life by <i>safeguarding networks systems, functions and data</i>	Build a more lethal cyber force	<i>Collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict</i>
Promote American prosperity	Promote prosperity by nurturing a <i>secure, thriving digital economy and fostering strong domestic innovation</i>	Compete and deter in cyberspace	<i>Defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict*</i>
Preserve peace through strength	Preserve peace and security by strengthening the ability of the United States, its partners, and allies to <i>deter and punish those who use cyber maliciously</i>	Strengthen alliances and attract new partnerships	
Advance American influence	Advance influence to extend the key tenets of an <i>open, interoperable, reliable, and secure internet</i>	Reform the department and cultivate talent	

Figure 2. This chart shows the various U.S. Cyber Strategies, nested from the national level to the defense department. Importantly, alliances and forward defense play a key role in the current approach. Synchronization across these strategies is crucial. Consistency is key to successful messaging regarding who we are, what we stand for, and how we intend to compete. This information is derived from the CRS's Cyberspace Operations Defense Primer. It is current as of 15 December 2020 and is available at: <https://fas.org/sgp/crs/natsec/IF10537.pdf>.

Bibliography

- Alba, Davey, and Sheera Renkel. "Why Facebook's Blocking of New Political Ads May Fall Short." *New York Times*. September 4, 2020.
<https://www.nytimes.com/2020/09/04/technology/facebook-political-ads-block-election.html>.
- Amnesty International U.K. "Mass Surveillance: Why We're Taking the U.K. to Court Over Massing Spying." Last modified May 18, 2020. <https://www.amnesty.org.uk/why-taking-government-court-mass-spying-gchq-nsa-tempora-prism-edward-snowden>.
- Bandow, Doug. "Xi Xiping Wants to Become the New Mao." *Cato Institute*. May 26, 2020.
<https://www.cato.org/publications/commentary/xi-jinping-wants-become-new-mao>.
- Barno, David and Nora Bensahel. "Fighting and Winning in the 'Gray Zone.'" *War on the Rocks Special Series: Strategic Outpost*. May 19, 2015.
<https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/>.
- Barrett, Brian. "Security News This Week: Russia's SolarWinds Hack Is a Historic Mess." *Wired Magazine*. December 19, 2020. <https://www.wired.com/story/russia-solarwinds-hack-roundup/>.
- Beattie, Tracy, Emilia Currey, and Fergus Hanson. "The Chinese Communist Party's Coercive Diplomacy." *Australian Strategic Policy Institute, International Cyber Policy Centre*. Policy Brief no. 36. 2020. <https://www.aspi.org.au/report/chinese-communist-partys-coercive-diplomacy>.
- Bradley, Tony. "The Standard Cybersecurity Model is Fundamentally Broken." *Forbes*, October 7, 2019. <https://www.forbes.com/sites/tonybradley/2019/10/07/the-standard-cybersecurity-model-is-fundamentally-broken/?sh=7ccc8a271189>.
- Buchanan, Ben and Fiona S. Cunningham,. "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis." *Texas National Security Review Special Issue: Cyber Competition* 3, no. 4 (October 2020): 7.
<http://dx.doi.org/10.26153/tsw/10951>.
- Burton, Joe. "Review: *Cyber War versus Cyber Realities*." *H-Net: Humanities and Health Sciences Online*. Last edited April 2016. <https://networks.h-net.org/node/28443/reviews/118703/burton-valeriano-and-maness-cyber-war-versus-cyber-realities-cyber>.
- Center for Strategic & International Studies. "Significant Cyber Incidents." Accessed on September 2, 2020. <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.
- Chesney, Robert. "The Domestic Legal Framework for Legal Operations." *Hoover Institution*.

