NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE SPACE BETWEEN: POLICY IMPLICATIONS FOR THE CONCEPTUALIZATION OF CYBERSPACE AS A DOMAIN

by

Jonathan Miller

March 2022

Co-Advisors: Mollie R. McGuire
Anthony Canan

THIS PAGE INTENTIONALLY LEFT BLANK

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

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

4. TITLE AND SUBTITLE THE SPACE BETWEEN: POLICY IMPLICATIONS FOR THE CONCEPTUALIZATION OF CYBERSPACE AS A DOMAIN	**5. FUNDING NUMBERS**
6. AUTHOR(S) Jonathan Miller	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

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

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

13. ABSTRACT (maximum 200 words)

The objective of this thesis is to identify the extent to which defining cyberspace as domain will affect the formulation of Homeland Security Enterprise (HSE) policy related to cyberspace in the future. However, as cyberspace lacks a consistent definition, a prerequisite for this discussion is establishing exactly what cyberspace is. Having provided framework for understanding cyberspace, the policy approaches of the last five presidential administrations were examined to determine whether they treat cyberspace as a domain and what this suggests about future policy development. In the end, there appears to be a tendency for each presidential administration to treat cyberspace as an instrument rather than a domain, which is an approach that will likely require adjustment as threats within cyberspace evolve so as to adequately address them.

14. SUBJECT TERMS cyberspace, cybersecurity, metaphysics	**15. NUMBER OF PAGES** 71
	16. PRICE CODE

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

NSN 7540-01-280-5500

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

THE SPACE BETWEEN: POLICY IMPLICATIONS FOR THE CONCEPTUALIZATION OF CYBERSPACE AS A DOMAIN

Jonathan Miller
Crime Analyst - Strategic Services Division, City of Portland, Portland Police Bureau
BA, Portland State University, 2015
MA, Middlebury Institute of International Studies at Monterey, 2017

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2022**

Approved by: Mollie R. McGuire
Co-Advisor

Anthony Canan
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The objective of this thesis is to identify the extent to which defining cyberspace as domain will affect the formulation of Homeland Security Enterprise (HSE) policy related to cyberspace in the future. However, as cyberspace lacks a consistent definition, a prerequisite for this discussion is establishing exactly what cyberspace is. Having provided framework for understanding cyberspace, the policy approaches of the last five presidential administrations were examined to determine whether they treat cyberspace as a domain and what this suggests about future policy development. In the end, there appears to be a tendency for each presidential administration to treat cyberspace as an instrument rather than a domain, which is an approach that will likely require adjustment as threats within cyberspace evolve so as to adequately address them.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

AC	Activity Chain
C→C	Cyberspace to Cyberspace
C→P	Cyberspace to Physical Space
CNCI	Comprehensive National Cybersecurity Initiative
CPR	Cyberspace Policy Review
EO	Executive Order
FOB	Forward Operating Base
HSE	Homeland Security Enterprise
NCS	National Cyber Strategy
NFT	Non-fungible Token
NIPP	National Infrastructure Protection Plan
NPISP	National Plan for Information Systems Protection
NSS	National Security Systems
NSSC	National Strategy to Secure Cyberspace
P→C	Physical Space to Cyberspace
P→P	Physical Space to Physical Space
PD	Presidential Directive
PPD	Presidential Policy Directive
TCP/IP	Transmission Control Protocol/Internet Protocol
WTO	World Trade Organization

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The objective of this thesis is to identify the extent to which defining cyberspace as a domain will affect the formulation of homeland security enterprise (HSE) policy related to cyberspace in the future. To that end the primary research question is as follows:

- What will be the practical impact of defining cyberspace as a domain on Homeland Security Policy?

While the term "cyberspace" frequently makes appearances throughout the HSE, there is a lack of common agreement on (a) whether cyberspace is a "space" at all, and (b) if it is a space, what that space looks like. Those who disagree on these points can generally be divided into two categories: instrumentalists, or those that view cyberspace as a tool and basically a convenient metaphor for network infrastructure; and spatialists, or those that view cyberspace as a space.[1] Disagreement on what cyberspace is leads to inconsistencies in policies meant to govern cyberspace, as the concerns and focus look different depending on how the policy views cyberspace. Therefore, assessing how cyberspace has been understood in the past is necessary when determining what future policy may look like if the use of cyberspace as a concept persists. As assessing the entirety of HSE perspectives on cyberspace would be a touch impractical, this thesis focuses narrowly approaches to cybersecurity by the Clinton, Bush, Obama, Trump, and Biden administrations.

However, as there is no extant common agreement on what cyberspace is or how it works, prior to engaging in the aforementioned analysis one must establish that baseline first. Herein, cyberspace is considered first metaphysically, and described as a multi-mind dependent reality that exists independently of any lone-mind. It is a reality nested within physical reality, and so limited by both physical laws and the constraints placed on behavior and the creation of artifacts therein by the technical infrastructure that makes its existence possible. Based upon this understanding, three key considerations must be present with

[1] Rebecca Bryant, "What Kind of Space Is Cyberspace?," *Minerva: An Internet Journal of Philosophy* 5 (2001): 138–55; Orin S. Kerr, "The Problem of Perspective in Internet Law," *Georgetown Law Journal* 91 (2002), https://doi.org/10.2139/ssrn.310020.

policy for it to adequately address cyberspatial issues. These are the mutability of cyberspace, the composition and nature of things in cyberspace, and the nature of trans-spatial activity. Of these, the first is probably the most accessible if only because the narrative vis-à-vis the speed with which network technology has developed and is developing is so common.[2] Cyberspace is constantly changing, in part, because the technology that supports it is constantly evolving. As to the second, whereas physical objects are identified as such because their component parts are physically proximate, the component parts of a thing in cyberspace may or may not be. A website like Facebook, for example, is not stored on a single server somewhere in California, and yet is understood to be one "thing."[3] As to the nature of trans-spatial activity, there are moments where activity in cyberspace can affect physical space and vice versa. Examples include everything from the increasing size and value of data sets as a result of both manual and automated data entry, the value of physical data storage devices increasing when storing cryptocurrency, or a person acting out after being radicalized online. If one fails to account for the preceding, they have effectively failed to account for some fundamental features of cyberspace. For example, the Amazon website, like Facebook, is not comprised of components that exist in one physical place, and so one cannot simply seize it without identifying all of the data sources that contribute to it, and nor can they fail to consider that doing so would result in real consequences for physical global supply chains.

Given the strictly instrumental approach of four of the past five presidential administrations to cybersecurity, it would seem that cybersecurity has surprisingly little to do with cyberspace at all. Beginning with the Clinton administration, discourse around cybersecurity has been inextricably linked with critical infrastructure protection, focusing

---

[2] William J. Clinton, "Public Papers of the Presidents of the United States: William J. Clinton (1997, Book II) - Remarks Announcing the Electronic Commerce Initiative," 1997, https://www.govinfo.gov/content/pkg/PPP-1997-book2/html/PPP-1997-book2-doc-pg895.htm; John D. Moteff, "Critical Infrastructures: Background and Early Implementation of PDD-63" (Library of Congress Washington, DC, Congressional Research Service, June 19, 2001), https://apps.dtic.mil/sti/citations/ADA478523; The White House, "National Strategy to Secure Cyberspace" (United States. White House Office, February 2003), https://www.hsdl.org/?abstract&did=1040; The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 8, 2009," National Security Archive, May 8, 2009, https://nsarchive.gwu.edu/document/21424-document-28.

[3] "Facebook Data Centers," Facebook Data Centers, accessed December 13, 2021, https://datacenters.fb.com/.

narrowly on the vulnerabilities of network infrastructure.[4] The one exception was the approach of the Trump administration, which explicitly engaged with concerns about behavior within cyberspace that were not addressed by previous administrations nor have they been addressed by the Biden administration at the time of this writing.[5] When engaging with more recent topics around behavior like dis/misinformation on-line, the topic does not tend to be covered within cybersecurity discourse at the administrative level because dis/misinformation can spread without exploiting network vulnerabilities, even though it is sometimes framed as a cybersecurity issue. Consequently, in answer to the principal research question of this thesis, one would presume that in the future either (a) that discursive space will be created within the context of cybersecurity discourse, or (b) a new and secondary policy framework will arise to address issues related to cyberspace that cybersecurity discourse has thus far failed to account for. Otherwise, cybersecurity policy will fail to account for those unique challenges that cyberspace presents.

[4] James D. Boys, "The Clinton Administration's Development and Implementation of Cybersecurity Strategy (1993–2001)," *Intelligence and National Security* 33, no. 5 (July 29, 2018): 762, https://doi.org/10.1080/02684527.2018.1449369.

[5] The White House, *National Cyber Strategy of the United States of America.* (Washington, District of Columbia: United States. White House Office, 2018), 87.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The author would like to thank Dr. Mustafa Canan and Dr. Mollie McGuire for their willingness to extend their expertise; the 2005/2006 CHDS cohort and instructors for facilitating many spirited discussions on the contents herein; and his wife, Betsy Miller, for her love, support, and patience, without which this document would not exist, and for whom the effort is dedicated.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The 20th and 21st centuries saw the rise of the internet, an advanced communication technology comprising innumerable interconnected devices that has provided mankind with an opportunity for the exchange of information and ideas. The space provided by that technology, cyberspace, has only been recently recognized as a domain within which one may exercise either altruistic or malign intent.[1] Prior to the invention of cyberspace, the inventions of man were analyzed only as manufactured products. Since that invention, mankind has been forced to cope with a purely human made space within which people may interact, and this presents unique challenges. Despite cyberspace's existence as a medium that empowers the rich exchange of information, whether cyberspace constitutes a separate domain is not necessarily agreed upon.[2] To some, the internet is simply an instrument—a means for spanning vast distances between organizations and individuals so as to enable collaborative activity regardless of physical separation. To others, the internet supports a space within which people may substantively interact. This differentiation is key: Does cyberspace truly exist, or is it simply an abstraction of human activity that relies on the use of advanced communication technologies? From a policy perspective, is the object of interest a space within which people interact or an instrument that people use? According to the U.S. Department of Defense, cyberspace is a warfighting domain, and this perspective has been reflected at several levels within the homeland security enterprise.[3] Given that cyberspace as a "space" represents a premise for strategic policy, what effects does this have on U.S. preparedness

[1] "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit," NATO Cooperative Cyber Defence Centre of Excellence, accessed February 14, 2021, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

[2] Chris McGuffin and Paul Mitchell, "On Domains: Cyber and the Practice of Warfare," *International Journal* 69, no. 3 (2014): 394–412; Michael Kreuzer, "Cyberspace Is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age," The Strategy Bridge, July 8, 2021, https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age.

[3] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Department of Defense, 2011), 19.

vis-à-vis cyberspace over time? Formulating policy based on this premise forces policymakers to think about human activity within a domain that exists solely as a consequence of human action, and this is unprecedented. Given the trajectory of cyberspace's development, it is expected that the cyberspace of the future will be as unfamiliar to us as the cyberspace of today would have been to a practitioner working before the introduction of the iPhone. If this is true, then radical change remains on the horizon. Preparing in advance for those changes will be critical for ensuring that the United States will be positioned to operate within cyberspace effectively and efficiently; as such, preparation must be based on a robust conceptual understanding of what cyberspace is. This thesis is intended to provide a potential foundation for that understanding. To examine how this distinction might alter or affect policymaking, one must first develop an understanding of what such a space might comprise: What is cyberspace? Second, one must examine how U.S. policy interacts with said space. Third, one must assess whether established policy adequately considers the nuances of how cyberspace functions. Finally, one must consider whether extant policy is flexible enough to cope with what cyberspace may become.

B. RESEARCH DESIGN

The objective of this thesis is to identify the extent to which defining cyberspace as a domain will affect the formulation of homeland security enterprise (HSE) policy related to cyberspace in the future. To do so, the thesis first discusses what cyberspace is and then considers instances when HSE policy has been oriented toward handling cyberspace as a domain. As capturing the totality of HSE policy would be impractical within the boundaries of a thesis, focus is be placed on the strategic approaches of the Clinton, Bush, Obama, Trump, and Biden presidential administrations vis-à-vis cybersecurity. As strategic objectives articulated at that level inform policies developed at lower echelons within the HSE, this was an accessible means for considering the HSE as a whole. The respective postures of these administrations were treated as cases, and analyzed to assess how this policy space has evolved and where it might be heading. Cybersecurity in particular was chosen as a point of focus because cyberspace plays a central role in the topic.

