THOUGHTS INVADE US: LEXICAL COGNITION AND CYBERSPACE

BY

LIEUTENANT COLONEL CHRISTOPHER S. CORBETT

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2017

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the U.S. Government, Department of Defense, or the United States Air Force.

ABOUT THE AUTHOR

Lieutenant Colonel Corbett is a 2002 Graduate of Charleston Southern University, where he majored in Computer Science/Mathematics. His 14-year career on active duty with the Air Force has taken him to a variety of assignments and places. Prior to his assignment to SAASS, he was the Director of Operations for the 315th Network Warfare Squadron.

ACKNOWLEDGMENTS

I would like to thank my thesis advisor, Dr. David Benson, for his encouragement, guidance, and friendship during this project. He helped me see through the haze of my initial assumptions, kept me digging for the truth, and remained committed to my professional growth as an officer and as a scholar. Thank you.

I will remain eternally grateful to our nation and to the U.S. Air Force for the gift of a year at SAASS, which has allowed me to think deeply about many aspects of our national security. I hope my continued service will prove this year to have been a worthy investment.

Finally, I am unable to express the fullness of my appreciation and affection to my bride and to my children. Their patience, love, and support throughout this year have been staggering. This was truly a team effort, and I remain humbled by their many contributions and by the joy they bring into my life.

Soli Deo gloria.

ABSTRACT

This study examines the conventional wisdom that language and discourse are the dominant elements in cognition, in order to ascertain whether the way in which the Department of Defense perceives cyberspace is, in fact, related to the way it has chosen to define the term to begin with. The author explains how words and discourse appear to fashion our mental frames, which combine to ultimately shape our actions. Two case studies involving GEN (Ret.) Keith Alexander and the U.S. Congress test whether the theory of lexical cognition holds true. The study concludes that the theory does not hold true and that something other than language and discourse must have a higher degree of agency in how people approach and interpret an immaterial phenomenon such as cyberspace.

CONTENTS

Chapter page

DISCLAIMER i

ABOUT THE AUTHOR ii

ACKNOWLEDGEMENTS iii

ABSTRACT iv

1. INTRODUCTION 1

2. LITERATURE REVIEW AND THEORY 4

3. METHODOLOGY 16

4. EMPIRICS 24

5. CONCLUSIONS 55

BIBLIOGRAPHY 62

Chapter 1

Introduction

Even a cursory analysis of recent activity in cyberspace shows that the domain will be a significant factor in future conflicts. In acknowledgment of this trend, the United States, our allies, and our international competitors have all invested heavily in cyberspace capabilities and expertise. For over ten years the U.S. Air Force (USAF) and the Department of Defense (DoD) as a whole have been trying to come to terms with an "information age" environment where warfare extends into cyberspace. Since warfare in the cyberspace domain is relatively new, questions abound regarding cyberspace's place in the current conflict and in future war. To that end, military service components have devoted considerable resources to understanding factors like how to best use cyberspace, what it will mean for future conflict, the best way to develop and employ military forces within cyberspace, and a host of other considerations.

Each of these considerations are important, and rests on a common predicate, namely, a perspective of "what cyberspace *is*." Some purport that cyberspace is purely a man-made domain, which is simply an extension of an information environment existing in networked form. Others advocate a more utilitarian perspective, where cyberspace is seen as a collection of unique information technologies which create operating efficiencies, force enhancements, and advanced communications. Regardless of which perspective an organization chooses to adopt, the consensus that cyberspace is man-made seems to fall into one of two camps: interpretivism and critical realism. The interpretivist perspective extends a purely social construction of cyberspace, where the domain changes simply as an extension of social dynamics, utility, and collective desire. To the critical realist camp, an objective and

interdependent element called “cyberspace” now exists, but the way we perceive cyberspace is a function of social conditioning.

What emerges quickly from these two philosophical camps is that the way we act with respect to cyberspace is tied to our *perceptions* of what cyberspace is to begin with. So naturally, the way we choose to employ force in cyberspace is tied to our *perceptions* of the domain rather than any unique ontological understanding. Therefore, our perceptions *about* cyberspace shapes our employment within the domain and becomes a significant factor in both theory and strategy. While perceptions certainly affect operational employments in physical domains, the degree to which cyberspace is socially constructed has a compound effect on our operational employment within cyberspace. This is because two strong social forces are at work simultaneously: the actual technological environment, which is highly socially constructed, and collective perceptions about the environment. Particularly within cyberspace, then, perception and cognition interact in ways that directly influence theory, military strategy, and grand strategy. Therefore, this study focuses on identifying and understanding what is the dominant influence on perception and cognition, in hopes of shaping how we build military doctrine, theory, and strategy.

This study challenges the dominant linguistic narrative by testing the basic question of *whether* perceptions and cognition are really language and discourse-dominant, and finds that the conventional wisdom is mistaken. Conventional wisdom suggests that language and discourse maintain the dominant role in cognition because language maps to how we apprehend, judge, and then reason about everything in the world. In fact, the evidence suggests that people are more likely to be organizationally oriented or thought oriented than they are to be language and discourse oriented. In both of the following case studies, language and discourse are both shown *not* to be dominant elements in cognition. Rather than conforming to any theory of cognitive linguistics, the case studies demonstrate that neither individuals nor

organizations act in ways consistent with the supposition that discourse exercises a high degree of agency in shaping mental frames.

Both case studies are designed to test complementary aspects of cognitive theory. Lexical cognition would predict that GEN (Ret.) Alexander, the former commander of U.S. Cyber Command, would be reluctant to change a firmly entrenched perspective of cyberspace; that was not the case. Likewise, the theory would predict that the U.S. Congress could never really converge on a unified perspective of cyberspace, but they have. In both cases, conventional wisdom, which holds that language has a dominant degree of agency in creating and maintaining mental frames, did not prove true.

Chapter 2

Literature Review and Theory

Conventional wisdom suggests ideas are strongly linked to language, and therefore language exerts a high degree of agency on a person's thoughts. Human minds are understood to act through common and distinct processes, and that fact becomes the theoretical basis for why words, language, and discourse ultimately shape our actions. Words, sentences, and paragraphs influence our perspective because they directly translate to the three basic acts of the mind: simple apprehension, judging, and reasoning.[1] Lexical meaning interacts with our mental frames to inform our approach to a given concept, which tends to result in predictable actions.[2]

According to this understanding, language connects an objective phenomenon to how we communicate about it, before acting in fixed patterns. Therefore, the *words* we assign to immaterial concepts like cyberspace bind our perceptions in a variety of measurable ways.[3] How the AF defines a distinct domain like cyberspace should have a profound impact on how the AF develops and employs Airmen to meet future operational challenges. If this is true, then deceptively simple factors such as the definition of cyberspace will have a profound effect on our future decision-making. For example, assuming cyberspace is the *sine qua non* for enacting our will in the Information Age, then developing a definition with respect to utility instead of physics could leave us unprepared for the next war.

---

1. Peter Kreeft, *Socratic Logic: A Logic Text Using Socratic Method, Platonic Questions & Aristotelian Principles*, ed. 3.1, ed. Trent Dougherty (South Bend, Ind: St. Augustine's Press, 2010), p. 28-29.
2. Benjamin Lee Whorf, *Language, Thought, and Reality: Selected Writings* (Cambridge, 1956), accessed December 28, 2016, http://hdl.handle.net/2027/uc2.ark:/13960/t9n300r6z.
3. Whorf, *Language, Thought, and Reality*.

Discourse, Frames, and Action

Languages are particularly influenced by the living cultures from which they emerge, and require a shared understanding of words, terms, definitions, syntax, and basic rules of grammar in order to communicate.[4] Language allows people to share concepts with each other, which is how civilizations progress towards higher levels of knowledge.[5] In this sense, at least, our shared language is crucial to how we understand a particular phenomenon. Genuine dialog between willing participants assumes everyone involved in the discussion truly wants to come to an understanding that reflects both reality and context; dialog is the foundation for how we derive shared meaning.