- July 29, 2020. <https://www.hoover.org/research/domestic-legal-framework-us-military-cyber-operations>.
- Chesney, Robert and Max Smeets. "The Dynamics of Cyber Conflict and Competition." *Texas National Security Review Special Issue: Cyber Competition* 3, no. 4 (October 2020): 2-3. <https://repositories.lib.utexas.edu/handle/2152/83971>.
- Cimpanu, Catalin. "China has been 'Hijacking the Vital Internet Backbone of Western Countries.'" *ZDNet*. October 26, 2018. <https://www.zdnet.com/article/china-has-been-hijacking-the-vital-internet-backbone-of-western-countries/>.
- Clarke, Arthur C. "Superiority." *The Magazine of Fantasy and Science Fiction* 2, no. 4 (August 1951): 3-11. <http://nob.cs.ucdavis.edu/classes/ecs153-2019-04/readings/superiority.pdf>.
- Clausewitz, Carl von. *On War*. Translated and edited by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976).
- Cook, Sarah. "China's Media Influence has Gone Global. So has the Pushback." *The Diplomat*, June 18, 2020. <https://thediplomat.com/2020/06/chinas-media-influence-has-gone-global-so-has-the-pushback/>.
- Cook, Sarah. "The Globalization of China's Media Controls: Key Trends from 2019." *The Diplomat: The Debate*, January 21, 2020. <https://thediplomat.com/2020/01/the-globalization-of-chinas-media-controls-key-trends-from-2019/>.
- Craig, Anthony and Brandon Valeriano. "Realism and Cyber Conflict: Security in the Digital Age." *E-International Relations Collection*, February 3, 2018. <https://doi.org/10.1177/0022343313518940>.
- Cronk, Terri Moon. "White House releases First Cyber Strategy in 15 Years." *DoD News*, September 21, 2018. <https://www.defense.gov/Explore/News/Article/Article/1641969/white-house-releases-first-national-cyber-strategy-in-15-years/#:~:text=The%20first%20new%20National%20Cyber,strength%3B%20and%20advancing%20American%20influence>.
- Dahir, Abdi. "China Is Exporting Its Digital Surveillance Methods to African Governments." *Nextgov*, November 1, 2018. <https://www.nextgov.com/emerging-tech/2018/11/china-exporting-its-digital-surveillance-methods-african-governments/152495/>.
- Dahir, Abdi. "The African Union is doubling down on deepening its relationship with Huawei." *Quartz Africa*, May 31, 2019. <https://qz.com/africa/1632111/huawei-african-union-sign-deal-to-boost-5g-ai-cloud-computing/>.
- Davidson, Philip S. "USINDOPACOM Commander's Keynote Address for the 33rd Annual National Symposium." Honolulu, Hawaii. January 12, 2021.

- <https://www.pacom.mil/Media/Speeches-Testimony/Article/2469844/33rd-annual-sna-national-symposium/>.
- Defense Forum Washington. "Remarks from GEN Mark A. Milley, USA, Chairman of the Joint Chiefs of Staff." U.S. Naval War Institute. Video: 24:08. December 14, 2020. <https://www.youtube.com/watch?v=CVU9CY4PKvI>.
- Demchak, Chris. "Conflicting Policy Presumptions about Cybersecurity: Cyber–Prophets, –Priests, –Detectives, and –Designers, and Strategies for a Cybered World." *Atlantic Council Issue Brief* (2010): 1-2. https://www.jstor.org/stable/resrep03333?seq=3#metadata_info_tab_contents.
- Demchak, Chris. "Cybered Conflict, Hybrid War, and Informatization Wars." In *Routledge Handbook of International Cybersecurity*. Edited by Eneken Tikk and Mika Kerttunen. New York: Routledge, 2020.
- Demchak, Chris. "Cybered Conflict vs. Cyber War." *Atlantic Council Blog* (blog), October 20, 2010. <https://www.atlanticcouncil.org/blogs/new-atlanticist/cybered-conflict-vs-cyber-war/>.
- Demchak, Chris. "Three Futures for a Post-Western Cybered World." *Military Cyber Affairs* 3, no. 1:6 (2018): 1-19. <https://doi.org/10.5038/2378-0789.3.1.1044>.
- Demchak, Chris and Yuval Shavitt. "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking." *Military Cyber Affairs* 3, no. 1:7 (2018): 1-9. <https://doi.org/10.5038/2378-0789.3.1.1050>.
- Democratic Staff Report for the Committee on Foreign Relations, Ranking Member: Robert Menendez. *The New Big Brother: China and Digital Authoritarianism*. Washington, DC: U.S. Senate, 2020. <https://www.foreign.senate.gov/imo/media/doc/2020%20SFRC%20Minority%20Staff%20Report%20-%20The%20New%20Big%20Brother%20-%20China%20and%20Digital%20Authoritarianism.pdf>.
- Department of Defense. *Cyberspace Operations*. Joint Publication 3-12, Washington DC: Department of Defense, 2018.
- Department of Defense. *DoD Dictionary of Military and Associated Terms*. Office of the Joint Chief of Staff. Washington, DC: Department of Defense, 2020. <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.
- DiCicco, Jonathan M. and Brandon Valeriano. "International Rivalry and National Security." *The Oxford Handbook of U.S. National Security*. Edited by Nikolas K. Gvosdev, Derek S. Reveron, and John A. Cloud, 1-20. New York: Oxford University Press, 2018.