Collectively, the following chapters are intended to answer the question: What will be the practical impact of defining cyberspace as a domain on Homeland Security Policy? To get to the answer, the content is structured to move from a foundational understanding of what cyberspace is to a conversation about how policy has been developed to manage it. Chapter II begins by exploring how cyberspace is presently viewed, and describes a canon bounded by two poles: those that believe cyberspace is a "space," and those that do not. While this document draws the conclusion that cyberspace is indeed a space, when that view is expressed in the existing canon, there appears to be a general lack of clarity about what is meant when one is refers to it as a "space" or says it "exists." Given that, the literature review is followed by a metaphysical discussion, applying a modified Kantian perspective to develop a baseline understanding of what terms like "reality," "existence," and "space" actually mean. This exploration is necessary because in making the claim that cyberspace is a space, and indeed bounded by a novel reality, these terms as they are commonly understood cannot be invoked without some explanatory context.

Armed with a metaphysical description of cyberspace, Chapter III outlines considerations that should be taken into account when formulating policy. Chapter IV explores how the aforementioned presidential administrations have approached cybersecurity, as reflected in policy documents produced by each of them. Finally, Chapter V seeks to provide an answer to the primary point of inquiry.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CYBERSPACE

A. UNDERSTANDING CYBERSPACE

As noted by a December 1996 New York Magazine article, "Cyber is such a perfect prefix, because nobody has any idea what it means, it can be grafted onto any old word to make it seem new, cool—and therefore strange, spooky."[4] The fact that today one could form a cogent sentence by suggesting a "cyberpunk practiced cybersex in cyberspace irresponsibly from a cybersecurity perspective in their Cybertruck" illustrates the extent to which the prefix seems to do little other than denote a vague relationship with the internet or a contemporary aesthetic. Merriam-Webster define cyber as "of, relating to, or involving computers or computer networks (such as the internet)."[5] It is a generalization by definition. So much so that it lends itself to usage in a wide variety of contexts, ultimately leading to unnecessary semantic difficulties that impede serious discussion.[6]

Cyberspace suffers from a similar issue. A lack of specificity around what is meant when the term is invoked lends itself to generalizations that make the development of a common understanding of cyberspace difficult. Is it an instrument, a space, more than one thing, or a metaphor gone amok? Recall the amorous cyberpunk referenced above. In that illustration they are presented as being *in* two "places" at once: in cyberspace, and in a Cybertruck—a physical vehicle—hopefully parked on sufficiently private property. While the illustration remains entirely reasonable, it is easy enough to see why this might be a source of confusion and debate.

---

[4] New York Magazine, "Cyber Extra!," *New York Magazine*, December 23, 1996; Online Etymology Dictionary, "Cyber-," accessed November 7, 2021, https://www.etymonline.com/word/cyber-#etymonline_v_29224.

[5] Merriam-Webster, "Definition of CYBER," accessed November 13, 2021, https://www.merriam-webster.com/dictionary/cyber.

[6] Andrew Futter, "'Cyber' Semantics: Why We Should Retire the Latest Buzzword in Security Studies," *Journal of Cyber Policy* 3, no. 2 (May 4, 2018): 201–16, https://doi.org/10.1080/23738871.2018.1514417.

"Cyberspace" as a concept has been debated since William Gibson coined the term in his 1984 novel *Neuromancer*.[7] Therein, he describes it as "a consensual hallucination experienced daily by billions of legitimate operators."[8] This presents it as a space that is corporeally inaccessible as it has no physical attributes yet exists as an abstract common ground within which people can exchange information and share experiences. When cyberspace is discussed today, one regularly sees references to "operating in" cyberspace, which would suggest that, like Gibson, cyberspace is perceived of as occupiable.[9] However acceptance of that view is not universal. At one end of the spectrum, some scholars suggest it is comparable to physical space, as the ways in which "it" is interacted with appear to meet the criteria we would apply when accessing physical space itself.[10] At the other end, some suggest that viewing cyberspace and physical space as comparable can be problematic as conflating cyberspace with physical space may lead one to treat actions taken using the internet differently than they would otherwise based upon an exaggeration of user experiences.[11]

The majority of discussions around cyberspace fall somewhere between existence and non-existence and may be directed less toward whether or not cyberspace "is" in favor of assessing whether or not it would be relevant if it were to a particular field.[12] If cyberspace does exist, the absence of language required to discuss it is problematic, for experiences had therein can inform human behavior in physical space as well; and that behavior will be difficult to analyze absent a common understanding of the phenomena that drive it.

---

[7] William Gibson, *Neuromancer* (New York: Penguin Random House, 2019).

[8] Gibson, 51.

[9] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*.

[10] Bryant, "What Kind of Space Is Cyberspace?"

[11] Kerr, "The Problem of Perspective in Internet Law."

[12] Julie Cohen, "Cyberspace as/and Space," *Columbia Law Review* 107 (2007): 210–56; Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 321–36.

1. Spatialism: Cyberspace Exists

Scholars arguing in favor of describing cyberspace as a space or domain, whom will hereafter be referred to as "spatialists," premise their conclusions on how physical space is understood, in an attempt to identify whether cyberspace is categorically similar. Physical space as concept has been long debated, and is often framed as an issue of identifying whether or not it is substantive, meaning that it is an independent substance, or relational, meaning that it is non-substantive but rather descriptive of spatial relationships between entities.[13] The thinking of Isaac Newton is often presented as being representative of the substantive view, while the Gottfried Wilhelm Leibniz is often presented as being representative of the relational view, though there is debate as to whether or not characterizing Newton's perspective as being substantive is fair.[14] For his part, Newton ascribes essential properties to space, describing it as "continuous or infinitely divisible, infinite, motionless, eternal, immutable, and uniform, among other things," and therefore an independent extant thing.[15] For Leibniz, space is clearly relational, or "an abstraction from distances between physical objects in time, which is made up by the human mind and thus only ideal."[16] Consequently, while Leibniz would not describe space as anything other than a relational concept, describing it necessarily invokes similar concepts as described by Newton. Whereas Newton would describe a distance between two points in space, thereby necessitating the invocation of notions of distance, place, and time; Leibniz would suggest that such descriptions require at least two extant objects, but still apply those similar criteria of distance, place, and time. Thus, whether or not space is substantive or relational, these fundamental descriptors provide a touchstone for scholars examining cyberspace to apply and assess whether cyberspace may be similarly understood. However, when making these comparisons, spatialists often diverge with respect to how they

---

[13] Bryant, "What Kind of Space Is Cyberspace?"; Alejandro Cassini, "Newton and Leibniz on Non-Substantival Space," *Theoria. Revista de Teoría, Historia y Fundamentos de La Ciencia* 20, no. 1 (March 1, 2005): 25–43.

[14] Cassini, "Newton and Leibniz on Non-Substantival Space."

[15] Cassini, 27.

[16] Wolfgang Malzkorn, "Leibniz's Theory of Space in the Correspondence with Clarke and the Existence of Vacuums," in *Twentieth World Congress of Philosophy* (Twentieth World Congress of Philosophy, Boston, MA, 1998), https://www.bu.edu/wcp/Papers/Mode/ModeMalz.htm.

conceptualize cyberspace generally. In her 2001 article "What Kind of Space is Cyberspace," Rebecca Bryant suggests there are "two spurs of cyberspace…a 3-D cyberspatial environment…[and a] world of networks of computers linked via cables and routers."[17] Focusing on the latter spur, she outlines how fundamental notions of place, distance, movement, route, time, and dimension might be applied and, therefore, qualify cyberspace as a space based on criteria similar to what was presented by Newton and Leibniz.[18] Julie E. Cohen in her 2007 article "Cyberspace as/and Space," presents cyberspace as a more abstract space defined solely by shared experience rather than a physical network or 3-D visualization.[19] Thus we have three distinct versions of cyberspace being held up as a point of comparison: A physical Network, a 3-D virtual environment, and an abstract shared space.[20]

A more recent example of a spatialist view attempts to blend these perspectives into a single model. Published in 2018, *Joint Publication 3-12: Cyberspace Operations* (JP 3-12) is the joint doctrine used by the U.S. Department of Defense (DOD) "to plan, execute, and assess cyberspace operations.[21] It defines cyberspace as "the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data,"[22] and describes it as being comprised of both physical and non-physical components by applying a 3 layer model. These are the "Physical Network Layer" (PNL), "Logical Network Layer" (LNL), and "Cyber-Persona Layer" (CPL).[23] The PNL includes physical devices, the LNL includes elements of a network that may correspond with one or more components of the PNL (e.g., a website is not stored in one location, but is the consolidation of data from many locations), and the

---

17 Bryant, "What Kind of Space Is Cyberspace?," 139.

18 Bryant, 141; Michael Benedikt, ed., *Cyberspace: First Steps* (Cambridge, MA: MIT Press, 1991), 125.

19 Cohen, "Cyberspace as/and Space," 226.

20 Cohen, 226.

21 "JP 3-12 Cyberspace Operations" (Washington, DC: Joint Chiefs of Staff, 2018), i, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

22 "JP 3-12 Cyberspace Operations," I–1.

23 "JP 3-12 Cyberspace Operations," I–3.

CPL includes user accounts, where a cyber-persona may be comprised of many accounts consolidated and perceived of singularly.[24] JP 3-12 approaches the "space" problem by breaking it apart into conceptual components.

These perspectives are rather typical with respect to understanding the nature of cyberspace after 2000. Interestingly though, some of the deepest thinking on cyberspace as a space presented itself much earlier, and well before the cyberspace of today was established. In 1991, only seven years after the word cyberspace was created, *Cyberspace: First Steps*, edited by Michael Benedikt, was published.[25] This collection of pieces explores what cyberspace is and how people did and would interact with it. While there are a range of viewpoints in the book, the general consensus points toward the more abstract line of thinking emphasized by Cohen, with one author suggesting "cyberspace is like Oz—it is, we get there, but it has no location."[26] To get there, the authors repeatedly point to well-established philosophical writings by such minds as Newton, Leibniz, and Plato, suggesting their own works runs along similar lines—to define what it means to exist.

2. Instrumentalism: Cyberspace Does Not Exist

Scholars arguing against the concept of cyberspace as a space, hereafter referred to as "instrumentalists," prefer to view it as simply a metaphor for what is experienced when using network technology as an instrument; and emphasize the extent to which applying the metaphor may be misleading, irrelevant, or produce problematic consequences. Authors like Timothy Wu suggest the metaphor was largely adopted out of convenience and that in the end, the place-based understanding of cyberspace is disproved by its own technology, which can but does not necessarily require the creation of places.[27] Martin Libicki suggests that identifying cyberspace as a space, or not, is a pointless exercise; though he explicitly endorses the instrumental view, contending that "understanding

---

[24] "JP 3-12 Cyberspace Operations," I-2-I–4.

[25] Benedikt, *Cyberspace*.

[26] Nicole Stenger, "Mind Is a Leaking Rainbow," in *Cyberspace: First Steps* (Cambridge, MA: MIT Press, 1991), 53.

[27] Timothy Wu, "When Law & the Internet First Met," *Green Bag 2d* 3 (2000 1999), https://heinonline.org/HOL/LandingPage?handle=hein.journals/grbg3&div=28&id=&page=.

cyberspace as a warfighting domain is not helpful when it comes to understanding what can and should be done to defend and attack networked systems."[28] Both of these authors argue effectively that network architecture is significant, but in doing so they conveniently side step the arguments made by spatialists. As their arguments lean on the irrelevancy of the metaphor, there is no need within their framework to even engage in the spatialist discussion.

3. An Absence of Consensus: The Need for Spatial Clarity

The current body of literature that describes viewpoints on what cyberspace is or might be is diverse. While a diversity of views is reflective of a robust academic discourse, the absence of some kind of consolidation into a common understanding of what cyberspace is or is likely to be is problematic. Among spatialists there is disagreement as to what "cyberspace" they are discussing, while among instrumentalists there is little said other than to state that the spatialist view is incorrect. Given that instrumentalists do not tend to present arguments that address those presented by spatialists, and nor do arguments presented by spatialists necessarily preclude those presented by instrumentalists, it would appear that neither view has been invalidated completely. Conceptualizing cyberspace as a space does have merit, though an understanding of that space cannot exclude consideration of the way the infrastructure that comprises it is used. That being said, while the instrumentalist view is rather clear in so far as instrumentalists agree upon the composition of the instrument under discussion, the absence of consensus on the part of spatialists make the consistent application of their concepts difficult if not impossible, and therefore requires clarification. If one is to operate knowledgably within a space, one must have an understanding of what that space is.