Linguistic formulation is also wedded to basic human reasoning. Human reason works through common thought structures as we move from apprehending a specific phenomenon towards a collective understanding of it. In this cognitive progression, we take objects of comprehension, make judgments about them, and then translate that understanding into a spoken language to communicate with ourselves and with others.[6] Some of the most important things we communicate are *what* and *why*, which combine with a sense of purpose to produce a "so what" or a "so then," which are requisites for our later actions.[7] Words, sentences, and paragraphs create the linguistic and syntactical formulations which emerge through language.[8]

The degree of agency language has in producing subsequent actions is related to cognitive frames. Frames encompass the structure into which we deposit thoughts and ideas, and from which we draw conclusions.[9] Thoughts

4. Hilary Putnam, *Mind, Language, and Reality*, His Philosophical Papers; v. 2 (New York: Cambridge University Press, 1975).
5. Noam Chomsky, *Language and Mind*, 3rd ed (New York: Cambridge University Press, 2006), p. xiv.
6. Kreeft, *Socratic Logic*, p. 139.
7. Kreeft, *Socratic Logic*, p. 36.
8. Putnam, *Mind, Language, and Reality*, p. 126.
9. Timothy Ferris, *The Mind's Sky: Human Intelligence in a Cosmic Context* (New York: Bantam Books, 1993), p. 4.

flow through cognitive frames, which mediate between a person's perceptions and actions, and filter incoming information.[10] Frames also act as a triggering mechanism towards specific behavior, and while they do not prescribe *specific* courses of action, they do shape peoples' thoughts and ideas, which form the basis for future action.[11] This is not a one-way transaction, but a reciprocating and self-reinforcing process whereby the person involved in the mental transaction imposes his mental frame on both objective reality and on the language he is using to communicate about that reality.[12] Frames are a significant factor when trying to understand cognitive linguistics within a deeper context like history, culture, and environment, all of which influence thought.

On the surface, today's cultural milieu certainly seems to conform to many aspects of cognitive theory. Media outlets and politicians are masters at re-naming concepts in order to shape the narrative which best fits their desired outcome. Words influence public policy debates, debates of theory within scientific communities, and doctrinal development within the Armed Forces. The real question is not whether words matter, but *how* they matter. How do words function in relation to cognition, mental frames, and subsequent action? If words have agency, then what degree of agency do they have within the broader application of language?

From Words to Concepts

In cognitive theory, one of the hardest elements to fully understand is agency. Elements like culture, context, language, organizational imperative, belief, and desire all have some degree of agency that shape our frames and emerge through our later actions. Cognitive linguistics focuses on the impact that language has on human interaction, and maintains that everything from

10. Ferris, *The Mind's Sky*, p. 5.
11. R. C. Sproul and Keith A. Mathison, *Not a Chance: God, Science, and the Revolt Against Reason* (Grand Rapids, Michigan: Baker Books, 2014), p. 107.
12. Here and throughout I use 'he' as a gender *inclusive* pronoun in the traditional literary sense.

word choice, grammar, and syntax plays a role in shaping our actions because they help structure our mental frames.

Language goes beyond simply bridging words and concepts. Rather, language allows people to share or expand concepts, which become cognitive building blocks upon which civilizations progress towards higher levels of knowledge. For example, it is more difficult to arrive at a new concept than it is to use conventional ones, and this is especially true when dealing with things which are immaterial or unobservable.[13] We can "conceive of objects or concepts for which there is no lexicon or vocabulary, but it's much harder to hold or communicate those thoughts."[14] Words like "genes" and "atoms" are very hard to think about without *a priori* concepts of each. Therefore, having words like "atom" and "cyberspace" allows us to communicate about increasingly complex concepts.[15]

Language and concepts are linked, but there has to be a prior concept against which to assign terms in the first place. So then, having an existing public word with shared meaning is dependent on the existence of the objective reality encompassed by the concept; the concept under investigation continues to exert influence over throughout the process of communication. In addition, the language of thought is "tied to the public language…[but] we still have the capacity to think beyond the conventional established public language, as is shown by our ability to express new thoughts in new words."[16]

Taken as a whole, we begin to see how language brings concepts into focus, allows us to build upon a collective understanding, and solve complex problems. Does language have a direct impact on a person's immediate actions, and if so can we actually measure it? Benjamin Whorf thought we could.[17]

---

13. Michael Devitt and Kim Sterelny, *Language and Reality: An Introduction to the Philosophy of Language*, vol. 2nd ed (Cambridge, Mass: MIT Press, 1999), p. 218.
14. Devitt and Sterelny, *Language and Reality*, p. 219.
15. Devitt and Sterelny, *Language and Reality*, p. 218.
16. Devitt and Sterelny, *Language and Reality*, p. 155.
17. Whorf, *Language, Thought, and Reality*.

Words in Action

Benjamin Whorf was one of the earliest linguistic theorists to connect the words people used to describe an object to their later actions, and he is widely known for advancing studies of linguistic cognition. While analyzing mishap reports from a wide range of residential and business fires, Whorf initially focused only on the physical conditions surrounding the fire: defective wiring, building code, presence or lack of air spaces, etc.[18] Over time, he began to realize that the physical conditions were insufficient to account for either the range of fires or for their severity. Whorf came to believe that the words—or more specifically, the associative meaning behind the words—people used to describe a situation were a significant factor in the onset of a fire. "It became evident that not only a physical situation *qua* physics, but the meaning of that situation to people, was sometimes a factor, through the behavior of the people, in the start of the fire. And this factor of meaning was clearest when it was a linguistic meaning, residing in the name or description commonly applied to the situation."[19] Many fires would start once people associated words like "empty" with the concepts of nothing, null, negative, and inert, and apply the same term to a physical situation without regard to the actual condition of the environment. In reality, the true physical situation may have offered pristine conditions for a fire: the presence of vapor, flammable liquid, small bits of stray trash—the exact opposite of empty.[20] As a matter of routine, people's actions in a situation were consistent with the lexical meaning of words like "empty," "off," and "pool of water," which regularly led to disastrous behaviors. Whorf proposed that the words people used to describe a situation directly translated into their actions.

Linguistic or syntactical determinism is a more extreme form of cognitive studies, understood by overemphasizing the degree agency words have on our actions; linguistic determinism is a line of reasoning I specifically want to

18. Whorf, *Language, Thought, and Reality*, p. 135.
19. Whorf, *Language, Thought, and Reality*, p. 135.
20. Whorf, *Language, Thought, and Reality*, p. 136.

avoid.[21] In a conventional theory of linguistic cognition, language and thoughts are related but thoughts are by no means wholly subordinate to language. If thought were completely subordinate to language, both logically and temporally, no human being would be able to think or speak because languages are learned; *thinking* is what enables us to learn a language to begin with. In the same way that technology is socially constructed but later exerts influence within a heterogeneous system, words are also socially constructed and exert a degree of agency into our thought process.[22] They do not, however, become the singular dependent variable in our understanding. Language *influences* knowledge, frames, and action, but the ultimate priority remains with the larger category of thought.[23] Cognitive linguistics in its conventional form is more about a primacy of agency than its dominance over thought.

Frames: The Unwitting Intermediary

Largely due to the influence of cognitive linguists, conventional wisdom maintains that language is a dominant and self-reinforcing means by which we develop and maintain mental frames.[24] Many people take it for granted that a person's actions are more consistent with their perceptions than they are with objective reality or objective circumstances. We intuitively know it is impossible for any person to be truly objective (in the strictest sense of the term) in situations in which they have significant or highly personal experience.[25] This is true because we all possess individual *frames* that mediate our actions and filter incoming information, thereby exerting substantial influence over our decisions.

---

21. Incidentally, Devitt concludes that Whorf's later works place him squarely in the linguistic determinist camp. See Devitt and Sterelny, *Language and Reality*, p. 217.
22. For more information on the social construction of technology, see Merritt Roe Smith and Leo Marx, eds., *Does Technology Drive History?: The Dilemma of Technological Determinism* (Cambridge, Mass: MIT Press, 1994).
23. Devitt and Sterelny, *Language and Reality*, p. 219.
24. This essay demonstrates the roles frames play but does not specifically test them. Rather, the goal is to understand the degree of agency language has on the intermediary of frames to produce certain effects.
25. Daniel Kahneman, *Thinking, Fast and Slow*, 1st ed (New York: Farrar, Straus / Giroux, 2011), p. 323.

Lexical meaning interacts with our frames, produces predictable actions, and shapes the way we approach a concept both intellectually and emotionally.[26] To this end, a person's frames will never be *about* cyberspace per se, but they play a key role in understanding the *meaning* of cyberspace within a larger context. So then, what role do a person's frames play in relation to cognition?