- Ding, Iza and Jeffrey Javed. "Why Maoism Still Resonates in China Today." *Washington Post*, May 29, 2019. <https://www.washingtonpost.com/politics/2019/05/29/why-maoism-still-resonates-china-today/>.
- Economy, Elizabeth, "China's New Revolution: The Reign of Xi Jinping." *Foreign Affairs* 97, no. 3 (2018): 60-74. <https://www.foreignaffairs.com/articles/china/2018-04-17/chinas-new-revolution>.
- Ellick, Adam B., and Adam Westbrook. "Operation Infektion Video Series, Russian Disinformation: From Cold War to Kayne." *New York Times*, November 12, 2018. <https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html>.
- Evanson, Nina. "American Culture." *IES: Cultural Atlas*. Last edited in 2016. <https://culturalatlas.sbs.com.au/american-culture/american-culture-business-culture>.
- Ferling, John. *Whirlwind: The American Revolution and the War That Won It*. New York: Bloomsbury Press, 2015.
- FireEye. "What is a Zero-Day Exploit." Accessed on February 8, 2021. <https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html>.
- Fischerkeller, Michael P. and Richard J. Harknett. "Persistent Engagement and Tacit Bargaining: A Path toward Constructing Norms in Cyberspace." *Lawfare*, November 9, 2018. <https://www.lawfareblog.com/persistent-engagement-and-tacit-bargaining-path-toward-constructing-norms-cyberspace>.
- Forescout Research and Cyber Alerts. "Multibillion Dollar Damage Caused by Notpetya and Wannacry – Learn how Forescout Visibility Platform can Help Address." Last edited September 12, 2018. <https://www.forescout.com/company/blog/multibillion-dollar-damage-caused-by-notpetya-and-wannacry-learn-how-forescout-visibility-platform-can-help-address/#:~:text=A%20recent%20WIRED%20Magazine%20article,on%20Danish%20shipping%20giant%20A.P.&text=NotPetya%20and%20WannaCry%20are%20equal,percent%20device%20visibility%20is%20required>.
- Freedberg, Sydney J. Jr. "Trump Eases Cyber Ops but Safeguards Remain." *Breaking Defense*, September 17, 2018. <https://breakingdefense.com/2018/09/trump-eases-cyber-ops-but-safeguards-remain-joint-staff/>.
- Frenkel, Sheera, and Julian E. Barnes. "Russians Again Targeting Americans with Disinformation." *New York Times*, September 1, 2020. <https://www.nytimes.com/2020/09/01/technology/facebook-russia-disinformation-election.html>.
- Friedman, Uri. "The New Concept in Washington Everyone is Talking About." *The Atlantic*,

- August 6, 2019. <https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/>.
- Funk, Allie, and Adrian Shahbaz. "Freedom on the Net 2019 Report." *Freedom House*, November 2019. https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf.
- Galante, Laura, Robert K. Knake, and David E. Sanger. "Cyber Conflict: The Evolution of Warfare." *Council on Foreign Relations* (June 20, 2018). <https://www.cfr.org/event/cyber-conflict-evolution-warfare>.
- Garamone, Jim. "Dunford Describes U.S. Great Power Competition with Russia, China," *Defense.gov*, March 21, 2019. <https://www.defense.gov/Explore/News/Article/Article/1791811/dunford-describes-us-great-power-competition-with-russia-china/>.
- Gold, Josh. "The First Ever Global Meeting on Cyber Norms Holds Promise, But Broader Challenges Remain." *Council on Foreign Relations*, September 30, 2019. <https://www.cfr.org/blog/first-global-meeting-cyber-norms>.
- Goldman, Emily O. "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy." *Texas National Security Review: The Strategist* 3, no. 4 (Fall 2020): 84-101. <http://dx.doi.org/10.26153/tsw/10950>.
- Greenberg, Andy. *Sandworm: A New Era of Cyber War and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday, 2019.
- Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *Wired Magazine*, August 22, 2018. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
- Harlow, Giles D., and George C. Maerz, eds. *Measures Short of War: The George F. Kennan Lectures at the National War College, 1946-47*. Washington, DC: National Defense University Press, 1990.
- Harvard University. "Enlightenment and Revolution." *The Pluralism Project*. Last accessed December 29, 2020. <https://pluralism.org/enlightenment-and-revolution>.
- Healey, Jay and Robert Jervis. "The Escalation Inversion and Other Oddities of Situational Cyber Stability." *Texas National Security Review Special Issue: Cyber Competition* 3, no. 4 (September 2020): 30-53. <http://dx.doi.org/10.26153/tsw/10962>.
- Hinman, Lawrence M. *Ethics: A Pluralistic Approach to Moral Theory*. Boston: Wadsworth, Cengage Learning, 2018.
- Hoffman, Stacie, and Emily Taylor. "EU-US Relations on Internet Governance." *Chatham*