Imagine for a moment if one were to examine physics literature and found no generalizable consensus on how to describe physical phenomena, or even what general context one might place those phenomena within—a jumbled heap of metaphysical exposition and ideological theorizing. Such a canon would be practically useless, and

[28] Libicki, "Cyberspace Is Not a Warfighting Domain," 322.

paralyzing from a policy perspective, as there would be no shared understanding of how the world works upon which to base strategic policy development. There are no ships absent the concept of buoyancy; no planes without lift; no rockets without gravity. Furthermore, since the mid-2000s, the philosophical exploration of what cyberspace is seems to have waned considerably, and work vis-à-vis cyberspace is more oriented toward how the military, public sector, or private sector, for example, should operate within it. Consequently, descriptions of what 'works best' in cyberspace abound in the absence of a shared consensus of what cyberspace looks like, or even what authors are referring to when they invoke the term. As there is currently a lack of consistency in the available canon, it will be necessary to create a description and lexicon to analyze domain-based policy. Before building such references, however, we must clarify what is meant when one suggests cyberspace exists.

B. REALITY, EXISTENCE, AND SPACE

Debates about how best to describe cyberspace are ultimately premised upon a simple declarative statement: cyberspace exists. Far from a metaphysical distraction, this notion is the singular premise that justifies presenting cyberspace as a domain, and consequently is deserving of a degree of clarity. When it is said that "cyberspace exists," what does that mean? To achieve that clarity, a few concepts need to be explored beforehand so this discussion can make sense: reality, existence, and space.

1. Reality and Existence

Reality is, first and foremost, a concept; the notion of a context within which things exist, and to exist is to occupy a context and be bounded by it. Therefore, when attempting to answer the question "what is reality," one is not seeking a description of a singular object or phenomenon, but rather a description of a context that contains objects and phenomena. As prior to the advent of cyberspace there had been no need to be so particular, when one previously asked that question it often had less to do with exploring what the concept of reality is, than what *this* reality is; meaning the specific context within which they exist, or perceive themselves to exist. This is a rather critical distinction, for while reality is itself simply an abstraction, *this* reality can and has been described by philosophers, physicists,

and mystics since time immemorial. Now that cyberspace does exist, the notion of an accessible parallel reality may be explored directly as one is now available to analyze. As a full review of humanity's predilection for existential theorizing would be a touch beyond the scope of this writing, for the purposes of this work the focus will be on two primary concepts: mind-independent reality, and mind-dependent reality. Mind-independent reality, also referred to as *metaphysical realism*, is "the thesis that the objects, properties and relations the world contains, collectively: the structure of the world, exists independently of our thoughts about it or our perceptions of it."[29] Should humanity vanish from the earth, the earth will persist in spite of our lack of stewardship. Mind-dependent reality, also referred to as *metaphysical antirealism*, by contrast posits that reality as we know it is reality as it is in a very literal sense. It does not necessarily preclude the existence of physical objects, but rather emphasizes the indivisibility of the external physical world and our own internal perceptions of that world.[30]

This tension between the internal and external pervades the discourse around what reality is, but there does seem to be a consensus that reality at least includes external inputs of some type. Therefore, this thesis argues that reality is comprised of mind-independent and mind-dependent; external and internal components. There is, however, a distinction to be made here with respect to hierarchy, for while mind-independent features exist independently, mind-dependent features exist within mind-independent containers: bodies. Thus, while from our perspective reality is the confluence of mind-independent and mind-dependent features, these two categories are not coequal as the former contains the latter. While it would be inappropriate to say that reality generally "exists," insofar as the suggestion infers that it exists *somewhere* (e.g., a super-reality), there is nothing

[29] Drew Khlentzos, "Challenges to Metaphysical Realism," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Spring 2021 (Metaphysics Research Lab, Stanford University, 2021), https://plato.stanford.edu/archives/spr2021/entries/realism-sem-challenge/.

[30] Hilary Putnam, "Realism," *Philosophy & Social Criticism* 42, no. 2 (February 1, 2016): 117–31, https://doi.org/10.1177/0191453715619959; Ruth Garrett Millikan, "Metaphysical Anti-Realism?," *Mind* 95, no. 380 (1986): 417–31.

problematic with pointing at a person and identifying *a* reality; a mind, as these sub-realities, or contexts for thought, are self-contained within a perceptible body.[31]

2. The Composition of Mind-Dependent Reality

Conceptualizing mind-independent reality is a relatively accessible task. Simply stating that discrete things exist outside of ourselves is sufficient to express the concept. By contrast, mind-dependent reality is more difficult to describe, as doing so requires describing the composition of thought which is a touch more abstract. For this we need to adapt some of the thinking that underlies the work of Immanuel Kant. According to Kant, reality is as we have thus far articulated it, to the extent that it includes both external and internal properties.[32] For him, however, there is no means for us to directly interact with external things as they are directly. Objects outside ourselves are seen by us as "appearances," meaning a projection of an object's, or "noumenon's," attributes as dictated by how we sensorily process them, or "sensible intuition." Collectively these appearances contribute to "phenomenon," or a concept of the sensed object. The noumena concept is further subdivided into positive and negative. Negative noumena are those objects described above, meaning an object that is perceivable via the senses. Positive noumena are perceivable by a non-sensible or "intellectual intuition." "A sensible intuition is one that can only intuit objects by being causally affected by them; a non-sensible intuition is one in which the intuition of the object brings the object into existence." Kant posits that even the possibility of positive noumena is not understandable to human beings as we

[31] Suggesting reality "exists" would infer the presence of a super-reality, or a context within which reality's existence was possible. While this would be an interesting discussion vis-à-vis supernatural phenomena and the metaphysical necessity of God, this could only be theoretical absent empirical evidence or faith. This would be, mostly, outside the scope of this writing, though we may return to this topic when discussing the relationship between humanity and cyberspace. See Benedikt Paul Göcke, "Did God Do It? Metaphysical Models and Theological Hermeneutics," *International Journal for Philosophy of Religion* 78, no. 2 (October 1, 2015): 215–31, https://doi.org/10.1007/s11153-014-9489-7. for an interesting discussion on this topic.

[32] Nicholas F. Stang, "Kant's Transcendental Idealism," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Spring 2021 (Metaphysics Research Lab, Stanford University, 2021), https://plato.stanford.edu/archives/spr2021/entries/kant-transcendental-idealism/.

interpret the world via sensory inputs that are subsequently processed by intellect rather than with intellect directly.[33]

Diverging from Kant on one semantic point, and two substantive points: the application of the term "object" when discussing mind-dependent reality, the discreetness of mind-dependent features, and the non-perceptibility of positive noumena. First, with respect to the use of the word "object" vis-à-vis the features of mind-dependent reality, this is perhaps inappropriate as to call something an "object" is to suggest it exists objectively, meaning in the absence of mind-dependence. As all things within the mind are ascribed a value by the mind itself, nothing simply exists therein, and therefore may be better referred to as "artifacts."

Second, in specifying "appearances" and "phenomena" as related but discreet features, Kant is imposing a view of external reality upon the mind. While, surely there are discreet sensory inputs in the form of appearances, once present within the mind they inform a cognitive process that results in the formulation of phenomena, which then itself informs continued cognition, etc. Therefore, it is probably more appropriate to conceive of things in mind-dependent reality as a concentration point of a thought process, as internally no specific idea will be divorced from the cognitive process that created it, nor that which follows it.

Third, with respect to the non-perceptibility of positive noumena, Kant is suggesting that external objects must be perceived through the senses alone, and therefore the non-sensible is imperceptible, but what of ideas? Internally, once one reaches a point in a thought process sufficiently concentrated for outward expression, is that not the point where a distinguishable idea has been formed? Does the intuition of the idea not bring the idea into existence? From the point of view of the thinker this does seem to be a positive noumena, if not at least function like one. Furthermore, once an idea is expressed externally—read: placed within mind-independent reality—a third party observer may via their senses engage with it, but only to the extent that the idea has been properly expressed and with no access to the idea itself. However, this idea is certainly not a physical object,

[33] Stang.

and so cannot be described as a "noumena" in Kantian terms, even though it functions in a similar manner. Therefore, mind-dependent artifacts may be understood as "nousmena," drawing on the "nous-" prefix from the Greek meaning "mind" or "intellect."[34] As your eyes read these words and interpret the presented meaning (negative nousmena), you ascribe a meaning to them based upon what you read and understand from the text (appearances), and therefore are no less limited by your senses in interpreting them than you are in recognizing the paper they are written on. From the author's perspective however, these words are the representation of an idea that has been brought into existence as a consequence of their own thought processes (positive nousmena). To the observer, the idea is a negative nousmenon, and their perception of that idea is the appearance that begins the chain of their own cognitive process; it informs their mind-dependent reality in much the same way as a mind-independent object would. Therefore, it may be stated that the perceptibility of nousmena is relative, appearing as positive to the progenitor, and negative to the consumer. This, of course, does not capture the complexity of human interaction, for the aforementioned describes a one-way exchange rather than a discourse. After the requisite volume of discursive exchange existential consensus is developed as individuals compare their own positive nousmena with the negative nousmena produced by their discursive partners. It can be said that their shared reality has been socially constructed via the repetitive exchange of ideated nousmena, thus connecting formerly isolated mind-dependent realities into a multi-mind-dependent reality: a reality dependent not on one mind alone, but on a multitude. As a multi-mind-dependent reality is dependent upon a collection of minds, its evaporation would require the elimination of all minds involved, and given a large enough population the loss of one mind would likely be irrelevant. Therefore, while a multi-mind-dependent reality is comprised by minds, it can exist and persist independently of any particular lone mind within that composition, and therefore is lone-mind-independent.

[34] Britannica, "Nous," Britannica.com, accessed January 29, 2022, https://www.britannica.com/topic/nous.

3. Space

If reality is the notion of a context within which things exist, then naturally this would suggest that reality is subject to some kind of boundary or set of limitations. Anything that would fall outside of that theoretical boundary would be unreal by virtue of its acontextuality. When referencing space, one is considering such a boundary's interior separately from any extant thing that the boundary contains, and is therefore answering the question 'where *could* things exist' rather than 'where *do* things exist.' Thus, if reality is the notion of a context within which things *do* exist, space is the notion of a context within which things *could* exist as restrained by the boundary that reality provides.

In the mind-independent reality, which humans perceives as physical space, our collective knowledge of the boundary of reality is represented by the extent to which humanity has been able to investigate them, or sense them in Kantian terms. As humanity has engaged in scientific inquiry and has extended the reach of its senses through the use of technology, it has developed physical laws to describe as best as possible what could be considered the boundary of reality; or at least the boundary of reality as far as is known. It is upon the basis of this knowledge that humanity interacts with its environment, and this holds true irrespective of how formalized that knowledge has been made. For instance, prior to articulating the notion of gravity, humanity had managed to intuit that falling from a great height should generally be considered to be a bad idea. However, once such a notion was formalized as the law of gravity, the foundation was laid for the development of rocketry. While physical laws restrain our activity within physical space, increasing knowledge of the physical laws permits us to expand our activities therein.

In a mind-dependent reality, space functions in much the same way insofar as it describes the potential for the presence and concentration of thought. However, what distinguishes space in a mind-dependent reality from mind-independent reality is the absence of negative space, and how human beings conceive of their ability to exercise will therein. As to the first, in physical space we perceive discreet things and negative space between them, or a space that could have an extant thing therein, but does not at the moment (e.g., the space between Earth and Mars). Within the mind, there is no moment where

cognitive processing ceases as long as a conscious being remains conscious, and therefore no negative space between thoughts.

Certainly, one could conceive a perceived distance between concentrations of thought but as thought is an ongoing process, that perceived distance is filled with conscious and unconscious notions that draw a mind from one thought to the next. As to the second, because each new concentration of thought is the result of a process, one may not know said result prior to pursuing a line of reasoning. Therefore, unlike physical space where one may be simultaneously aware of point A and point B and subsequently traverse the distance between them, within the mind one may be aware of point A, and can choose a direction to travel (e.g., searching for the answer to a specific question), but cannot know what point B is or how to get there until they have already arrived.