Mental frames are the triggering mechanism between the independent variable "cause" and the dependent variable "effect." They encompass the structure into which we deposit thoughts and ideas, and from which we draw conclusions. Frames do not prescribe courses of action, but they do shape our understanding. Additionally, frames are not unbiased, which is evidenced in many ways throughout the scientific community, where frames superimpose individual perceptions into the research progress.[27] For example, choices to employ a tool one way or another to measure an effect requires a prior assumption about what sort of results or circumstances might occur in the first place.[28] Frames also have a substantial effect on cognitive consistency, where the validity of new information is not determined by objective evidence but by how well both the evidence and the initial proposition fit into existing frames.[29] Frames are so influential in scientific, mental, and doctrinal thought processes, that even in the face of new and discrepant information people will hold to their current understanding and theory. People generally assume that they are correct and that any new information incompatible with their frame must be either invalid or susceptible to reinterpretation.[30]

Frames also act as intermediaries between a universe which exists objectively and our capacity to know it. Timothy Ferris used the metaphor of an

---

26. Richard Bailey, "Dilating Pupils: The Pedagogy of Cyberwar and the Encouragement of Strategic Thought," *Air and Space Power Journal* 7, no. 3 (2016): p. 11, accessed November 8, 2016, http://www.au.af.mil/au/afri/aspj/apjinternational/aspj_f/article.asp?id=185.
27. Thomas S. Kuhn, *The Structure of Scientific Revolutions*, Fourth edition, in collab. with Ian Hacking (Chicago and London: The University of Chicago Press, 2012).
28. Kuhn, *Structure*, p. 59.
29. Robert Jervis, *Perception and Misperception in International Politics* (Princeton, N.J: Princeton University Press, 1976), p. 157.
30. Jervis, *Perception*, p. 156.

hour glass to describe our relationship to the universe in respect to our frames, where everything that *is* the universe passes through our frame (the neck of his hour glass) and alters our perception:

> On one side is the outer realm, inhabited by galaxies, stars, the plants and animals, and our fellow human beings. Most of us (the solipsists aside) believe that this outer world exists, though we appreciate that our direct perceptions of it are limited and skewed. On the other side is the inner realm of the mind, where each of us is destined to live and die; here resides all we can ever know. Through the neck of the glass flow the sense data by which we perceive the outer realm, and (flowing the opposite way) the models we apply to nature, and the alterations and abridgments *we impose on her*.[31]

Our perceptions depend not only on the accuracy of our observations but also on the frames through which we conceptualize the universe. Given that our linguistic development is both personal and contextual, and that no two people have identical frames, the *meaning* of the words and language by which we communicate also differs by varying degrees. All things are framed by the "limitations and peculiarities of our sensory apparatus, the prejudices of our presupposition, the multiplicity of each individual mind, and *the restrictions of language*."[32] Since we have individual experiences and frames, we may communicate approximately within a shared language about an unambiguous term, but our language remains somewhat tainted.[33]

Information presented through language collides with our frames with predictable results, because our actions are bound by frames instead of by reality.[34] In fact, individual perceptions would be inconsequential without frames triggering specific behavior. For example, "cold cuts described as '90% fat-free' are more attractive than they are described at '10% fat.' The equivalence of the alternative formula is transparent, but an individual normally sees only on the formulation."[35] Marketers rely on language that will shape perceptions and interact with the prevailing narrative to influence the buyer.

---

31. Ferris, *The Mind's Sky*, p. xii-xiii. My emphasis.
32. Ferris, *The Mind's Sky*, p. 5. My emphasis.
33. Sproul and Mathison, *Not a Chance*, p. 108.
34. Kahneman, *Thinking, Fast and Slow*, p. 367.
35. Kahneman, *Thinking, Fast and Slow*, p. 88.

In addition, notice the common responses to two propositions presented to various students, which highlights how words trigger a consistent response when they interact with the students' frames:[36]

(a) Should a child exemption be larger for the rich than for the poor?

Predictably, students found the idea of favoring "the rich" with a larger exemption to be unacceptable.

(b) Should the childless poor pay as large a surcharge as the childless rich?

Again, the students expressed a similar reaction. Both questions address contradictory choices to the same problem and are intentionally pejorative to appeal to the students' common perception. However, a choice for (a) necessitates (b), and vice-versa, though both choices sound unappealing. These examples demonstrate how words trigger different responses that coincide with general inclinations that "fat is bad," and, "when in doubt, favor the poor."[37] Perceptions would be meaningless without frames acting as a triggering mechanism towards specific behavior.

The impact of frames is not limited to theoretical applications of philosophy or to the social sciences, but are also tangible in the natural science. Prior to 1962, the prevailing narrative throughout the scientific community was that scientific pursuits were conducted through purely objective means of discovery and observation.[38] Natural sciences were generally understood to be unbiased representations of objective reality, where scientists relied on available empirical data for scientific progress. However, rather than processing discrete evidence logically and empirically, scientists actually approached evidence through frames, which *bound* their observations to the prevailing theory.[39] For example, an investigation into the history of atomic theory revealed that to the chemist, helium was seen to be a molecule because it acts consistent with the

36. Kahneman, *Thinking, Fast and Slow*, p. 369.
37. Kahneman, *Thinking, Fast and Slow*, p. 369.
38. Kuhn, *Structure*.
39. Kuhn, *Structure*.

kinetic theory of gasses. On the other hand, for the physicist it was not taken to be a molecule because it displayed no molecular spectrum.[40] "Presumably both [researchers] were talking about the same particle, but they were viewing it through their own research training and practice."[41] The researchers' frames superimposed biases into what would otherwise be objective empirical observations and demonstrated that people will go to great lengths to preserve their images "in the face of what seems [be] clear evidence to the contrary. We ignore information that does not fit, twist it so that it confirms, or at least does not contradicts, our beliefs, and deny its validity."[42] These findings challenged the perspective that science was a purely rational enterprise, and suggested that scientific pursuits were influenced by frames which locked groups of scientists into specific modes of thinking and research.[43]

Based on these observations, the interaction of lexical meaning with our frames seems to hold a degree of agency over our actions. This interaction is not a one-way transaction, but a reciprocating and self-reinforcing process, whereby the person involved "imposes his frame not only on the phenomena but on the language he uses to describe or represent the phenomena."[44] Insomuch as lexical meaning self-reinforces and perpetuates both collective understanding and behavior, then as a person or organization discuss a concept within a particular vein of thought they will slowly develop understandings which are difficult if not impossible to change. By that token, if military leaders perceive cyberspace to be a collection of well-managed IT and data, and define the cyberspace domain consistent with that commoditized understanding, then according to cognitive linguistics leaders will naturally organize and employ cyber forces to protect our commodities and to exploit those of our adversaries.

---

40. Kuhn, *Structure*, p. 51.
41. Kuhn, *Structure*, p. 51.
42. Jervis, *Perception*, p. 143.
43. Thomas Kuhn coined the term 'paradigm,' to refer to this tendency.
44. Sproul and Mathison, *Not a Chance*, p. 107.

Theoretical Implications

Conventional wisdom reflects a broad understanding that ideas flow from language and that language is self-reinforcing over time. If the theory of lexical cognition proves true, then changing people's actions begins by changing the words they use.[45] This could have a significant impact on the DoD's approach to cyberspace, because how we develop and employ forces to achieve any operational manifestation of power partly rests on the language we use to describe cyberspace. Insomuch as the DoD's approach to cyberspace reflects a decidedly utilitarian understanding, then we will organize, train, and equip the force to provide and defend utilitarian functions. If we decided to change how we approach cyberspace, so as to take a more ontological approach rather than a commoditized one, then the first and most basic step would be to come to terms with a new definition.