- House: International Security Department, November 2019.
<https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-14-EU-US-Relations-Internet-Governance2.pdf>.
- Homeland Security Today. “U.S. Government to Spend Over \$18 Billion on Cybersecurity.” Last Modified June 23, 2020. <https://www.hstoday.us/subject-matter-areas/cybersecurity/u-s-government-to-spend-over-18-billion-on-cybersecurity/>.
- Human Rights Watch. “China: Abusive Cybersecurity Law set to be Passed.” Last modified November 6, 2016. <https://www.hrw.org/news/2016/11/06/china-abusive-cybersecurity-law-set-be-passed>.
- Ichihara, Maiko. “The Changing Role of Democracy in Asian Geopolitics.” *Carnegie Endowment for International Peace*, September 14, 2017, <https://carnegieendowment.org/2017/09/14/changing-role-of-democracy-in-asian-geopolitics-pub-73110>.
- International Civil Aviation Organization. “About ICAO.” Accessed January 26, 2021. <https://www.icao.int/about-icao/Pages/default.aspx>.
- Jensen, Benjamin, and Brandon Valeriano. *The Myth of the Cyber Offense: The Case for Restraint*. Cato Institute Policy Analysis no. 862. Washington DC: Cato Institute, 2019. <https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint>.
- Jensen, Benjamin, Ryan Maness, and Brandon Valeriano. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford: Oxford University Press, 2018.
- Jones, Bruce, and Torrey Taussig. “Democracy & Disorder: The Struggle for Influence in the New Geopolitics.” Brookings Institute Report. Washington DC: The Brookings Institute, 2019. https://www.brookings.edu/wp-content/uploads/2019/02/FP_20190226_democracy_report_WEB.pdf.
- Kagan, Robert. “History’s Back: Ambitious Autocracies, Hesitant Democracies.” *Carnegie Endowment for International Peace*, August 25, 2008. <https://carnegieendowment.org/2008/08/25/history-s-back-ambitious-autocracies-hesitant-democracies-pub-20401>.
- King, Angus. “NDAA Enacts 25 Recommendations from the Bipartisan Cyberspace Solarium Commission.” Last modified January 02, 2021. <https://www.king.senate.gov/newsroom/press-releases/ndaa-enacts-25-recommendations-from-the-bipartisan-cyberspace-solarium-nyecommission>.
- Kranzberg, Melvin. “Technology and History: ‘Kranzberg’s Laws.’” *Technology and Culture* 27, no. 3 (1986): 544-560.
- Lane, Charles. “Why Big Tech’s Attempt to Stifle Free Speech Could be Futile – or Worse.”