However, within a multi-mind-dependent reality, mind-dependency begins to appear much less limiting due to the notion of lone-mind-independence. Because of that independence one may begin to act within space in a multi-mind-dependent reality in a similar manner as they do in physical space as engagement in a multi-mind-dependent reality is predicated on the interpretation of the appearances of negative nousmena produced by others, in much the same way as interacting with physical space is predicated upon sensory interaction with negative noumena. Just as places and things are concentrations of noumena in physical space, so too are places and things in a multi-mind-dependent reality concentrations of nousmena. Dust coalescing into planets and opinions coalescing into consensus may not be so different. For example, imagine a conversation involving three people. Two are arguing and one is a neutral third party. After listening for a while, the third party *takes a side*. Meaning they position themselves within the discursive space at a *place*. Furthermore, they can *choose* to do so because they now have a mind-dependent point b that could not exist within one mind alone. Now expand the analogy to a discursive exchange among *billions*. With that kind of rich exchange, it should be no surprise that being “on” the internet, going “to” Facebook, or leaving a comment “in” a reddit thread makes sense intuitively. From a technical perspective the internet is simply a mediated exchange of ideated nousmena, thereby facilitating the creation of a multi-mind-dependent reality: Cyberspace.

C. WHAT IS CYBERSPACE?: THE CAVE WE BUILT

> SOCRATES: Imagine this: People live under the earth in a cave like dwelling. Stretching a long way up toward the daylight is its entrance, toward which the entire cave is gathered. The people have been in this dwelling since childhood, shackled by the legs and neck. Thus they stay in the same place so that there is only one thing for them to look at: whatever they encounter in front of their faces. ... From the beginning people like this have never managed ... to see anything besides the shadows that are projected on the wall opposite them by the glow of the fire. ... Now if they were able to say something about what they saw and to talk it over, do you not think that they would regard that which they saw on the wall as beings?
>
> GLAUCON: They would have to.[35]

It can be generally stated that within a mind-independent reality existence begets knowledge.[36]

In The Allegory of the Cave, Plato, speaking through Socrates, outlines abstractly the process and consequences of building knowledge, moving from a superficial understanding of a thing gleaned via the shadows it creates to a more complete understanding provided by direct observation. Importantly, however, prior to direct observation, prisoners within the cave have no direct insight into the shadow casting object; they do not know it exists, and so their understanding and worldview is informed solely by shadows. One can imagine them sharing their viewpoints on different shadows; crafting narratives around their perceived movement and actions; describing where they are in the cave, how and why they interact. To them these shadow actors and spaces exist within a mind-dependent reality; and so for the prisoner, knowledge begets existence.[37]

Cyberspace and the Plato's cave are akin, and human actors exist in some form both within and without. Human actors existing in physical space; their ideas, actions, and motivations; are themselves the shadow casting objects. While they cannot enter the cave

---

[35] Plato, "The Allegory of the Cave," in *Republic, VIi 514 a, 2 to 517. Translated by Thomas Sheehan*, accessed October 8, 2021, https://web.stanford.edu/class/ihum40/cave.pdf.

[36] Robert Lehe, "Realism and Reality," *Journal of Philosophical Research* 23 (January 1, 1998): 219–37, https://doi.org/10.5840/jpr_1998_19.

[37] F. Allan Hanson, "Models and Social Reality: An Alternative to Caws," *American Anthropologist* 78, no. 2 (1976): 323–25.

directly, they can certainly contribute silhouettes of themselves to the cave walls. While humanity is firmly rooted within physical space, when reading the cyberspatial cave walls and considering how concepts interact with those contributed by others, individuals find themselves firmly in the role of prisoner, restricted solely to interpreting the totality of those contributions in the absence of direct physical interaction. Just as Plato's cave prisoners are forced to look directly at the cave wall, so too are we digitally constrained, limited to interacting with online content by our devices. Shackled though humans may be, unlike Plato's prisoners, individuals interacting with cyberspace are aware that external physical inputs are casting shadows; that there is a mind-independent reality outside of the cave, though they may not be aware of exactly what those physical inputs are. Cyberspace serves as a means for humans to explore and operationalize knowledge in a space without disregarding physical space entirely.

1. Cyberspace as a Domain

The definition of "Domain" provided by Merriam-Webster is sub-divided into 10 parts, 7 of which are specific to particular topic areas such as law, mathematics, biology, etc.[38] The remaining three are as follows: (1) "a territory over which dominion ... is exercised," (2) "a region distinctively marked by some physical feature," and (3) "a sphere ... of knowledge, influence, or activity."[39] Of these, definition 2 is closest to what is inferred when discussing the more traditional domains of land, sea, air and space. All three however, are relevant when classifying cyberspace as a domain.

The first definition, "a territory over which dominion is exercised," applies both lexically and practically. The word "cyberspace" is derived from "cybernetics," which was coined in 1948 by Norbet Wiener and refers to the "theory or study of communications and control."[40] William Gibson took the "cyber-" prefix, and coined "cyberspace" in 1984, describing it as "a consensual hallucination experienced daily by billions of legitimate

[38] Merriam-Webster, "Definition of DOMAIN," accessed December 7, 2021, https://www.merriam-webster.com/dictionary/domain.

[39] Merriam-Webster.

[40] Online Etymology Dictionary, "Cyber-." The term cybernetics and may be based upon the 1830s French term *cybernétique*, or "the art of governing."

operators," effectively describing the multi-mind-dependent reality that cyberspace remains.[41] The common thread between cybernetics and cyberspace is "cyber-" which denotes a kind of governance or control, and hence dominion over the space it's attached to. Cyberspace's existence is made possible by both technical infrastructure and the active participation of human beings. Therefore, while no one entity exercises dominion over cyberspace entirely, it can be classified as a domain in this sense as it is subject to the dominion of decentralized participants.

The second definition, "a region distinctively marked by some physical feature," applies, though metaphorically given cyberspace is mind-dependent and hence has no physical properties. The "physical" feature is contained within technology that supports it. It should be emphasized here that 'technology' as referenced here is not solely the internet, but rather the totality of technology supporting cyberspace to include portions that may be separated from a cohesive whole. As a point of comparison consider the land domain. When discussing 'land,' what is being referenced is *any* land whether or not it is contiguous. It includes continents, islands, peninsulas, mountains, and anything else that exists as solid ground. Similarly, cyberspace includes activity on the global internet, but also includes isolated intranets, systems, and devices that may be disconnected and air-gapped from the internet itself.[42]

The third definition, "a sphere of knowledge, influence, or activity," applies due to its mind-dependent composition. Cyberspace is quite literally "of knowledge, influence, or activity" given that it is comprised of the coalesced contributions of participant minds. "Sphere" as it is invoked within this definition is meant to refer to "an area or range over or within which someone or something acts, exists, or has influence or significance."[43]

---

[41] Gibson, *Neuromancer*, 51.

[42] In actuality, it may be better to classify cyberspace as a meta-domain, or a domain of domains, rather than as a domain alone, as it is comprised of various distinct "regions" that need to be considered in their own right. The distinction between the traditional internet and web 3.0 technologies that enable activity on blockchains exclusively is a top-of-mind example. However, as domain is invoked herein to describe domains within mind-independent reality, breaking out cyberspace's sub-domains specifically would be inappropriate.

[43] Merriam-Webster, "Definition of SPHERE," accessed December 7, 2021, https://www.merriam-webster.com/dictionary/sphere.

Describing cyberspace as an area or range over and within which knowledge, influence, and activity acts, exists, and has influence and significance would be rather literal.

2. Cyberspace Is

When discussing "cyberspace" herein, I am specifically referring to a domain comprised of a multi-mind-dependent reality that is supported by advanced communication technology. Specifying technology here is important because, arguably, a kind of proto-cyberspace has been existence since long before the first computer was ever conceptualized. Consider the popular social media site Facebook. Via this website I could conceivably reach out to a colleague in Europe for advice, and it could be said that we would be communicating within cyberspace. This would be true whether that colleague could be bothered to respond within 3 seconds or 3 months. Either way we would both perceive ourselves as participating within a mutual discursive environment. This would also be true if, instead of using Facebook, I simply hired a courier to carry a letter over the Atlantic and place it in my colleague's hand directly. Advanced communications technologies have enabled more minds to share the same multi-mind-dependent reality, and contracted space and time to such an extent that that shared multi-mind-dependent reality is able to persist far more consistently and expansively than was previously possible. The space that has been "contracted" is physical space, meaning the physical distance between participants is increasingly less relevant as technology enables participation around the globe. However, by virtue of creating a technological framework to support that participation, the technology allows for negative space (e.g., unused bandwidth or storage) which is abnormal as that cannot normally exist within mind/multi-mind-dependent realities. Thus, while physical space has "contracted," cyberspace expands as the technology that underlies it evolves and allows greater participation, or space for potential participation therein.

The allowance for negative space is representative of a critical component of the technology that underlies cyberspace: it enables the persistence of a lone-mind-independent large scale multi-mind-independent reality. As discussed previously, multi-mind-independent realities are lone-mind-independent, meaning that if one participant

mind departs the reality remains. Therein, reality starts to look a bit more like mind-independent reality, as the notion of place is rendered possible through discourse. Without assistance however, this is the extent to which mind-dependent reality can be made independent. Technology provides a means to further enhance independency by creating frameworks that facilitate discursive exchange, thereby allowing that exchange to persist in a form that is structured similarly to mind-independent reality. A library, for example, is a type of physical structure used to store and order ideas. Therein, ideas and debates are printed on leaves; bound within books; stored on shelves; ordered in rows; and divided into sections in broad categories that are representative of the structure of the discourse that generated them. It emphasizes lone-mind-independence by providing a physical structure within which to store negative nousmena, thereby establishing a foundation upon which that reality may be built and persist over time. The technology that underlies cyberspace serves the same purpose but with differences in structure and speed. A library is primarily mind-independent, meaning that one literally needs to account for the capacity for individuals to walk up to a shelf, pick up books, and sit at desks to read them. Access to discourse is limited by the literal physical activity used to do so. Cyberspace by contrast is physically accessible by means that are essentially frictionless, and once accessed there are no physical limitations that dictate how information is organized. It is the equivalent of building a library without the need to account for how shelves and books are organized, and instead letting discursive structure dictate that internal organization more directly. Furthermore, information exchanged therein can occur at a such a rate that that organization and content can be modified in real time. Whereas in a physical library, a book one picks up is representative of ideas that were formulated at some time in the past, in cyberspace one may engage with ideas *as they are created*, thereby facilitating a persistent multi-mind-dependent reality. Cyberspace is still structured to some degree in a manner that echoes physical space by virtue of the fact that those participating in it are accustomed to engaging with mind-independent phenomena. Arguably, this is the true purpose of the underlying technology: to cause multi-mind-dependent reality to take a shape that relies upon familiar structures derived from mind-independent reality to both sustain cyberspace and render it navigable and useful.

III. CONSIDERATIONS WHEN INTERACTING WITH CYBERSPACE

> Thus when the supreme being formed the universe, and created matter out of nothing, he impressed certain principles upon that matter, from which it can never depart, and without which it would cease to be. When he put that matter into motion, he established certain laws of motion, to which all moveable bodies must conform. And, to descend from the greatest operations to the smallest, when a workman forms a clock, or other piece of mechanism, he establishes at his own pleasure certain arbitrary laws for it's [sic] direction; as that the hand shall describe a given space in a given time; to which law as long as the work conforms, so long it continues in perfection, and answers the end of it's [sic] formation.[44]

The true nature of cyberspace is the confluence of technology and the mind. It is a domain unlike land, sea, air, and space insofar as its existence is predicated upon human involvement. Given a hypothetical mass extinction, code, logs of conversations, and physical infrastructure might remain; but absent participant minds capable of coalescing things in cyberspace cannot exist. All that would remain is the technical infrastructure that once supported it. This is a key difference between cyberspace and physical space. Whereas our collective understanding of a classical domain is predicated upon some understanding of its nature, cyberspace's nature is predicated upon the consensus of those acting within it. Cyberspace exists backwards, and this has some implications regarding policy development and governance.

As our starting point for identifying those implications is an understanding of what cyberspace is; of its nature, it would be prudent to consider policy documentation built upon a similar premise. The founding documents of the United States were greatly influenced by the 18th century jurisprudential commentary of Sir William Blackstone, who in his *Commentaries on the Laws of England* takes "natural law" as a premise for the development of what laws humans create for themselves.[45] For Blackstone, his

---

[44] William Blackstone, *The Project Gutenberg EBook of Commentaries on the Laws of England, by William Blackstone (Originally Published 1765)* (Project Gutenberg, 2009), https://www.gutenberg.org/files/30802/30802-h/30802-h.htm#Page_38.