On the other hand, language may not have the degree of agency attributed by linguistic theory and therefore not be a dominant player in cognition. If the way we *think* about cyberspace matters more than the language we use to communicate about it, then we have to turn to other sources of cognitive influences to shape our understanding. The way we think about cyberspace may, in fact, be shaped organizationally, culturally, and contextually more so than by language. If the latter is the case, simply focusing on developing our warfighters by shaping educating, training, and doctrine would be insufficient. Leaders would also have to focus on different mechanisms, such as organizational challenges, competitive conditions, character, and culture if they truly wanted to effect change in perception.[46] In theory, the longer a person talks

45. This would be most consistent with Whorf's work on cognitive linguistics.
46. For a more complete discussion of organizational culture and organizational change, see Nilofer Merchant, "Culture Trumps Strategy, Every Time," March 22, 2011, accessed November 2, 2016, https://hbr.org/2011/03/culture-trumps-strategy-every, as well as Robert Kegan and Lisa Laskow Lahey, *Immunity to Change: How to Overcome It and Unlock Potential in Yourself and Your Organization*, Leadership for the Common Good (Boston, Mass: Harvard Business Press, 2009).

about a phenomenon a certain way, the more he will cement his frame around his current understanding. This would be measurable first in his language and subsequently in his actions. From an organizational perspective, an organization's understanding of cyberspace should change if the environment experiences an influx of additional people contributing to the conversation using outside linguistic inferences. For example, if an organization consistently brings in new members with a disparate understanding of the phenomenon under study, then their collective understanding should either remain in flux or at least remain fairly nebulous so as to appeal to only the basic or universal principles. However, if an organization consistently brings in diverse members and perspectives, only to have a nebulous understanding converge over time into a unified taxonomy, then the theory may be invalid. Likewise, if an individual thinks and talks about cyberspace for many years using a consistent taxonomy, and then begins to slide into a different taxonomy based on where he now operates, then the theory would also break down.

Chapter 3

Methodology

To test this theory I created a stable taxonomy with which to evaluate how people and institutions generally perceive the cyberspace domain. I constructed the taxonomy by researching four main sectors' perspectives relating to cyberspace: The Department of Defense, the larger federal government, academia, and commercial industry. Though perceptions of cyberspace are somewhat diverse, they generally fall into one of four categories of understanding: commodity, utilitarian, axiomatic, and perspective dependent.

Next, I created two case studies with which to test a cognitive linguistic theory, incorporating a textual analysis to determine how the actors involved understood cyberspace, and whether that understanding changed over time. For the first case study I selected General (Ret.) Keith Alexander, who retired as the Director of the National Security Agency (NSA), also known as DIRNSA, and as the Commander of U.S. Cyber Command (USCYBERCOM). GEN Alexander participated in a number of public interactions throughout his time at the NSA and USCYBERCOM and has since maintained a public presence. To be consistent with cognitive linguistics, GEN Alexander's perspective of cyberspace should be remain unchanged after his retirement in March of 2014.

The next case study I selected was the House Armed Services Committee (HASC) of the U.S. Congress, beginning with the 109th Congress, 2005 congressional cycle. Congressional dialog is well documented, and the HASC produces two products which are very useful in evaluating current perspectives: annual reports to the Congress and the National Defense Authorization Act (NDAA). Given that the members of congress rotate frequently through subcommittees, we would expect their understanding of cyberspace to somewhat nebulous, or at least axiomatic.

Taxonomy

The way in which people regard cyberspace generally falls into one of four perspectives. The first is a *commoditized* perspective, where cyberspace is understood in light of its commodities. For example, the government tends to understand cyberspace as a combination of Information Technology (IT) and resident data, both of which are commodities. Another way people understand cyberspace is by using a *utilitarian* approach—"What's most useful to me?" Most commercial industry takes a utilitarian approach to cyberspace, defining or talking about the domain in terms of its utility to their specific company or product. If Company A is selling a cybersecurity service or a "hunt" platform, then they tend to favor language to discuss cyberspace that will validate a wide need for their product. A third way people understand cyberspace is to look at it *axiomatically*; some people or organizations speak of cyberspace simply as a self-evident phenomenon. Usually, an axiomatic understanding manifests itself when a person's main focus is tangential to cyberspace, but they still rely on cyberspace's existence for study or for profit. In an axiomatic understanding, the organization makes no attempt at reification but accepts cyberspace as they would any independent variable like air, space, or time. The final way people characterize cyberspace is using *perspective dependent* language. Perspective dependence is easily summed up in the concept of "where you stand is where you sit," and is especially noticeable in academia. For example, institutions with a strong historic background in Law will generally approach cyberspace in light of law code.

Deriving Four Perspectives

To create this taxonomy, I surveyed the DoD, government, academia, and industry to determine the way in which they approached cyberspace. I began with the Department of Defense and the federal government, and then shifted to

corporate leaders for a counter perspective. Academia provides the final group, being informed by some of America's best educated people who *think* a lot about cyberspace.

The two foundational documents within the DoD which discuss and integrate cyberspace are Joint Publication 3-12(R), *Cyberspace Operations* and The National Military Strategy for Cyberspace Operations (NMS-CO). Lateral documents such as service-specific doctrine and the DoD Strategy for Operating in Cyberspace build on those foundational works. To research how academia thinks about cyberspace, I used the 2014 Ponemon Report on *Best Schools for Cybersecurity* as my basis for school selection. This report was sponsored by HP Enterprise Security, and commissioned to "determine those institutions that are achieving a high level of excellence and [study] the characteristics that set them apart."[1] The Ponemon Institute surveyed 5,003 institutions for criteria such as academic excellence, practical relevance, expertise of program faculty, background of students and alumni, and the school's professional reputation within the cyberspace community.[2] Given their rankings as the top academic institutions currently studying cyberspace, then examining these institutions' publications provides a reliable cross-section for how academia tends to think about cyberspace.

Finally, the market data firm Cybersecurity Ventures compiles an industry pool of top cybersecurity organizations through their "Cybersecurity 500" list.[3] According to Cybersecurity Ventures, "the Cybersecurity 500 creates awareness and recognition for the most innovative cybersecurity companies—ranging from the largest and most recognizable brands to VC-backed startups and emerging players, to small firms with potentially game-changing technologies."[4] Instead of

1. Ponemon, *2014 Best Schools for Cybersecurity*, Research Report (Ponemon Institute), p. 1. Accessed March 15, 2017, https://www.ponemon.org/local/upload/file/2014%20Best%20Schools%20Report%20FINAL%202.pdf.
2. Ponemon, *2014 Best Schools for Cybersecurity*, p. 1.
3. "Cybersecurity 500 List of Top Cybersecurity Companies," Cybersecurity Ventures, March 1, 2017, accessed March 15, 2017, http://cybersecurityventures.com/cybersecurity-500-list/.
4. "Cybersecurity 500 List of Top Cybersecurity Companies."

ranking companies by revenue, the number of employees, or annual growth, the report focuses on 15 intrinsic and extrinsic factors to highlight current relevance to cyberspace. Surveying the top 25 companies on the Cybersecurity 500 list provides a cross-section of industry players who are the most active in thinking about cyberspace as a whole.

Sector Perspectives on Cyberspace

The Department and Defense and the federal government tend towards a commoditized approach when thinking about cyberspace. Joint Publication 3-12(R) defines cyberspace as "a global domain within the information environment consisting of the interdependent networks of *information technology* infrastructures and resident *data*, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] Distilled to the basics, the DoD definition focuses mainly on information technology or information systems, plus data. This perspective was also reflected in the NMS-CO, where cyberspace is seen to use the Electromagnetic Spectrum to "store, modify, and exchange *data* via *networked systems* and associated physical *infrastructures*."[6] The most recent National Military Strategy (NMS), published in 2015, continues with a commoditized understanding. Referring to *Providing for Military Defense of the Homeland*, the 2015 NMS states that "emerging state and non-state capabilities pose varied and direct threats to our homeland. Thus we are striving to interdict attack preparations abroad…and *protect cyber systems and physical infrastructure*."[7] Based on reviewing the DoD's lexical choice with respect to cyberspace, we can also derive the top two

5. "Joint Publication 3-12 (Redacted): Cyberspace Operations," p. 69. My emphasis. Accessed November 28, 2016, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
6. "National Military Strategy for Cyberspace Operations (NMS-CO)," p. 3. My Emphasis. Accessed November 28, 2016, http://www.dod.mil/pubs/foi/Reading_Room/Joint_Staff/07-F-2105_doc_1.pdf.
7. "The National Military Strategy of the United States of America," p. 11. My emphasis. Accessed November 28, 2016, http: //www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

commodities which receive the most emphasis in cyberspace within the DoD: Information Technology (or systems) and data.