- Washington Post*, January 11, 2011. https://www.washingtonpost.com/opinions/why-big-techs-attempt-to-stifle-free-speech-could-be-futile--or-worse/2021/01/11/e912acac-5432-11eb-a931-5b162d0d033d_story.html.
- Lee, Sang, Ainsley Katz, Karrie Jefferson, Val Cofield, and Laura Bate. "The Cyberspace Solarium Commission on Norms." *Council on Foreign Relations Blog*, April 16, 2020, <https://www.cfr.org/blog/cyberspace-solarium-commission-norms>.
- Leiner, Barry, Vinton Cerf, David Clark, Robert Kahn, Leonard Kleinrock, Daniel Lynch, Jon Postel, Larry Roberts, and Stephen Wolff. "Brief History of the Internet: 1997." *Internet Society*. Last edited 1997. <https://www.internetsociety.org/resources/doc/2017/brief-history-internet/>.
- Lerman, Rachel, and Cat Zakrzewski. "Facebook Bans on New Political Ads Starts Off with Major Hiccups." *Washington Post*, October 27, 2020. <https://www.washingtonpost.com/technology/2020/10/27/facebook-ban-new-political-ads/>.
- Lewis, Larry L, and Diane Vivrichek. *Rethinking the Drone War: National Security, Legitimacy, and Civilian Casualties in U.S. Counterterrorism Operations*. Quantico, VA: Marine Corps University Press, 2016. <https://www.hsdl.org/?view&did=798675>.
- Libicki, Martin. "Why Cyberdeterrence is Different." In *Cyberdeterrence and Cyberwar*, 52-56. Santa Monica: RAND Corporation, 2009.
- Liles, Samuel. "Cyber Security Defense and Attribution" Lecture by Samuel Liles, 2015-2018 Special Advisor & "Ciso in Residence," Cyber Threat Analysis, Department of Homeland Security. By Chris Demchak. US Naval War College. May 18, 2017. <http://selil.com/archives/6791>.
- Limbago, Andrea. "The Global Push for Cyber Sovereignty is the Beginning of Cyber Fascism," *The Hill*, December 14, 2016. <https://thehill.com/blogs/congress-blog/technology/310382-the-global-push-for-cyber-sovereignty-is-the-beginning-of>.
- Lucas, George. *Ethics and Cyber War: The Quest for Responsible Security in the Age of Digital Warfare*. New York: Oxford University Press, 2017.
- Lucas, George. "State Sponsored Hacktivism and the Advent of 'Soft War.'" *Ethics and Armed Forces*, no. 2 (2014): 16-23.
- Macaes, Bruno. "Russia to China: Together We Can Rule the world." *Politico*, February 17, 2019. <https://www.politico.eu/blogs/the-coming-wars/2019/02/russia-china-alliance-rule-the-world/>.
- Mahnken, Thomas G., and Roger I. Zakheim. "Biden's Post-COVID Defense Budget Choice: A

- Resurgence or a Decline.” *Defense News*, January 19, 2021.
<https://www.defensenews.com/smr/transition/2021/01/19/bidens-post-covid-defense-budget-choice-a-resurgence-or-a-decline/>
- Malcomson, Scott. “The New Cyber Normal.” *Carnegie Reporter*, June 7, 2018.
<https://medium.com/carnegie-reporter/the-new-cyber-normal-8cd50fb17ea0>.
- Maness, Ryan, and Brandon Valeriano. “The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-11.” *Journal of Peace Research* 51, no. 3 (2014): 347-360.
<file:///Users/emilleprosko/Downloads/CyberdyanamicsJPR51-3.pdf>.
- Mazarr, Michael, Oriana Mastro, Christopher Preble, and Kori Shake. “Great Power Competition.” *Defense 2020*. Podcast audio. January 15, 2020.
<https://www.csis.org/analysis/great-power-competition>.
- McCabe, David. “F.C.C Designates Huawei and ZTE as National Security Threats.” *New York Times*, June 30, 2020.
<https://www.nytimes.com/2020/06/30/technology/fcc-huawei-zte-national-security.html>.
- Microsoft. “Protecting People in Cyberspace: The Vital Role of the United Nations in 2020.” Last modified December 2019. <https://www.un.org/disarmament/wp-content/uploads/2019/12/protecting-people-in-cyberspace-december-2019.pdf>.
- Mordor Intelligence. “Cybersecurity Market-Growth Trends, COVID-19 Impact, and Forecasts (2021-2026) Report.” Accessed on January 20, 2021.
<https://www.mordorintelligence.com/industry-reports/cyber-security-market>.
- Nakasone, Paul M. “A Cyber Force for Persistent Operations,” *Joint Forces Quarterly* 92 (2019): 10-14 <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf>.
- Ney, Paul C. “DOD General Counsel Remarks at U.S. Cyber Command Legal Conference.” Speech. Fort Meade, Maryland, March 2, 2020.
<https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>.
- North Atlantic Treaty Organization. “NATO Cyber Defence.” Fact Sheet. Last modified July 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.
- Nye, Joseph. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, Issue 3 (2017): 68-69. https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266.
- Offer, Avner. *The First World War: An Agrarian Interpretation*. Oxford: Clarendon Press, 1991.
- Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. *Defense Budget*

Overview: Irreversible Implementation of the National Defense Strategy. Washington, DC: U.S. Department of Defense, 2020.
https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/fy2021_Budget_Request_Overview_Book.pdf.