[45] Blackstone; Albert Alschuler, "Rediscovering Blackstone," *University of Pennsylvania Law Review* 145, no. 1 (November 1, 1996): 1.

interpretation of natural law was a combination of physical law, as we understand it today, as well as God given "immutable laws of human nature, whereby that [man's] freewill is in some degree regulated and restrained."[46] For the purposes of this document, the focus is on the former, in that it seeks to identify policy considerations given cyberspace's intrinsic makeup. Therefore, consideration of how the United States' founding documents reflect consideration of physical reality may illuminate points of consideration regarding cyberspace. To that end, excerpts of the Declaration of Independence and the U.S. Constitution are considered.

There are three key considerations that need to be accounted for when engaging in policy development and governance related to cyberspace: (1) the mutability of cyberspace, (2) the composition of things in cyberspace, and (3) the nature of trans-spatial activity. The first two of these deal with features of cyberspace that are alien to physical space insofar as they represent issues that do not need to be accounted for when considering physical space alone. The third has to do with dealing with the implications of the intersection between physical space and cyberspace.

A. THE MUTABILITY OF CYBERSPACE

> When in the course of human events, it becomes necessary for one people to dissolve the political bands which have connected them with another, and to assume among the powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a descent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation[47]

The opening statement of the Declaration of Independence asserts the primacy of the Laws of Nature in Blackstonian terms. As the founders understood them, the laws of nature are absolute and unimpeachable insofar as what they prescribe is immutable, and while men may both establish and dissolve political bands, these choices are ultimately and irrevocably bounded. Setting aside that their formulation is predicated upon a particular

---

[46] Blackstone, *The Project Gutenberg EBook of Commentaries on the Laws of England, by William Blackstone (Originally Published 1765)*, 39.

[47] "Declaration of Independence: A Transcription," National Archives, November 1, 2015, https://www.archives.gov/founding-docs/declaration-transcript.

religious perspective, the premise is that there is a set of inviolable laws that must dictate behavior. Therefore, all policy and jurisprudence must conform to these laws as well. However, beyond such grandiose statements there is little in the founding documents invoking that immutability in narrow terms. There is simply no need to append statements with the boiler plate caveat "as long as the laws of gravity and motion persist."

Humanity lacks the same convenience of the immutability, or perceived immutability, of physical space that permitted the invocation of "natural law" absent the aforementioned caveat when considering cyberspace. Here the *perception* of immutability is emphasized because, as noted previously, physical laws are simply success statements for what humanity understands to be absolute thus far. When a law is disproven, the presumption is that humanity was simply mistaken, rather than a change through divine intervention.

As cyberspace is humanity's creation, it can change. It is mutable. It therefore falls to humanity to be specific enough to account for its evolution, and therefore account for both its impermanence and fallibility. Impermanence is relevant because one may not craft a policy regarding cyberspace based solely on physical or present cyberspatial realities with the practical expectation that these policies will remain relevant in the long term. Consider the physical example of highway speed limits. Such limitations were initially put in place due to concerns over limited fuel supplies, and then later applied or modified based upon balancing the risks to drivers and passengers with public preferences.[48] Those writing the laws had no expectation that (a) the availability of oil could at some point become unlimited, or (b) that a human being could be immune to the ill effects of decelerating from 100 mph to 0 mph in the space of a second. While technology might evolve to make these facts less relevant, the questions of flammability and vulnerability were never questions, but constants.

In cyberspace there can be no similar assumptions, as technological advancements could modify cyberspatial conditions in such a way as to alter the very the rules that govern

[48] American Safety Council, "The History of Speed Limits in America: A Nation Speeding Up," accessed January 8, 2022, https://blog.americansafetycouncil.com/the-history-of-speed-limits-in-america/.

the behavior of things therein. A recent example of something like this occurring was the 2021 end of life of Adobe Flash Player. This technology, which was first released in 1996 as Macromedia Flash, and was widely used for adding graphics to websites, enabling casual game play, and advertising.[49] However, as it more generally became a means by which users could customize how others interact with content, it was applied in a variety of applications, including the Dalian Train Operation Depot's browsers in northeast China.[50] After flash reached its end of life, on January 12, 2021 the Dalian Train Operation Depot's browsers ceased to function properly, and continued to malfunction for 20 hours until their IT staff were able to resolve the issue.[51] The environmental constants that permitted software predicated upon flash to operate changed in such a way as to render it inoperable. Consequently, any policies governing the use of that software vis-à-vis how train schedules should be handled and monitored were rendered moot not because the software changed, but because environmental constraints changed. A policy area where this could come into play in the U.S. is the notion of Net Neutrality, or "the idea that internet service providers ... should treat all content flowing through their cables and cell towers equally."[52] This philosophy generally treats cyberspace as an instrument akin to electricity, as it frames the issue in terms of data flows, and positions policy to guarantee equal access to data volumes. In the absence of Net Neutrality, the thinking is that internet service providers (ISPs) will use their privileged positions as data-stewards to prioritize access to specific content out of self-interest, thereby degrading access to parts of cyberspace that do not directly benefit them. The problem is that this policy only narrowly addresses the issue of data flows and ignores the narrow issues that Net Neutrality is intended to address: an equal opportunity to participate in on-line marketplaces and spaces. It amounts to an effort to regulate physical property, rather than behavior in cyberspace. Addressing data limitations makes

---

[49] Maria Korolov, "An Adobe Flash Ghost May Be Haunting Your Data Center," *Data Center Knowledge*, March 23, 2021, https://www.datacenterknowledge.com/security/adobe-flash-ghost-may-be-haunting-your-data-center.

[50] Lily Hay Newman, "Flash Is Dead—but Not Gone," *Wired*, accessed January 8, 2022, https://www.wired.com/story/zombie-flash-security-problems/.

[51] Newman.

[52] Klint Finley, "Net Neutrality: Here's Everything You Need To Know," *Wired*, accessed January 8, 2022, https://www.wired.com/story/guide-net-neutrality/.

sense today because ISPs are monolithic, and data volumes dictate experience. However, as the internet evolves, it is entirely plausible that the role of ISPs will change, and that the relevancy of fluctuations in data volumes will be less relevant to all involved as data becomes cheaper through modernization. Should that occur, Net Neutrality will be rendered a moot point, and people will be left with few protections that ensure equity of access. This is not to suggest that regulating infrastructure is entirely futile, for the way in which data coalesces into things in cyberspace is predicated upon the technology that allows it to do so. Should the underlying technical limitations change, implicitly the pathways that allow multiple minds to connect will also change. However, such policy can only be short term, given the mutability of cyberspace.

Cyberspace evolves as a consequence of human actors. Programs, algorithm, and code written by individuals coalesce into spaces, actions, and entities. No matter whether a single coder alone or a collection of individuals, the generation of all these determinative commands and conditions inevitably results in gaps and loopholes. As systems become increasingly complex, they become inherently less predictable. This is a fundamental challenge for policy makers as this evolution is, to a point, beyond the control of even the most adept practitioners in the space. It is unpredictable, and unforeseen consequences of this growth will generate errors or bugs. Some of these are benign, or even useful, as the adage "it's not a bug, it's a feature" would suggest.[53] However, on the dark side of this spectrum exists the "zero-day exploit," or an "unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong."[54] A famous example of a zero-day exploit driven attack was Stuxnet, "a computer worm exploiting as many as four Zero-Day vulnerabilities" to target an Iranian nuclear facility.[55]

---

[53] Nicholas Carr, "'It's Not a Bug, It's a Feature.' Trite—or Just Right?," *Wired*, accessed January 8, 2022, https://www.wired.com/story/its-not-a-bug-its-a-feature/.

[54] FireEye, "What Is a Zero-Day Exploit?," FireEye.com, accessed January 8, 2022, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html.

[55] Arik Hesseldahl, "Here's What Helped Sony's Hackers Break In: Zero-Day Vulnerability," Vox, January 20, 2015, https://www.vox.com/2015/1/20/11557888/heres-what-helped-sonys-hackers-break-in-zero-day-vulnerability.

With respect to the mutability of cyberspace, the main takeaway is twofold. First, because one cannot rely upon the environment remaining constant, one cannot develop policy predicated upon its ontology and expect it to have the same impact as it would in physical space in the long term. Consequently, it may be required to more explicitly formulate policy in manner that expresses desired intent rather than solely restricting behavior. Considering the Net Neutrality example, preventing abuse by ISPs is important, but will likely require the additional step of providing explicit requirements banning activities that broadly prevent individuals from accessing markets. This requirement will likely make policy negotiations more difficult. At present, two parties who disagree on a desired outcome can identify a middle ground where they both agree on a set of policy prescriptions because it meets the needs of both parties, even if the negotiating parties' respective ends differ. Policy for cyberspace that will be resilient in the long term will need to have the intended ends of that policy expressed explicitly, which may leave less room for agreement. Secondly, policymakers must also operate in an environment where the totality of constraints is unknowable. While this may also be true in physical space, what physical laws are waiting to be discovered are not likely to impact the day-to-day life of the average person. In cyberspace, the rules can change in a way that does, and without warning.

B. THE COMPOSITION AND NATURE OF THINGS IN CYBERSPACE

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[56]

The Constitution's fourth amendment discusses physical objects in terms of ownership, emphasizing the need to specify things, spaces, and persons for the state to execute a seizure. While other components of the document reference specific things, the fourth amendment is somewhat unique in that it covers the handling of objects generally,

56 "Constitution of the United States," accessed January 10, 2022, https://www.senate.gov/civics/constitution_item/constitution.htm#amendments.

and so is a useful touchpoint when consider how to cope with cyberspatial equivalents from a policy perspective. In contemplating the notion of a seizure, what this language suggests is the forceable acquisition of another's property; the literal taking of an object, or holding of a person. In physical space holding and containing a single object is a simple task, but in cyberspace this is not always the case; and in some cases cannot be done at all except under some specific conditions.

First, data may coalesce into a single object solely by virtue of that data being conceptually proximate, meaning that a single "thing" in cyberspace may be comprised of data that is not collocated within a single location on a network or device. For example, if one has a copy of Microsoft Excel on their device, that single piece of software is not "single" at all, but rather comprised of many files. If one wished to uninstall it, that would require running a different program so as to ensure all its component parts are eliminated in the process. Even a user on their own device often cannot "seize" software without assistance. Furthermore, even the Excel files themselves, meaning saved documents, are not "single" files, although they appear so to the user. If the ".xlsx" extension on an excel file is changed to ".zip," the file will change to reveal its true form: yet another folder filled with subfolders and files that comprise the so-called single document. With the advent of cloud computing, these files may be distributed not across a single device, but across multiple devices and platforms around the globe. Consequently, when discussing the seizure of a things in cyberspace, one must account not just for the target artifact, but all of its component parts, which at times will simply be impractical. Second, when holding a thing, there may be a need beyond to just to have possession of a thing, but also to deny others possession of it, say in the case of the state trying to restrict access to a particularly dangerous weapon, or a private company placing protections on its intellectual property. This too can be difficult to execute due to the ease with which things in cyberspace may be duplicated. Being comprised of data, duplication of a thing in cyberspace only requires the duplication of the arrangement of data so as to create a copy. This takes all of four clicks to accomplish in most cases: Ctrl+C, Ctrl+V. The near equivalent in physical space would be the duplication of a physical object by mapping out an object's entire atomic structure and rebuilding it atom by atom so as to instantaneously create a perfect duplicate. Data

does not physically exist, or rather the meaning behind it doesn't. It is in some sense the meaning behind the subtle physical differences within devices that "hold" it. As it is simply information, when duplicating a thing in cyberspace one may literally create a copy that is indistinguishable, because as long as the data's meaning between the original and the copy are consistent, there is no discernable difference between them. This ability to create perfect duplicates points to something unique about the nature of things in cyberspace, namely that they are intrinsically non-unique by definition, whereas physical objects are intrinsically unique. This feature makes sense given that cyberspace is a multi-mind dependent reality, for just as two minds can consider a single idea, so too can two files document it, to include the construction of it. This is an example of two containers containing a single thing: the meaning and value of the idea itself. There are budding technical efforts to attempt to achieve uniqueness in cyberspace, though this is done through trickery. Non-fungible tokens (NFTs) are a type of technology used to create "unique" items, by documenting ownership.[57] A thing is tokenized, and is essentially assigned a kind of serial number, and that serial number is assigned to a single owner or "wallet." When that specific artifact changes hands, that transaction is documented on an immutable ledger, or decentralized ledger meant for recording such transactions. "Uniqueness" is achieved not by actually creating an unduplicable idea, but rather by recording provenance.