Unlike the DoD, commercial industry generally discusses cyberspace using a utilitarian approach, though commoditized approaches are sometimes prevalent. Utilitarian approaches taken by companies such as Clearwater Compliance, Check Point, and BAE Systems are usually reflected in their product offerings more so than their published work. For example, Clearwater Compliance uses a business model that specializes in risk management and compliance for medical care providers trying to protect personal medical information or patient safety.[8] Clearwater markets their products under Services, Software, Security, and total solutions, but the words Clearwater uses to highlight cyberspace change within each product offering. Their security offering is closely geared towards cybercrime within the medical care industry, and therefore focuses on securing data breaches and on mitigating operational risk.[9] However, when discussing their software offering, Clearwater Compliance focuses less on cybersecurity per se, and more on automated auditing functions through data analysis.[10] In that regard, Clearwater typifies a company who takes a utilitarian approach to cyberspace—"What's most useful to me?"

While most companies on Cybersecurity Ventures's Cybersecurity 500 list prefer a utilitarian approach to cyberspace, some also use a commoditized understanding. This is most prevalent in companies like Symantec or Kaspersky Labs, whose offerings focus in on single problems like information security or data integrity. Both Symantec and Kaspersky mostly discuss cyberspace in light of commodity management. Another useful example of a company who takes a commoditized approach is CISCO, long known for their high-end infrastructure

8. Clearwater, *Healthcare Security Readiness*, March 2017, accessed March 15, 2017, https://clearwatercompliance.com/wp-content/uploads/2017/02/Intel-Clearwater-Compliance-Healthcare-Security-Readiness-Program.pdf.
9. Clearwater, *Healthcare Security Readiness*.
10. Clearwater, *Clearwater IRM Analysis*, accessed March 15, 2017, https://clearwatercompliance.com/wp-content/uploads/2015/07/Clearwater_IRM_Analysis_Data-Sheet-1.pdf.

hardware. CISCO embraces a cyberspace perspective of "networked IT systems," which is reinforced by their "Architecture of Trust."[11] CISCO's use of trusted services, systems, and processes is geared specifically towards IT systems, infrastructure, and network management, respectively. So, while commercial industry generally favors a utilitarian approach to understanding cyberspace, companies whose product offerings focus on more acute problems often lean towards a commoditized understanding.

Whereas the DoD and Federal Government heavily favor a commoditized approach to cyberspace, and industry leans more towards a utilitarian approach, academia has no dominant perspective. Schools surveyed from the Ponemon Institute report used all four approaches to discussing cyberspace with equal regularity.[12] For example, Berkeley's Center for Long-Term Cybersecurity (CLTC) takes an axiomatic approach to cyberspace when advocating for areas of academic or policy improvement.[13] The CLTC's policy recommendations for space outlined everything from the role of cyberspace in public safety, to nation-state behavior in cyberspace, to cyberspace's role as "an existential risk to core American interests and values, rising close to the level of major armed conflict and climate change."[14] The University of Pittsburgh, on the other hand, tends to discuss cyberspace more in perspective-dependent terminology, shifting terms based on school-specific perspectives within the larger university construct.

11. CISCO, *Building an Architecture of Trust: The Network's Role in Securing Cyberspace*, January 2011, p. 7. Accessed March 15, 2017, https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/Architecture_of_Trust_WP.pdf.
12. I must note here that performing a textual analysis of academic institutions is more problematic than industry or the federal government because their publications tend to be rather diverse and their academic programs are written to be all-encompassing. The resulting ambiguity sometimes leaves more to interpretation than other major industries would.
13. Berkeley, *Cybersecurity Policy Ideas for a New Presidency*, November 2016, accessed March 16, 2017, https://cltc.berkeley.edu/files/2016/11/Center_for_Long_Term_Cybersecurity.pdf.
14. Berkeley, *Cybersecurity Policy Ideas for a New Presidency*, p. 2.

Case Selection

To test the conventional understanding of lexical cognition onto cyberspace I chose two case cases on which to build a textual analysis. The first case looks at General Keith Alexander, who retired as the commander of U.S. Cyber Command (USCYBERCOM). Prior to assuming command of USCYBERCOM, GEN Alexander was the Director of the National Security Agency (NSA), and he continued to lead both organizations until he retired. Of his 30 years of military service, almost 10 were directly associated with the NSA and 4 with USCYBERCOM. Given GEN Alexander's longevity serving in roles directly related to cyberspace, we would expect his word choice, language and discourse to remain consistent after he retired. Since the DoD takes a decidedly commoditized view of cyberspace, then a commoditized view should be evident in GEN Alexander's speeches his last several years in service, and continue into his retirement.

The second test case is a textual analysis of documents produced by the U.S. House of Representatives' Committee on Armed Services.[15] The HASC annual report to Congress, committee hearings, and the National Defense Authorization Act (NDAA) provide the basis for understanding how the HASC understands cyberspace as an organization. The HASC is a useful test case because the members of the HASC rotate frequently through its many subcommittees. Members of congress tend to participate in two or three major committees in additional to various subcommittees.

Elected representatives to Congress come from all over the United States and with diverse professional backgrounds. Given a two-year election cycle to the U.S. House and the members' rotation in and out of committees, we would expect the perspectives echoed in the NDAA to reflect a vague or axiomatic understanding of cyberspace. Consistent with the theory of lexical cognition,

15. The Committee is more generally known by the name House Armed Services Committee, or HASC. Throughout this study, I mostly use the less formal "HASC."

another possibility would be that dominant personalities or events within a particular congressional cycle could steer the committee towards a particular perspective. However, if that were to occur we would still be able to measure a shift in lexical understanding from one Congress to another.

Chapter 4

Empirics

Conventional wisdom holds that language exerts a high degree of influence on how a person perceives and then interacts with any phenomenon. Language and dialog are also said to shape a person's frame and become self-reinforcing over time; the longer a person perceives and communicates about a phenomenon using a particular taxonomy, the more that person will become bound by that understanding. Actions are predicated on language and discourse, which develops, interacts with, and strengthens mental frames through an iterative process. Therefore, measuring and quantifying lexical patterns over time should be a strong indicator of not only how a person perceives cyberspace now, but how they are likely to perceive it in the future.

By conducting a textual analysis on General Alexander and then the U.S. Congress, this section tests whether or not the conventional wisdom of lexical cognition holds true. By the time GEN Alexander retired he should have been well-steeped in a particular perspective with a distinct taxonomy, and we can expect he will maintain that perspective for many years into the future. Additionally, as the U.S. Congress begins to discuss cyberspace, we can expect their understanding to never coalesce around a singular taxonomy but rather change over time. Rather than adopting a uniform taxonomy, it should be readily apparent that the Congress's perception of cyberspace shifts loosely between the four taxonomies.

General Keith B. Alexander

Speech to CSIS: Jun 2010

On June 3rd, 2010, GEN Alexander delivered a speech to the Center for Strategic and International Studies (CSIS) on U.S. cybersecurity policy and the role of U.S. Cyber Command.[1] His speech came two weeks after taking command of the newly-established U.S. Cyber Command (USCYBERCOM) and serves as a useful indicator of how he understood cyberspace at the time.[2] Throughout GEN Alexander's speech, he uses examples and analogies to explain operational challenges which had manifested themselves over the preceding years. First, he discusses the nature of the cyberspace challenge as a "team sport," requiring the DoD and national agencies to work together for national security.[3] In his assessment, USCYBERCOM's role in the team is to:

> be responsible day to day for directing the operations and defense of the Department of Defense information networks and for the systemic and adaptive planning, integration and synchronization of cyber-activities, and when directed under the authority of the president, the secretary of defense and the commander of U.S. STRATCOM, for conducting full-spectrum military cyberspace operation to ensure U.S. and allied freedom of action in cyberspace.[4]

This precept is fairly indicative of positions GEN Alexander takes throughout his time as the USCYBERCOM Commander.