O'Rourke, Ronald. *Renewed Great Power Competition: Implication for Defense – Issues for Congress*. CRS Report No. R43838. Washington, DC: Congressional Research Service, 2020. <https://crsreports.congress.gov/product/pdf/R/R43838/71>.

Polyakova, Alina and Chris Meserole. "Exporting digital authoritarianism: The Russian and Chinese models." *Brookings Institute*. August 27, 2019. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

Pomerleau, Mark. "How 'Hunt Forward' Teams Can Help Defend Networks." *Fifth Domain*. February 12, 2020. <https://www.fifthdomain.com/dod/2020/02/12/how-hunt-forward-teams-can-help-defend-networks/>.

Rahn, Wesley. "Zhenhua Data Leak Exposes China's New 'Hybrid Warfare.'" *Deutsche Welle*. September 29, 2020. <https://www.dw.com/en/zhenhua-data-leak-exposes-chinas-new-hybrid-warfare/a-55083540>.

Richard, Carl, Thomas Ricks, and Caroline Winter, "What the Founders Learned from the Greeks and the Romans." Podcast audio. December 8, 2020.
<https://constitutioncenter.org/interactive-constitution/podcast/what-the-founders-learned-from-the-greeks-and-romans>.

Rovner, Josh. "Cyber War as an Intelligence Contest." *War on the Rocks Special Series: The Brush Past*, September 16, 2019. <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/#:~:text=The%20cyberspace%20competition%20is%20an,not%20be%20our%20best%20guide>.

Rovner, Josh. "Did the Cyber Solarium Commission Live Up To its Name." *War on the Rocks Special Series: The Brush Pass*, March 19, 2020. <https://warontherocks.com/2020/03/did-the-cyberspace-solarium-commission-live-up-to-its-name/>.

Rovner, Josh. "More Aggressive and Less Ambitious: CYBERCOM's Evolving Approach." *War on the Rocks Special Series: The Brush Past*, September 14, 2020.
<https://warontherocks.com/2020/09/more-aggressive-and-less-ambitious-cyber-commands-evolving-approach/>.

Ryan-Mosley, Tate. "Why Facebook's Political-ad Ban is Taking On the Wrong Problem." *MIT Technology Review*, September 6, 2020.
<https://www.technologyreview.com/2020/09/06/1008192/why-facebooks-political-ad-ban-is-taking-on-the-wrong-problem/>.

Schadlow, Nadia. "Peace and War, the Space Between" *War on the Rocks*, August 18, 2014. <http://warontherocks.com/2014/08/peace-and-war-the-space-between/>.

Schmitt, Michael N. "Grey Zones in the International Law of Cyberspace." *The Yale Journal of International Law* 42, no. 2 (2017): 1-21. https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf.

Schoka, Andrew. "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat." *War on the Rocks*, April 3, 2019. <https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/>.

Schneider, Jacquelyn. "A Strategic Cyber No-first-use Policy? Addressing the U.S. Cyber Strategy Problem." *The Washington Quarterly* 43, no. 2 (June 2020):159-175, <https://doi.org/10.1080/0163660X.2020.1770970>.

Seeing Red: The Development of Maoist Thought on Insurgency. Compiled by Bradford Lee in the NWC Strategy and Policy Department.

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.

Shepardson, David. "FCC Begins Process of Halting China Telecom U.S. Operations." *Reuters*, December 10, 2020. <https://www.reuters.com/article/usa-china-tech/fcc-begins-process-of-halting-china-telecom-u-s-operations-idUSKBN28K2ER>.

Slayton, Rebecca. "What is the Cyber Offense-Defense Balance?" *International Security* 41, no. 3 (2017): 72-109. https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00267.

Snow, John. "Top 5 most notorious cyberattacks." *Kaspersky Daily Blog*, November 6, 2018. <https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/>.

Solomon, Salem. "After Allegations of Spying, African Union Renews Huawei Alliance." *Voice of America*, June 7, 2019. <https://www.voanews.com/africa/after-allegations-spying-african-union-renews-huawei-alliance>.