Although mere trickery, NFTs still have some pretty stunning implications vis-à-vis cyberspace depending upon how they are employed. In particular, they make things in cyberspace unique and seizeable. Normally a thing in cyberspace can be duplicated one or one hundred times. In serializing things, one may now identify who owns that single thing irrespective of who or how many possess it. Taking the more complicated notion of what constitutes a "person" in cyberspace, and in consideration of the notion of seizing one as per the 4th amendment of the U.S. Constitution, it would be a simple matter to tokenize a physical person's idea of themselves, and then attribute or predicate their online activity to their personal NFT. Should that occur, it would be possible then be possible seize a

[57] Ethereum.org, "Non-Fungible Tokens (NFT)," Ethereum.org, accessed January 11, 2022, https://ethereum.org.

"person" by seizing their NFT, which today is not possible because an identity in cyberspace is a confluence of personal activity in the absence of any centralized touch point.

While it is difficult to truly seize and restrict access to a thing in cyberspace, particularly one that has been duplicated or whose component parts are widely distributed, it is not completely impossible. Ransomware is "a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable."[58] While this does work to lock up things in cyberspace, it does so not by targeting the things themselves, but rather the spaces they occupy. It is simply easier to lockdown an entire network and extort the owners of that space rather than surgically target and seize artifacts of unique value under the assumption that those artifacts have not been duplicated. Consequently, while seizure is possible, it often requires casting a much wider net than would be required in physical space.

C. THE NATURE OF TRANS-SPATIAL ACTIVITY

> [The Congress shall have Power…] To regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes.[59]

The Commerce Clause of the U.S. Constitution grants congress the power to regulate interstate commerce. This is not purely monetary, but "covers every species of movement of persons and things, whether for profit or not, across state lines, every species of communication, every species of transmission of intelligence, ... every species of commercial negotiation that will involve sooner or later an act of transportation of persons or things, or the flow of services or power, across state lines."[60] This notion of movement of things and value across state lines was critical to place within the U.S. constitution as the federal government was tasked with mediating the transfer of goods and services

[58] CISA, "Stop Ransomware," CISA, accessed January 11, 2022, https://www.cisa.gov/stopransomware.

[59] "Commerce Among the Several States," Legal Information Institute, accessed January 14, 2022, https://www.law.cornell.edu/constitution-conan/article-1/section-8/clause-3/commerce-among-the-several-states.

[60] Legal Information Institute.

between each of the newly established states. As each state had its own unique regulatory environment, establishing a kind of mediating framework allowed the federal government to smooth that process of exchange. Fundamentally, the commerce clause is a starting point for coping with a policy context that is subdivided into environments with distinct legal frameworks coexisting and interacting, which is exactly the type of challenge posed by the need to manage the realities of physical space and cyberspace simultaneously. Physical space and cyberspace both exist and interact with one another, and this interaction has consequences in both spaces. While the laws governing each space are not regulations per se, they do comprise the abstract rules of what is or is not possible therein. Therefore, as with interstate commerce, there is a need to understand trans-spatial activity, meaning activity that occurs both within and between physical space and cyberspace.

"Activity" in cyberspace boils down to information exchange. As a constructed space, the information that resides therein has been input by physical entities acting upon it, has been passively collected from physical space via environmental data collection, or is the result of an analysis of data that has been input or collected. Similarly, this information can act upon physical space via directly controlling the physical behavior of objects that rely upon it, as in the case of self-driving vehicles moving in physical space as dictated by code; or by influencing the behavior of persons consuming content therein, as in the case of on-line radicalization influencing a terrorist attack. These activities may be broken down into four categories of trans-spatial activity, two intraspatial and two interspatial, and are as follows:

Physical space to Physical space (P→P): P→P Includes intraspatial activity where a physical cause has a physical effect. While this only includes purely physical activity, this is included in this analysis as physical activity can be an indirect consequence of a chain of events begun in cyberspace, as well as part of a physical chain of events that ultimately affects cyberspace. For example, as these words are written, fingers are depressing keys on a keyboard.

Physical space to Cyberspace (P→C): P→C Includes interspatial activity where a physical cause has an effect in cyberspace. Any activity that involves the digitization of information qualifies as an P→C event. This includes direct data entry, as well as passive

collection mechanisms like environmental sensors and audiovisual recording devices. For example, as keys on a keyboard are depressed, that physical action is transformed into data.

Cyberspace to Cyberspace (C→C): C→C Includes intraspatial activity where a cause in cyberspace has an effect in cyberspace. For example, data is transmitted from a keyboard to a digital document, thereby placing letters and words on a digital page.

Cyberspace to Physical space (C→P): C→P Includes interspatial activity where a cause in cyberspace has a physical effect. For example. Once this document is completed, it will be printed. After the C→C activity of sending data to a printer, that printer will print the document; a physical representation of the data held within cyberspace.

Once isolated, each trans-spatial activity within a chain of events may be consolidated into an *Activity Chain* (AC) so as to diagram a sequence of events. For example, a full AC of the writing example outlined in the trans-spatial activity breakdown above would include the act of typing (P→P), transformation of key presses into data (P→C), transmission of data to a document (C→C), transmission of data to a printer (C→C), and the final printing of a document (C→P). This may be consciously diagramed as P→P→C→C→C→P.

An assessment of the impacts of trans-spatial activity requires an understanding of the information crossing between and within spaces. However, such an appraisal can only be completed in all cases within cyberspace. Once a C→P action has occurred, the value of a thing in cyberspace may only be assessed via physical means if that action has taken place in such a way as to make that possible. In the example above, the value of a printed document is readily accessible because it can be read. If the document were instead saved to a physical device rather than printed, the only way to determine the contents of that device is connecting to a device that would allow for the appraisal to occur. Furthermore, once a physical device contains a thing in cyberspace of a certain value, that device becomes equally valuable even though it is physically indistinguishable from a duplicate device that contains no data at all.

To this point, this thesis has argued that: (a) cyberspace is a domain comprised of a multi-mind-dependent reality that is supported by advanced communication technology;

(b) that reality is mutable; (c) things in cyberspace are composed of data that may or may not be physically collocated, and both those things and their component parts are more easily duplicable than things in physical space; and (d) causes in cyberspace may have effects in physical space and vice-versa. Taking these features into consideration is necessary to properly inform policy as it relates to cyberspace.

IV. PRESIDENTIAL APPROACHES TO CYBERSECURITY

A. INTRODUCTION

Armed with a better understanding of what cyberspace is, attention may now be turned to assessing whether policy that semantically treats cyberspace as a space or domain does so substantively. To do so, the approaches to cybersecurity of subsequent U.S. presidential administrations, from President Clinton through President Biden, are considered. President Clinton's presidency has been chosen as a starting point for this assessment due to the unique changes cyberspace and the public's use of technology underwent during his tenure. While there were networked systems, and by extension cyberspace, well before President Clinton took office, it was during his tenure that household adoption of personal computers and the internet began to increase dramatically according to the U.S. Census Bureau.[61] In 1993 the percentage of households with a computer was approximately 21%, increasing to almost 60% by 2001, and those with internet access increased from approximately 19% in 1997, to over 50% in 2001.[62]

As to the particular topic area: cybersecurity, this subject has been selected specifically because it centers on how best to cope with the implications of networked systems and cyberspace, where that subject is of central importance. Other topic areas may be equally worthy of analysis, but in this case there is a preference for focusing on a subject that treats the role of the internet and cyberspace as primary, rather than as an external complicating feature. For example, in Clinton's July 1, 1997 remarks announcing the Electronic Commerce Initiative, he spoke at length regarding the implications of the growing internet, noting that "we cannot imagine exactly what the 21st century will look like, but we know that its science and technology and its unprecedented fusions of cultures and economies will be shaped in large measure by the Internet."[63] During this commentary, Clinton indicated he would be

---

[61] US Census Bureau, "Computer and Internet Use in the United States: 2016," Census.gov, accessed February 6, 2022, https://www.census.gov/library/publications/2018/acs/acs-39.html.

[62] Bureau, 2.

[63] Clinton, "Public Papers of the Presidents of the United States: William J. Clinton (1997, Book II) - Remarks Announcing the Electronic Commerce Initiative."

directing his Ambassador of Trade "to work with the WTO ... to turn the Internet into a free-trade zone."[64] This statement would appear to be an example of Clinton treating cyberspace spatially rather than instrumentally, and therefore make the topic of commerce a worthy subject of analysis. However, such an examination would effectively focus more on the extent to which the advent of cyberspace has modified commerce, rather than narrowly focus on cyberspace directly. As the objective of this writing is that narrow focus, cybersecurity simply makes more sense. This analysis is done with an eye toward determining (a) whether cyberspace has explicitly or implicitly been described as a domain within presidential administrative policy, and (b) whether that policy has actually treated cyberspace as a domain.

B. CLINTON ADMINISTRATION: ESTABLISHING A BASELINE

In January 2000 the Clinton administration issued its National Plan for Information Systems Protection (NPISP), which outlined 10 programs the administration recommended with the objective of "ensur [ing] any interruption or manipulation of [critical information systems] must be brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States."[65] It was produced following the issuance of Presidential Directive 63 (PD-63) in 1998, which categorized threats to critical infrastructure, emphasized that both physical and cyber threats need to be accounted for, and called for the development of a plan to defend against cyber threats.[66] PD-63 is "the Clinton administration's most comprehensive document on the issue of cybersecurity," insofar as it outlines the bureaucratic infrastructure necessary to address cybersecurity issues within the context of critical infrastructure protection.[67] The NPISP by contrast narrowly outlines considerations for coping with the complexities of cyberspace in isolation, and therefore provides a more clear reflection of the administration viewed cyberspace at the time.

---

[64] Clinton.

[65] Moteff, "Critical Infrastructures."

[66] Boys, "The Clinton Administration's Development and Implementation of Cybersecurity Strategy (1993–2001)," 762; The White House, "Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0: An Invitation to a Dialogue" (United States. White House Office, 2000), iii, https://www.hsdl.org/?abstract&did=1575; Moteff, "Critical Infrastructures."

[67] Boys, "The Clinton Administration's Development and Implementation of Cybersecurity Strategy (1993–2001)," 762.

Cyberspace in the NPISP is primarily discussed instrumentally, though almost exclusively through inference. The word "cyberspace" only appears in the 199 page document 13 times and, aside from the National Coordinator for Security Richard A. Clark's commentary and the executive summary, is never invoked unless the author is quoting an outside source. When it is invoked in those leading pages of the document, it is in reference to "America's cyberspace" or "our cyberspace," suggesting that the authors are conceiving of it not as wholistic space, but rather a rhetorical device to describe a national infrastructural category.[68] This does not necessarily preclude the notion of space, as similar possessive language constructions could similarly be applied to "our terrain" or "our jurisdiction," though its use herein does leave the reader with the impression that cyberspace is a thing to be protected rather than a space or domain to be operational within. However, the direct definition provided in the document's glossary gets closer to that idea as it states that cyberspace "describes the world of connected computers and the society that surrounds them. Commonly known as the INTERNET."[69] When framing the scope of the problems posed by cyberspace at the end of Chapter I, the NPSIP does so in spatial terms, noting that "[our] national intelligence capabilities can 'see' ... troops …,'sense' the launch of missiles ... and 'hear' the sound of deployed submarines [but cannot] deal the detection of cyberattack."[70] Furthermore, when invoking language from PD-63 that distinguishes between "physical and cyberattacks on our critical infrastructures," the NPISP embraces the dichotomy between threats that are physical, and threats that are something-other-than physical: cyberattacks.[71]

This, however, is where any expression of spatial considerations regarding cyberspace seems to cease. All of the planning in the NPISP seems to be oriented toward coping with a malign actor using cyberspace rather than acting within it. Of the ten programs recommended within the NPISP, the first five describe areas of focus, while the remainder outline approaches for supporting the objectives of the first five. These first five programs are (1) "Identify Critical Infrastructure Assets and Shared Interdependencies and Address

68 The White House, "Defending America's Cyberspace," v.

69 The White House, 146.

70 The White House, 9.

71 The White House, xviii.

Vulnerabilities," (2) "Detect Attacks and Unauthorized Intrusions," (3) "Develop Robust Intelligence and Law Enforcement Capabilities to Protect Critical Information Systems, Consistent with the Law," (4) "Share Attack Warnings and Information in a Timely Manner," and (5) "Create Capabilities for Response, Reconstitution, and Recovery."[72] In each of these programs, the policy objective seems to be the same: hardening local systems, while ignoring the on-line space from which attacks are actually formulated and executed. For example, the NPISP references the 1998 Solar Sunrise incident, when an Israeli teenager and two U.S. teenagers systematically targeted Department of Defense systems.[73] There is no discussion within the NPISP of how the participants in that incident were introduced, coordinated behavior, engaged in planning, or the means used to transport and store stolen data. Rather than framing the incident as occurring within a dynamic and fluid environment, it is framed as a binary conflict: interval vulnerabilities vs external threats.