Particularly useful in GEN Alexander's speech to CSIS is his response to a question about deterrence. One of the audience, Randy Fort, associated with Raytheon, drew an equivocation from GEN Alexander's previous remarks to the concept of deterrence.[5] Mr. Fort specifically asked for GEN Alexander's thoughts

1. Keith B. Alexander, *CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. Cyber Command*, June 3, 2010, accessed March 21, 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/event/100603csis-alexander.pdf.
2. USCYBERCOM stood up on May 21st, 2010.
3. Alexander, *U.S. Cybersecurity Policy and the Role of U.S. Cyber Command*, p. 3-4.
4. Alexander, *U.S. Cybersecurity Policy and the Role of U.S. Cyber Command*, p. 4.
5. Specifically, Mr. Fort referenced GEN Alexander's remarks on "discouraging malevolent behavior in cyberspace." See Alexander, *U.S. Cybersecurity Policy and the Role of U.S. Cyber Command*, p. 11.

on "the potential of deterring…malevolent behaviors on the Web."[6] GEN Alexander's response is useful because deterrence theory has been well-established in military and political parlance since before—and certainly after—Thomas Schelling's landmark work, *Arms and Influence*, in 1966.[7] While Schelling's work was largely about nuclear deterrence, the key attributes of credibility, threats, and compellence have often been exported to a wide range of military theory. GEN Alexander would certainly be familiar with the topic, and so the core of his response is unorthodox. "If nation-states agree on what we're going to do to deter malicious actors in cyberspace, that will go a long ways to do this…but it's not good enough for what we need. [Putting] it from a nation's perspective, what's on those networks that we've got to secure? Well, it's our intellectual property. It's the future of our country."[8] Here as before, GEN Alexander's perspective on the strategic import of USCYBERCOM comes by way of protecting a key national asset—intellectual property. Intellectual property is a commodity that, in cyberspace, takes the form of data.

For the rest of his speech, GEN Alexander expands recurring themes of "information networks," "operations in cyberspace," and "freedom of action." When discussing the nature of cyberspace, GEN Alexander states that "cyberspace consists of vexingly complex systems that ship and store unimaginably vast amounts of data."[9] That sentence typifies a commoditized view of cyberspace, which is naturally in line with the DoD's perspective on primary cyberspace commodities: systems (or information technology) and data. Subsequent discussion proceeds down the same path, stating that "data…forms the basis of [U.S.] economic wealth and contribute to our quality of life. Tremendous opportunities for the future and tremendous vulnerabilities, *our data must be protected*".[10]

6. Alexander, *U.S. Cybersecurity Policy and the Role of U.S. Cyber Command*, p. 12.
7. Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 2008).
8. Alexander, *U.S. Cybersecurity Policy and the Role of U.S. Cyber Command*, p. 12.
9. Alexander, *U.S. Cybersecurity Policy and the Role of U.S. Cyber Command*, p. 4.
10. Alexander, *U.S. Cybersecurity Policy and the Role of U.S. Cyber Command*, p. 5. My emphasis.

Senate Hearing: Mar 2013

Roughly three years after GEN Alexander's speech to CSIS, he delivered his opening remarks to the Senate Armed Services Committee, testifying in his continued role as Commander of U.S. Cyber Command (USCYBERCOM). GEN Alexander begins with perfunctory introductory remarks about the USCYBERCOM organization and personnel, and then moves into his assessment of the current cyberspace strategic landscape.[11] Most of his comments with respect to the strategic landscape relate to the man-made nature of the cyberspace domain, where geographic boundaries are less evident in cyberspace and where the "cyber landscape changes rapidly with the connection of new devices and bandwidth, and with the spread of strong encryption and mobile devices."[12] In addition, GEN Alexander returns to the theme of intellectual property theft which he also discussed at CSIS in 2010. He noted that such theft was becoming increasingly state-sponsored. GEN Alexander stated that "foreign government-directed cyber collection personnel, tools, and organizations are targeting the data of American and western businesses, institutions, and citizens. They are particularly targeting our telecommunications, information technology, financial, security, and energy sectors…which jeopardizes our economic growth."[13] His statements speak to general problems in the cyberspace landscape and could be interpreted as GEN Alexander shifting to an axiomatic understanding of cyberspace. However, continuing to his priorities for USCYBERCOM his testimony firmly asserts a continued commoditized view of the domain, where the chief commodities remain information systems and data.

GEN Alexander's command priorities proceed along five main lines of effort: 1) creating a defensible architecture; 2) global situational awareness; 3) creating a concept operating in cyberspace; 4) developing cyberspace forces; and

11. Keith B. Alexander, *Statement Before the Senate Committee on Armed Services 12 March 2013*, March 12, 2013, p. 2, accessed March 22, 2017, https://www.armed-services.senate.gov/imo/media/doc/Alexander%2003-12-13.pdf.
12. Alexander, *Statement Before the Senate Committee on Armed Services 12 March 2013*, p. 2.
13. Alexander, *Statement Before the Senate Committee on Armed Services 12 March 2013*, p. 3-4.

5) capacity action in cyberspace when authorized.[14] His first line of effort is related specifically to IT systems; GEN Alexander notes that the DoD owns over seven million of them across several thousand enclaves.[15] He presents the linchpin to his defensible architecture as the Joint Information Environment (JIE), which is comprised of a "shared infrastructure, enterprise services, and a single security architecture to improve mission effectiveness, increase security, and realize IT efficiencies."[16] Clearly evidenced by this core effort is a reflection on infrastructure and IT efficiencies, which should notionally be harnessed to create operational effectiveness.

GEN Alexander's other lines of effort continue a commoditized reflection of cyberspace. For example, he links *operational awareness* to situational awareness of networks and links *operating concepts* to blocking malicious traffic that threatens network systems and data.[17] To be clear, GEN Alexander does not claim these goals are an end in themselves. In fact, he acknowledges that USCYBERCOM efforts are enabling functions for better command and control, better intelligence, and better cyberspace capabilities for Combatant Commanders.[18] Taken as a whole, GEN Alexander's testimony to the Senate Armed Services Committee three years after his speech to CSIS continues firmly along a commoditized view of cyberspace.

Senate Hearing: Feb 2014

GEN Alexander's final hearing before the Senate Armed Services Committee (SASC) occurred a month before he retired. In this hearing, GEN Alexander begins with virtually the same opening remarks from his 2013 testimony to the SASC, only deviating from his previous year's content to add an update on the Cyber National Mission Force. Returning to USCYBERCOM's

14. Alexander, *Statement Before the Senate Committee on Armed Services 12 March 2013*, p. 5.
15. Alexander, *Statement Before the Senate Committee on Armed Services 12 March 2013*, p. 5.
16. Alexander, *Statement Before the Senate Committee on Armed Services 12 March 2013*, p. 5.
17. Alexander, *Statement Before the Senate Committee on Armed Services 12 March 2013*, p. 6-7.
18. Alexander, *Statement Before the Senate Committee on Armed Services 12 March 2013*, p. 9.

mission priorities GEN Alexander uses the same description of the Joint Information Environment (JIE), but adds the following amplification: "The JIE, together with the cyber protection teams…will give our leaders the ability to truly defend *our data and systems*."[19] GEN Alexander's amplification underscores his persistent view of cyberspace, in that focal point of the JIE and cyber protection teams are both cyberspace commodities: data and systems.

GEN Alexander concluded his remarks by outlining his operational focus for USCYBERCOM.[20] In his section "Where Are We Going?", GEN Alexander adopts more of an axiomatic tone to cyberspace rather than speaking from a commodity-dominant perspective. GEN Alexander notes that his greatest concern is that USCYBERCOM would not be ready to respond in time to emerging threat, and adds the following observation: "unless Congress moves to enact cybersecurity legislation to enable the private sector to share with the U.S. Government the anomalous cyber threat activity detected on its networks on a real-time basis, we will remain handicapped in our ability to assist the private sector or defend the nation in the event of a real cyber attack."[21] While GEN Alexander's language is necessarily more vague as he pulls the conversation up to the strategic level, his basic understanding of cyberspace as a commodity remains unchanged. For example, the words "cyber threat activity detected on its networks" harkens back to his perspective on securing DoD's information systems through the JIE and National Mission Forces.

Interim Assessment

GEN Alexander retired from almost 40 years of military service on May 28, 2014. Theories of lexical cognition suggest that by this point in his career, GEN Alexander's commoditized understanding of cyberspace should be firmly

19. Keith B. Alexander, *Statement Before the Senate Committee on Armed Services 27 February 2014*, February 27, 2014, p. 4. My emphasis. Accessed March 22, 2017, https://www.armed-services.senate.gov/imo/media/doc/Alexander_02-27-14.pdf.
20. Alexander, *Statement Before the Senate Committee on Armed Services 27 February 2014*, p. 7.
21. Alexander, *Statement Before the Senate Committee on Armed Services 27 February 2014*, p. 7.

ensconced. GEN Alexander was serving as DIRNSA even before being dual-hatted as the Commander of USCYBERCOM, and his public statements remain consistently fixed on a version of cyberspace that provides much-needed commodities to Combatant Commanders and war planners alike. This does not mean that his understanding *cannot* change over time, but rather that it should take a considerable period of time or a significant event to force a paradigm shift.