Stanford Encyclopedia of Philosophy. "Deontological Ethics." *Stanford Center for the Study of Language and Information*, October 30, 2020. <https://plato.stanford.edu/entries/ethics-deontological/#DeoTheKan>.

Technavio Research. "Top 5 Vendors in the Global Submarine Fiber Cable Market from 2017 to 2021 | Technavio." *BusinessWire*, October 30, 2017.

- <https://www.businesswire.com/news/home/20171030006219/en/Top-5-Vendors-in-the-Global-Submarine-Fiber-Cable-Market-from-2017-to-2021-Technavio>.
- Tibken, Shara. "Questions show many Senators don't get Facebook." *CNET*, April 11, 2018. <https://www.cnet.com/news/some-senators-in-congress-capitol-hill-just-dont-get-facebook-and-mark-zuckerberg/>.
- The White House. *National Cyber Strategy of the United States of America*. Washington, DC: The White House, 2018. <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
- The White House. *United States Strategic Approach to the People's Republic of China*. Washington, DC: The White House, 2020. <https://china.usembassy-china.org.cn/wp-content/uploads/sites/252/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.24v1.pdf>.
- Theohary, Catherine A. *Defense Primer: Cyberspace Operations*, CRS Report No. IF10537. Washington, DC: Congressional Research Service, 2020. <https://crsreports.congress.gov/product/pdf/IF/IF10537>.
- U.N. General Assembly. *Resolution Adopted by the General Assembly on 23 December 2015*. 70th sess. 2015. Item 92. <https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf>.
- U.N. Group of Government Experts. General Assembly. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. 70th sess. 2015. Item 93. <https://undocs.org/A/70/174>.
- U.S. Army. *Offense and Defense*. Army Doctrine Publication (ADP) 3-90. Washington DC: U.S. Army, 2019.
- U.S. Congress. House. *The Evolution of Hybrid Warfare and Key Challenges: Hearing before the Committee on Armed Services, House of Representatives*. 115th Cong., 1st sess., 2017. <https://www.govinfo.gov/content/pkg/CHRG-115hhrg25088/pdf/CHRG-115hhrg25088.pdf>.
- U.S. Cyber Solarium Commission. *Cyberspace Solarium Commission Final Report*. Chaired by Senator Angus King and Representative Mike Gallagher. March 2020. <https://secureservercdn.net/166.62.108.22/5kb.d9b.myftpupload.com/wp-content/uploads/2020/03/CSC-Final-Report.pdf>.
- U.S. CYBERCOM. *Achieve and Maintain Cyberspace Superiority: Command Vision*. Washington, DC: USCYBERCOM, 2018. <https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf>.

U.S. Department of Defense. *Summary of the 2018 National Defense Strategy: Sharpening the American Military's Edge*. Washington, DC: Government Printing Office, 2018.

U.S. Department of Transportation. "National Highway Traffic Safety Administration Regulations." *NHTSA.gov*, <https://www.nhtsa.gov/laws-regulations/fmvss>.

Valeriano, Brandon. "Article 83 Review on 'What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.'" *H-Diplo/ISSF*. July 26, 2017. <https://issforum.org/articlereviews/83-cyber>.

Vergun, David. "Great Power Competition can Involve Conflict Below Threshold of War." *Defense.gov*, October 2, 2020. <https://www.defense.gov/Explore/News/Article/Article/2364137/great-power-competition-can-involve-conflict-below-threshold-of-war/>.

Volz, Dustin. "White House Confirms it has Relaxed Rules on U.S. Use of Cyber Weapons." *Wall Street Journal*, September 20, 2018. https://www.wsj.com/articles/white-house-confirms-it-has-relaxed-rules-on-u-s-use-of-cyber-weapons-1537476729_.

Weed, Scott. *US Policy Response to Cyber Attack on SCADA Systems Supporting Critical National Infrastructure*. Maxwell AFB: Air University Press, 2017. https://media.defense.gov/2017/Nov/20/2001846609/-1/-1/0/PPP0007_WEED_SCADA.PDF.

Westby, Jody. "SolarWinds Cyber Attacks Raise Questions About the Company's Security Practices and Liability." *Forbes Magazine*, December 16, 2020. <https://www.forbes.com/sites/jodywestby/2020/12/16/solarwinds-cyber-attacks-raise-questions-about-the-companys-security-practices-and-liability/?sh=4c80f174711d>.