The NPISP seems to account for the mutability of cyberspace, noting that "as networks change, new vulnerabilities are introduced."[74] There is, however, no apparent consideration given to the composition and nature of things in cyberspace, and the nature of trans-spatial activity. With respect to the former, because the problem has been framed as a binary competition between the state and external threats, more emphasis has been placed on preventing intrusions into "America's cyberspace" rather than getting down into the nuance of how the unique makeup of things in cyberspace might complicate cybersecurity methodologies. There is no explicit consideration of how to defend against cybersecurity threats that exploit trans-spatial activity. For example, the Solar Sunrise incident was purely a C→C operation. If an attack that followed it was instead a C→P→C operation (e.g., transportation of malicious software or sensitive information through physical space between distinct networks or network components), the approaches outlined in the NPISP would be insufficient to combat it because it conceives of cybersecurity threats as purely C→C phenomena. It therefore does not account for the potentiality of threats that may include trans-

[72] The White House, xi.

[73] The White House, xxiii,8,36.

[74] The White House, xiii.

spatial activity. Therefore, while the Clinton administration semantically described cyberspace spatially at times, it clearly approached it from an instrumental perspective.

C. BUSH ADMINISTRATION: DETERMINING RESPONSIBILITY

In 2003 the bush administration released the National Strategy to Secure Cyberspace (NSSC) which, even more so than the NPISP, treats cyberspace instrumentally.[75] The document describes cyberspace as being "an interdependent network of information technology infrastructures," and "composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work."[76] Notably absent here is the NPISP's reference to "the society that surrounds" this technical infrastructure within its own definition. Furthermore, there is almost no direct discussion of anything in cyberspace. In the entire document, the word "file" (i.e., as in a computer file) is used only once, websites are never discussed, and the worldwide web is described as "a planetary grid of systems."[77] Thus, the Bush administration's view of cyberspace as expressed in the NSSC is purely as a descriptive term for physical information technology generally, and this perspective did not seem to alter during the remainder of the Bush administration. In the January 2008 Presidential Directive 54: Cybersecurity Policy (PD-54), which led to the development of the 2008 Comprehensive National Cybersecurity Initiative (CNCI), cyberspace was defined as meaning "the interdependent network of information technology infrastructures, and includes the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries," maintaining the instrumental view.[78] What did change was the administration's perspective on the extent to which the state should centralize cybersecurity policy. The NSSC placed a special emphasis on ascribing that responsibility to end-users and organizations, framing the

---

[75] The White House, "National Strategy to Secure Cyberspace."

[76] The White House, vii.

[77] The White House, 6,8.

[78] George W. Bush, "National Security Presidential Directive 54/Homeland Security Presidential Directive 23," National Security Archive, January 2008, 3, https://nsarchive.gwu.edu/document/17291-george-bush-national-security-presidential.

challenge as one that should be addressed from the bottom up.[79] This notion was re-emphasized in the 2006 National Infrastructure Protection Plan (NIPP), but dialed back in the CNCI, possibly in response to criticism that the Bush administration lacked a unified cybersecurity strategy and that the absence of federal leadership was problematic.[80]

D. OBAMA ADMINISTRATION: TAKING RESPONSIBILITY

In 2009 the Obama Administration released a report titled *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (CPR).[81] This review was intended to assess the current state of cybersecurity policy at the time, and to provide recommendations for future policy formulation.[82] The document strongly advocates for the primacy of white house leadership regarding national cybersecurity policy, thereby emphasizing the apparent reversal that occurred near the end of the Bush administration.[83] As with previous administrations, this document discussed cyberspace with a purely instrumental view, describing it as the "globally-interconnected digital information and communications infrastructure," and additionally provides the text of the definition provided for in PD-54.[84] However, it at least infers some elements of a kind of spatial view, given repeated references in the document to operations, activity, and threats-to-be-countered "in" cyberspace.[85] This issue of defining cyberspace instrumentally while discussing it spatially continued in documentation produced throughout President Obama's tenure. In December 2016, President Obama amended Executive Order 13757 (EO 13757) in response to malign Russian interference in the 2016 presidential election, to "deal with the national emergency with respect to significant malicious cyber-enabled activities …, and in view of the increasing

---

79 The White House, "National Strategy to Secure Cyberspace," xiii; Richard J. Harknett and James A. Stever, "The New Policy World of Cybersecurity," *Public Administration Review* 71, no. 3 (2011): 456.

80 Harknett and Stever, "The New Policy World of Cybersecurity," 456.

81 The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 8, 2009."

82 Harknett and Stever, "The New Policy World of Cybersecurity," 457.

83 The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 8, 2009," v.

84 The White House, iii.

85 The White House, iii,2,8,B-1,B-5.

use of such activities to undermine democratic processes or institutions."[86] In describing Russian activity as cyber-enabled, the instrumental view of cyberspace is maintained, as cyberspace is viewed simply as a physical facilitator of activity, rather than a space within which such activity takes place.

E. TRUMP ADMINISTRATION: EMBRACING SPATIALISM

The Trump administration's approach to cyberspace was articulated in the 2018 *National Cyber Strategy of the United States* (NCS) and is far more spatially oriented than documents produced by previous administrations.[87] While the document does not provide a definition for "cyberspace," it places a special emphasis on the behaviors of individuals therein, dedicating one of its four pillars to the topic: "Pillar III: Preserve Peace through Strength."[88] This is not to suggest a total abandonment of the instrumentalist view of past administrations, as both the 2017 Executive Order 13800 (EO 13800) and the 2021 Executive Order 13984 (EO 13984) leverage the same "cyber-enabled" language used by past administrations.[89] However, the text of EO 13984 focuses not on infrastructure, but on controlling access to U.S. cloud infrastructure by malign actors, and seeks to do so by requiring "more robust record-keeping practices and user identification and verification standards within the industry."[90] While certainly past administrations advocated for credential verification and education vis-à-vis safe practices involving the same, this appears to be the first instance of a presidential strategy including such language to track and assess behavior, rather than to simply protect infrastructure from malign attacks. The text of EO 13800 is instrumentally oriented as it solely deals with infrastructure, and appears to serve

---

[86] Barack H. Obama Executive Order 13757, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," *Code of Federal Regulations*, title 3 (2017 comp.).

[87] The White House, *National Cyber Strategy of the United States of America.*

[88] The White House, 20.

[89] Donald J. Trump Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," *Code of Federal Regulations*, title 3 (2018 comp.); Donald J. Trump Executive Order 13984, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities," *Code of Federal Regulations*, title 3 (2022 comp.). The title of EO 13984 appears to be a direct duplicate of the title of President Obama's EO 13757.

[90] Trump Executive Order 13984.

more as a means for the white house to assert presidential authority rather than redefine a strategic approach. It states the President "will hold heads of executive departments and agencies accountable for managing cybersecurity risk to their enterprises," thereby further asserting control over cybersecurity issues not by the White House, but by the President himself.[91] While the Trump administration still worked within the instrumentalist framework that was established by prior administrations, it added a spatialist element to its strategic thinking regarding cybersecurity that was not previously present.

F. BIDEN ADMINISTRATION: RETURNING TO INSTRUMENTALISM

At the time of this writing, the Biden administration has not released a strategic document akin to those produced by his predecessors. What information is available comes in the form of an executive order, memorandum, and a handful of statements issued by the White House, all of which seem to reflect the instrumental view of the Clinton, Bush, and Obama administrations. The 2021 Executive Order 14028 (EO 14028) concerns "the prevention, detection, assessment, and remediation of cyber incidents;" relying upon the definition of "cyber incident" provided in the Obama administration's Presidential Policy Directive 41 (PPD-41).[92] Statements issued by the White House on October 01, 2021 and January 27, 2022 emphasize the importance of protecting critical infrastructure and sensitive information.[93] A January 19, 2022 memorandum "sets forth requirements for National Security Systems (NSS) that are equivalent to or exceed the cybersecurity requirements for Federal Information Systems set forth within Executive Order 14028."[94] While president has

---

[91] Trump Executive Order 13800.

[92] Federal Register, "Improving the Nation's Cybersecurity," Federal Register, May 17, 2021, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[93] The White House, "Statement by President Joe Biden on Cybersecurity Awareness Month," The White House, October 1, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/01/statement-by-president-joe-biden-on-cybersecurity-awareness-month/; The White House, "Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector," The White House, January 27, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/.

[94] The White House, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," The White House, January 19, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.

made public statements on the topic of disinformation on-line, the issue does not seem to have made its way into any articulated cybersecurity policy.[95]

G. CYBERSECURITY THUS FAR HAS HAD LITTLE TO DO WITH CYBERSPACE

Given that, with the exception of the Trump administration, all examined presidential administrations seemed to treat cyberspace instrumentally within their strategic policy frameworks, there is relatively little available for analysis. The impression is that cybersecurity as it has been approached thus far has little to do with cyberspace at all, but rather is narrowly focused on defending networked systems from malign actors without any regard given to the "space" that is cyberspace. This is possibly the result of two issues: abstractness and framing. With respect to the former, the notion of cyberspace as articulated in preceding chapters is highly abstract, and thus may not be easily incorporated into practical policy applications. It would be difficult to imagine consistent policy frameworks applied to a space that has been largely left undefined. As to the latter, when the Clinton administration started this conversation in the 1990s, it was focused on the threat networked systems might pose to existing physical infrastructure. Once that foundation was laid, any conversation falling under the cybersecurity heading, in building on policy thinking that came before, seemed to fall in the same mold. Given that the objectives of Clinton's NPISP, Bush's NSSC, and Obama's CPR all looked rather similar; aiming for enhancing resiliency, educating the public, safeguarding networked systems, it would appear that cybersecurity policy development was somewhat naturally constrained to those topics. The Biden administration, while not having released a full strategic document vis-à-vis cyberspace at the time of this writing, appears to be following similar instrumental lines, though there is limited information available thus far. The Trump administration's more spatial orientation is interesting, and the outlier, because it did not seem to be subject to the same constraints that restricted other

[95] Analysis by Oliver Darcy Business CNN, "Analysis: Biden Calls out Anti-Vax Liars for Promoting 'dangerous Misinformation.' But Don't Expect Anything to Change," CNN, accessed February 20, 2022, https://www.cnn.com/2021/12/21/media/biden-misinformation-reliable-sources/index.html; Zolan Kanno-Youngs and Cecilia Kang, "They're Killing People: Biden Denounces Social Media for Virus Disinformation," *The New York Times*, July 16, 2021, sec. U.S., https://www.nytimes.com/2021/07/16/us/politics/biden-facebook-social-media-covid.html.

administration's conceptualization of cybersecurity threats to infrastructure alone. There is equal emphasis placed upon managing malign behavior within cyberspace as there is upon the protection of the infrastructure that makes that behavior possible.

None of the examined administrations' policy frameworks were adequate. The mutability of cyberspace was taken into consideration in each administration's approach, because each administration at one point or another made mention of the speed with which network technology is evolving. Beyond that, however, the composition and nature of things in cyberspace, and the nature of trans-spatial activity largely goes unaddressed. The Trump administration at least conceptualizes cyberspace as a space, but that is as far as that goes. From the perspective of the U.S. presidency, cyberspace has been treated as largely irrelevant to cybersecurity. Consequently, the policy frameworks that have been produced by subsequent administrations have been structured primarily to protect technical infrastructure, with almost no accounting for potential threats posed by the reality that infrastructure supports.