We can also note specific *behavior* by GEN Alexander which is consistent with how discourse and frames interact to shape a person's actions. One of the most evident impacts of this would be his shaping of the three USCYBERCOM core missions, which GEN Alexander established prior to his departure and which remain in effect to this day: 1) defend the Defense Department information networks; 2) support combatant commanders; and 3) when directed by the president or secretary of defense, to protect U.S. critical infrastructure from attacks of significant consequence.[22] Even a cursory examination of each core mission reveals GEN Alexander's influence, which remains consistent with his understanding of cyberspace even before he took command of USCYBERCOM.[23]

To this day, GEN Alexander is a prominent public figure whose expertise and advice are sought by the U.S. Congress, think tanks, and many professional organizations. Taken as a whole, the lexical theory predicts a strong correlation in GEN Alexander's future lexical choice to the words and discourse he used for over a decade. We would expect to see continued evidence of his commoditized understanding of cyberspace, rather than an understanding that is axiomatic, utilitarian, or perspective dependent. Surprisingly, this is not the case.

22. Antoinette Smith, "Cyberwarfare: What are we doing today?," U.S. Air Force, September 20, 2016, Quoting Lt. Gen. J. Kevin McLaughlin, Deputy Commander of U.S. Cyber Command, accessed March 23, 2017, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/949919/cyberwarfare-what-are- we-doing-today.aspx.
23. Antoinette Smith's full article provides Lt Gen McLaughlin's clarifying statement: "with forces assigned to support all combatant commands, they have the ability to *protect critical data* and provide full spectrum (both offense and defense) cyber capabilities to joint forces."

RSA Security Conference, May 2015

The RSA Security Conference hosts an annual gathering of over 45,000 attendees, making it one of the world's largest cybersecurity events.[24] In May of 2015, GEN (Ret.) Alexander was invited to be a guest speaker to share his insights and experiences since leaving the NSA and USCYBERCOM, along with how those experiences have played out in starting his company, IronNet. Of the discussion between GEN (Ret.) Alexander and the moderator, Ted Schlein, the elements which provide the most direct linkage to cyberspace are: 1) GEN (Ret.) Alexander's answers in response to the moderator regarding the top five best nation-states in cyberspace; 2) his discussion on the proper balance of offensive vs. defensive capability in cyberspace; and 3) his discussion about IronNet.

First, to Mr. Schlein's question: "can you give us the quick run-down, kind of in order…one through five, of the nation states which have the best cyber capabilities that we as a country should be aware of?"[25] At no point in the ensuing discussion about cyber attacks and tiers of nation states did GEN (Ret.) Alexander use lexicons consistent with a commoditized understanding of cyberspace. In fact, GEN (Ret.) Alexander took a more axiomatic approach with respect to recent evolutions within cyberspace:

> …it shows that with the changing rate of technology, that an actor who was not even on the map five or six years ago can, with just technology and their dealings with other countries, can grow very quickly…countries are using cyber as a bridge between diplomatic, military, and economic ways of pressuring other countries. If you put sanctions on Iran and Russia, they have now a new vehicle to respond and they can be completely obvious or they can be very hard to attribute, but they can still push back.[26]

In this dialog GEN (Ret.) Alexander takes an axiomatic approach, not focusing on data and information systems, which were previously his dominant themes, but instead on geo-politics and attribution. Here, technology within cyberspace is a

24. "RSA Conference: About," accessed March 23, 2017, http://www.rsaconference.com/events/us17/about.
25. Keith B. Alexander, *General Alexander: Life After the NSA*, in collab. with RSA 2015 (May 5, 2015), timestamp 22:20. Accessed March 23, 2017, https://www.youtube.com/watch?v=DWR9mJu15qo.
26. Alexander, *Life After the NSA*, timestamps 23:50 & 24:15.

secondary aspect and the real discussion is about how various countries fit cyberspace capabilities into a larger portfolio of political response options.

Next, in response to a prompt about the right balance between offensive and defensive capabilities for the U.S., GEN (Ret.) Alexander does not speak using his former terms of creating network capability, but rather as cyberspace tools as an instrument of policy. He notes that

> …[cyber] offense is a policy decision. You want to have the offensive capability on your toolbox; you gotta have that. Those are the kinds of things that, when developing Cyber Command, [were] our thoughts…to create the toolbox so that the policy makers had the tools to do what they needed to do to protect the nation. The really interesting part, if we were to put that on the table, is that [policy makers] don't know how to use the toolbox yet.[27]

Again, his lexical approach to cyberspace is presented terms which are much more axiomatic. The metaphor of a toolbox could fit equally well in a discussion of capabilities available through the air, land, or sea domains, and reflects an axiomatic approach to cyberspace rather than a commoditized one.

Finally, Mr. Schlein questioned GEN (Ret.) Alexander about his motivations behind starting his new company, IronNet.[28] GEN (Ret.) Alexander outlined his foundational hypothesis, that only groups of companies working together could defend their networks in cyberspace because no one company working alone would be up to the task.[29] He went on to reflect on his experience in the DoD and arrived at the conclusion that when he was still serving on Active Duty, one of the biggest problems was a lack of situational awareness on networks. GEN (Ret.) Alexander concluded with "how do you provide the CISO and IT people a real way of seeing the network that's at network speed? You need a way of detecting when entities within the network change behavior."[30] His conclusion sets up the ensuing utilitarian discussion.

IronNet's product is based on network heuristics and analytics, which "helps fuse an industry consortium" to provide collective defense, collective

27. Alexander, *Life After the NSA*, timestamp 25:55.
28. Alexander, *Life After the NSA*, timestamp 28:10.
29. Alexander, *Life After the NSA*, timestamp 30:34.
30. Alexander, *Life After the NSA*, timestamp 31:10.

security, and "fundamentally change the way the world does cyber."[31] From this point in the presentation, until questions and answers from the audience, GEN (Ret.) Alexander discusses cyberspace within the utilitarian perspective of IronNet's contribution to cyber security and the various services they provide.[32] The language he uses in the latter part of his presentation shifts from being axiomatic to being utilitarian.[33]

Given the theory of lexical cognition, GEN (Ret.) Alexander's speech at RSA is somewhat surprising. He would be expected to *continue* his ten-year trend of discussing cyberspace in purely commoditized terms. Instead, he spends most of the presentation speaking in predominantly axiomatic or utilitarian terms.

Senate Hearings: Nov 2015

Six months after his speech to RSA, GEN (Ret.) Alexander was asked to appear as a witness before the Senate Armed Services Committee and present his perspective regarding the future of warfare. It was at this hearing that GEN (Ret.) Alexander made his much-quoted declaration that "the theft of intellectual property…represents the single greatest transfer of wealth in history."[34] In this speech, he only makes mention of "data" three times, and in two of those references data was not the focal point but rather a modifier for a larger concept such as "consumer data," or the advantage of big data when coupled with nanotechnology.[35] In addition, GEN (Ret.) Alexander makes no mention of information technology, information systems, or any variant thereof.