V. LOOKING TOWARD THE FUTURE

Given that cybersecurity policy is so intertwined with critical infrastructure protection, it would be difficult to imagine space being created for consideration of challenges posed by cyberspace as a space unless the concept of cybersecurity is broadened to permit that discussion to take place. Until that occurs, cyberspace will, at least in policy, continue to refer solely to the physical infrastructure that supports cyberspace as described in Chapter III. This is somewhat problematic given that, at the time of this writing, challenges are manifesting that are found within cyberspace alone. The dis/misinformation issues that became starkly apparent during the 2020 presidential election have no relationship to critical infrastructure issues, aside from the fact that network infrastructure has been used to propagate these narratives. Consequently, there is no discursive space available within present cybersecurity frameworks to adequately address these concerns. While the Trump administration started going down the spatial path, that direction has not necessarily been maintained by the Biden administration. However, given that dis/misinformation issues indeed remain a point of focus and concern from a policy perspective generally, one would expect that (a) cybersecurity policy will be expanded in such a manner as to account for similar phenomena, or (b) a new and secondary policy framework will arise to address those concerns, while cybersecurity will remain fixated on physical infrastructure. Thus far however, the notion of cyberspace as a space has been applied quite superficially to cybersecurity policy, which has left the U.S. vulnerable to phenomena in cyberspace that it has yet to account for. There will be no practical impact of describing cyberspace as a domain as long as policy continues to treat cyberspace instrumentally, but the necessities of present challenges may indeed force a more spatialist approach in one way or another.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alschuler, Albert. "Rediscovering Blackstone." *University of Pennsylvania Law Review* 145, no. 1 (November 1, 1996): 1.

American Safety Council. "The History of Speed Limits in America: A Nation Speeding Up." Accessed January 8, 2022. https://blog.americansafetycouncil.com/the-history-of-speed-limits-in-america/.

Benedikt, Michael, ed. *Cyberspace: First Steps*. Cambridge, MA: MIT Press, 1991.

Blackstone, William. *The Project Gutenberg EBook of Commentaries on the Laws of England, by William Blackstone (Originally Published 1765)*. Project Gutenberg, 2009. https://www.gutenberg.org/files/30802/30802-h/30802-h.htm#Page_38.

Boys, James D. "The Clinton Administration's Development and Implementation of Cybersecurity Strategy (1993–2001)." *Intelligence and National Security* 33, no. 5 (July 29, 2018): 755–70. https://doi.org/10.1080/02684527.2018.1449369.

Britannica. "Nous." Britannica.com. Accessed January 29, 2022. https://www.britannica.com/topic/nous.

Bryant, Rebecca. "What Kind of Space Is Cyberspace?" *Minerva: An Internet Journal of Philosophy* 5 (2001): 138–55.

Bureau, U.S. Census. "Computer and Internet Use in the United States: 2016." Census.gov. Accessed February 6, 2022. https://www.census.gov/library/publications/2018/acs/acs-39.html.

Bush, George W. "National Security Presidential Directive 54/Homeland Security Presidential Directive 23." National Security Archive, January 2008. https://nsarchive.gwu.edu/document/17291-george-bush-national-security-presidential.

Business, Analysis by Oliver Darcy, CNN. "Analysis: Biden Calls out Anti-Vax Liars for Promoting 'dangerous Misinformation.' But Don't Expect Anything to Change." CNN. Accessed February 20, 2022. https://www.cnn.com/2021/12/21/media/biden-misinformation-reliable-sources/index.html.

Carr, Nicholas. "'It's Not a Bug, It's a Feature.' Trite—or Just Right?" *Wired*. Accessed January 8, 2022. https://www.wired.com/story/its-not-a-bug-its-a-feature/.

Cassini, Alejandro. "Newton and Leibniz on Non-Substantival Space." *Theoria. Revista de Teoría, Historia y Fundamentos de La Ciencia* 20, no. 1 (March 1, 2005): 25–43.

CISA. “Stop Ransomware.” CISA. Accessed January 11, 2022. https://www.cisa.gov/stopransomware.

Clinton, William J. “Public Papers of the Presidents of the United States: William J. Clinton (1997, Book II) - Remarks Announcing the Electronic Commerce Initiative,” 1997. https://www.govinfo.gov/content/pkg/PPP-1997-book2/html/PPP-1997-book2-doc-pg895.htm.

Cohen, Julie. “Cyberspace as/and Space.” *Columbia Law Review* 107 (2007): 210–56.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, DC: Department of Defense, 2011.

Ethereum.org. “Non-Fungible Tokens (NFT).” Ethereum.org. Accessed January 11, 2022. https://ethereum.org.

Facebook Data Centers. “Facebook Data Centers.” Accessed December 13, 2021. https://datacenters.fb.com/.

Federal Register. “Improving the Nation’s Cybersecurity.” Federal Register, May 17, 2021. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

Finley, Klint. “Net Neutrality: Here’s Everything You Need To Know.” *Wired*. Accessed January 8, 2022. https://www.wired.com/story/guide-net-neutrality/.

FireEye. “What Is a Zero-Day Exploit?” FireEye.com. Accessed January 8, 2022. https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html.

Futter, Andrew. “‘Cyber’ Semantics: Why We Should Retire the Latest Buzzword in Security Studies.” *Journal of Cyber Policy* 3, no. 2 (May 4, 2018): 201–16. https://doi.org/10.1080/23738871.2018.1514417.

Gibson, William. *Neuromancer*. New York: Penguin Random House, 2019.

Göcke, Benedikt Paul. “Did God Do It? Metaphysical Models and Theological Hermeneutics.” *International Journal for Philosophy of Religion* 78, no. 2 (October 1, 2015): 215–31. https://doi.org/10.1007/s11153-014-9489-7.

Hanson, F. Allan. “Models and Social Reality: An Alternative to Caws.” *American Anthropologist* 78, no. 2 (1976): 323–25.

Harknett, Richard J., and James A. Stever. “The New Policy World of Cybersecurity.” *Public Administration Review* 71, no. 3 (2011): 455–60.

Hesseldahl, Arik. “Here’s What Helped Sony’s Hackers Break In: Zero-Day Vulnerability.” Vox, January 20, 2015. https://www.vox.com/2015/1/20/11557888/heres-what-helped-sonys-hackers-break-in-zero-day-vulnerability.

“JP 3-12 Cyberspace Operations.” Washington, DC: Joint Chiefs of Staff, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

Kanno-Youngs, Zolan, and Cecilia Kang. “They’re Killing People: Biden Denounces Social Media for Virus Disinformation.” *The New York Times*, July 16, 2021, sec. U.S. https://www.nytimes.com/2021/07/16/us/politics/biden-facebook-social-media-covid.html.

Kerr, Orin S. “The Problem of Perspective in Internet Law.” *Georgetown Law Journal* 91 (2002). https://doi.org/10.2139/ssrn.310020.

Khlentzos, Drew. “Challenges to Metaphysical Realism.” In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Spring 2021. Metaphysics Research Lab, Stanford University, 2021. https://plato.stanford.edu/archives/spr2021/entries/realism-sem-challenge/.

Korolov, Maria. “An Adobe Flash Ghost May Be Haunting Your Data Center.” *Data Center Knowledge*, March 23, 2021. https://www.datacenterknowledge.com/security/adobe-flash-ghost-may-be-haunting-your-data-center.

Kreuzer, Michael. “Cyberspace Is an Analogy, Not a Domain: Rethinking Domains and Layers of Warfare for the Information Age.” The Strategy Bridge, July 8, 2021. https://thestrategybridge.org/the-bridge/2021/7/8/cyberspace-is-an-analogy-not-a-domain-rethinking-domains-and-layers-of-warfare-for-the-information-age.

Legal Information Institute. “Commerce Among the Several States.” Legal Information Institute. Accessed January 14, 2022. https://www.law.cornell.edu/constitution-conan/article-1/section-8/clause-3/commerce-among-the-several-states.

Lehe, Robert. “Realism and Reality.” *Journal of Philosophical Research* 23 (January 1, 1998): 219–37. https://doi.org/10.5840/jpr_1998_19.

Libicki, Martin C. “Cyberspace Is Not a Warfighting Domain.” *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (2012): 321–36.

Malzkorn, Wolfgang. “Leibniz’s Theory of Space in the Correspondence with Clarke and the Existence of Vacuums.” In *Twentieth World Congress of Philosophy*. Boston, MA, 1998. https://www.bu.edu/wcp/Papers/Mode/ModeMalz.htm.

McGuffin, Chris, and Paul Mitchell. “On Domains: Cyber and the Practice of Warfare.” *International Journal* 69, no. 3 (2014): 394–412.

Merriam-Webster. “Definition of Cyber.” Accessed November 13, 2021. https://www.merriam-webster.com/dictionary/cyber.

———. “Definition of Domain.” Accessed December 7, 2021. https://www.merriam-webster.com/dictionary/domain.

———. “Definition of Sphere.” Accessed December 7, 2021. https://www.merriam-webster.com/dictionary/sphere.

Millikan, Ruth Garrett. “Metaphysical Anti-Realism?” *Mind* 95, no. 380 (1986): 417–31.

Moteff, John D. “Critical Infrastructures: Background and Early Implementation of PDD-63.” Library of Congress Washington, DC, Congressional Research Service, June 19, 2001. https://apps.dtic.mil/sti/citations/ADA478523.

National Archives. “Declaration of Independence: A Transcription,” November 1, 2015. https://www.archives.gov/founding-docs/declaration-transcript.

NATO Cooperative Cyber Defence Centre of Excellence. “NATO Recognises Cyberspace as a ‘Domain of Operations’ at Warsaw Summit.” NATO Cooperative Cyber Defence Centre of Excellence. Accessed February 14, 2021. https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/.

New York Magazine. “Cyber Extra!” December 23, 1996.

Newman, Lily Hay. “Flash Is Dead—but Not Gone.” *Wired*. Accessed January 8, 2022. https://www.wired.com/story/zombie-flash-security-problems/.

Obama, Barack H. and Executive Order 13757. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, *Code of Federal Regulations*, title 3 (2017 comp.) § (n.d.).

Online Etymology Dictionary. “Cyber-.” Accessed November 7, 2021. https://www.etymonline.com/word/cyber-#etymonline_v_29224.

Plato. “The Allegory of the Cave.” In *Republic, VIi 514 a, 2 to 517. Translated by Thomas Sheehan*. Accessed October 8, 2021. https://web.stanford.edu/class/ihum40/cave.pdf.

Putnam, Hilary. “Realism.” *Philosophy & Social Criticism* 42, no. 2 (February 1, 2016): 117–31. https://doi.org/10.1177/0191453715619959.

Stang, Nicholas F. “Kant’s Transcendental Idealism.” In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Spring 2021. Metaphysics Research Lab, Stanford University, 2021. https://plato.stanford.edu/archives/spr2021/entries/kant-transcendental-idealism/.

Stenger, Nicole. “Mind Is a Leaking Rainbow.” In *Cyberspace: First Steps*. Cambridge, MA: MIT Press, 1991.

White House. “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, May 8, 2009.” National Security Archive, May 8, 2009. https://nsarchive.gwu.edu/document/21424-document-28.

———. “Defending America’s Cyberspace: National Plan for Information Systems Protection Version 1.0: An Invitation to a Dialogue.” United States. White House Office, 2000. https://www.hsdl.org/?abstract&did=1575.

———. “Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector.” The White House, January 27, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/.

———. “Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.” The White House, January 19, 2022. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.

———. *National Cyber Strategy of the United States of America.* Washington, District of Columbia: United States. White House Office, 2018.

———. “National Strategy to Secure Cyberspace.” United States. White House Office, February 2003. https://www.hsdl.org/?abstract&did=1040.

———. “Statement by President Joe Biden on Cybersecurity Awareness Month.” The White House, October 1, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/01/statement-by-president-joe-biden-on-cybersecurity-awareness-month/.

Trump, Donald J. Executive Order 13800. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, *Code of Federal Regulations*, title 3 (2018 comp.) § (n.d.).

Trump, Donald J. Executive Order 13984. Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, *Code of Federal Regulations*, title 3 (2022 comp.) § (n.d.).

Wu, Timothy. “When Law & the Internet First Met.” *Green Bag 2d* 3 (2000 1999). https://heinonline.org/HOL/LandingPage?handle=hein.journals/grbg3&div=28&id=&page=.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California