His entire testimony takes on a more *axiomatic* tone, focusing on the links between cyberspace and terrorism, nation-state attacks, and the need for better

31. "IronNet Cybersecurity," accessed March 24, 2017, https://ironnetcyber.com/.
32. Specific services include: heuristics, big data, breach mitigation, and security reference architectures.
33. Recall, a utilitarian perspective is also the dominant perspective in the cyber security industry at large.
34. Keith B. Alexander, *Statement Before the Senate Committee on Armed Services November 3, 2015*, Washington, D.C., November 3, 2015, p. 3. Accessed March 25, 2017, https://www.armed-services.senate.gov/imo/media/doc/Alexander_11-03-15.pdf.
35. Alexander, *Statement Before the Senate Committee on Armed Services November 3, 2015*, p. 3.

public-private partnerships in a national approach towards cyber security. This shift in language comes in surprising contrast to his 2013 testimony, where data appeared 16 times and IT or information systems were relevant components of his testimony. In particular, with respect to nation-state attacks, GEN Alexander stated that "commercial and private entities cannot defend themselves alone against nation-state attacks nor nation-state-like attacks in cyberspace. We do not want them to 'fire' back. The U.S. Government is the only one that can and should 'fire' back…it is the Government's job to defend this country in cyberspace from…destructive attacks."[36]

Speech at CYCON: Dec 2016

Finally, in December of 2016, the U.S. Army Cyber Institute invited GEN (Ret.) Alexander to be the keynote speaker at CYCON U.S. 2016.[37] As with the senate hearing in Nov. 2015, GEN (Ret.) Alexander uses a lexical framework with discussing cyberspace that is axiomatic. For example, when discussing the likelihood of warfare adapting characteristically to cyberspace, he briefly describes the evolution of thought and technology beginning in the year 1830 and ends with the present impact of the Internet.[38] "[N]ow we look at the Internet, and we think about how important it is to us as a nation, and to our allies, to the world who are all connected. And it's where our intellectual property, our government, the way we vote, <pause> our wealth, our children's data…all of us now are in that environment."[39] GEN (Ret.) Alexander's main thrust is tangential to cyberspace and not focused on cyberspace commodities. Nor does he attempt to either reify cyberspace, concluding simply that cyberspace "will be used against us in warfare. Period. We can say we don't want

36. Alexander, *Statement Before the Senate Committee on Armed Services November 3, 2015*, p. 4.
37. Keith B. Alexander, *Keynote Address by Keith Alexander*, in collab. with Army Cyber Institute (December 20, 2016), accessed March 25, 2017, https://www.youtube.com/watch?v=StiCssdBzVE.
38. Alexander, *Keynote CYCON 16*, timestamp 12:00.
39. Alexander, *Keynote CYCON 16*, timestamp 13:30.

it. We can make up all the rules. But those who wish us harm, or our allies, will use this as a form of warfare."[40]

Throughout his keynote address, GEN (Ret.) Alexander discussed a variety of other themes in equally axiomatic terms. He discussed how public companies will defend themselves in cyberspace, the state of interconnectedness in modern society, information sharing, moving beyond incident response into a more proactive posture, the DoD's role in defending the nation in cyberspace, and the need for government to remain publicly accountable. In multiple instances GEN (Ret.) Alexander could have used a lexical framework holding to a commoditized view of cyberspace, which would have been in line with his previous statements. Instead, his perspective at CYCON 2016 was primarily axiomatic.

Summary: GEN Alexander

Conventional wisdom holds that GEN Alexander should have continued his discourse along the same lines of thinking and using the same lexical framework he maintained during his time on active duty. It turns out that for GEN Alexander this is not the case, and that theory of lexical cognition failed. Rather than being language bound, the evidence so far suggests GEN Alexander may be institutionally, contextually, or thought bound. With respect to the RSA 2015 event, one could dispute trying to read too much into his intent, given the RSA venue and his leadership role in IronNet; that criticism is more than fair. However, this does not account for a complete absence of any discussion regarding data, information systems, and other cyberspace commodities when those were dominant elements in his public presentations for more than five years before he retired.

According to the textual analysis above, when GEN Alexander retired from the DoD, he stopped understanding cyberspace in terms forms of commodities and began to see the domain more axiomatically. On the surface, the evidence so

40. Alexander, *Keynote CYCON 16*, timestamp 14:20.

far suggests that organizations and institutional variances have more to do with shaping frames and action than does language and discourse. Is GEN Alexander a special case? How does lexical cognition hold up against an institution as old and as structured as the U.S. Congress?

U.S. Congress

This empirical analysis of the U.S. Congress focuses on the House Armed Services Committee (HASC), beginning in 2005 with the 109th Congress. There are two main reasons for this approach: First, it was the 109th Congress which first formed the Unconventional Threats and Capabilities Subcommittee (UTC) under the HASC, which was given charge of "information technology and programs" along with other matters relating to terrorism. The UTC's full committee jurisdiction included a wide range of activities:

> Special Operations Forces; counter-proliferation and counter-terrorism programs and initiatives; science and technology policy and programs; information technology programs; homeland defense and Department of Defense-related consequence management programs; related intelligence support; and other enabling programs and activities to include cyber operations, strategic communications, and information operations.[41]

The HASC renamed the UTC several times from the 109th to the 114th Congress, so unless otherwise specified this section will use the name "threats and capabilities subcommittee" when referring to the subcommittee as a whole as it existed from the 109th Congress to the present day. The threats and capabilities subcommittee provides a test case that is sufficient in size and scope for a detailed analysis of how perspectives change over time.[42]

Second, the U.S. House of Representatives has a fairly high degree of turnover compared to other chambers of government. The House operates on a

41. U.S. Congress, *H. Rept. 112-123: First Semiannual Report of the Activities of the Committee on Armed Services for the One Hundred Twelfth Congress*, House Report H. Rept. 112-123 (Washington, D.C.: U.S. House of Representatives, January 24, 2011), p. 18. Accessed March 27, 2017, https://www.congress.gov/112/crpt/hrpt123/CRPT-112hrpt123.pdf.
42. The 109th Congress was also elected into the office the year before Apple introduced the first iPhone, which demonstrates how fast our national understanding and integration with cyberspace has evolved since 2005.

two-year cycle set forth by the U.S. Constitution, and members rotate through committees based on things like seniority, a central steering committee, and party loyalty. Of the 22 members elected to the UTC subcommittee in 2005, only five were assigned to the Emerging Threats and Capabilities subcommittee during the 114th Congress and only one, Mr. Kline, served during every congressional cycle.[43] Additionally, members of congress elected to the UTC have come from diverse backgrounds all across America. Since the threats and capabilities subcommittee has a significant degree of turnover between congressional cycles, we can be reasonably sure that if lexical cognition holds true, then we will *not* observe a consistent view of cyberspace emerging over time. Rather, we would expect that the language used in producing their main legislative products will shift among the four taxonomies in conjunction with the ebb and flow of congressional cycles.

As with GEN Alexander, this analysis will be a textual survey and will focus on the two main products that the U/ETC help produce: the National Defense Authorization Act (NDAA) and their Annual Reports to Congress.[44] The NDAA is an authorization bill and Committee Reports to the Congress are simply formal reports. Unlike GEN Alexander's personal speeches, both of these products tend to be much more specific—especially the NDAA, which is written to ultimately become law. The NDAA is written predominantly by the House Legislative Council, or by professional writers in consultation with the Legislative Council, to reflect the desires of elected members of congress. This degree of precision reflected in the NDAA and in the annual report to the Congress allows for a more straightforward assessment.

43. The members were: Mr. WILSON, Mr. KLINE, Mr. SHUSTER, Mr. LANGEVIN, and Mr. COOPER. The UTC was renamed the Emerging Threats and Capabilities (ETC) subcommittee during the 112th Congress

44. From the 109th Congress to the 114th Congress, the rules of the U.S. House of Representatives changed several times. The 109th Congress simply required a single report on the activities of the major committees that encompassed the full two-year congressional cycle. The 112th Congress changed the rules and required four semiannual reports, which was redefined to two annual reports for the 113th Congress. The 114th Congress completed the circle by returning to a single "Report on the Activities," required once per congressional cycle.

109th Congress

Beginning with the 109th Congress, the HASC delegated full charge of overseeing and directing cyberspace-related functions to a single subcommittee. Moving a specific portfolio to subcommittee's jurisdiction is one of the ways Congress ensures that the portfolio is afforded adequate attention. If a specific committee is not delegated to a subcommittee, then it remains under the purview of the full committee where it may or may not come up during the congressional cycle.

During the 109th Congress, the Chairman for the UTC was Mr. Saxton, who worked with Ranking Member Abercrombie to run the subcommittee. The UTC was responsible for "Special Operations Forces, the Defense Advanced Research Projects Agency, information technology and programs, force protection policy and oversight, and related intelligence support."[45] In 2005, the terms "cyber" and "cyberspace" were still fairly nascent in congressional circles, so analysis into the Report on the Activities of the HASC as well as the NDAA begins with ideas surrounding cyberspace to see how the Congress was discussing either the technology, the capabilities inherent within the domain, utilitarian functions. Concepts such as communication, networks, data, information, and technology serve as useful indicators around which to construct an initial search.

Neither the NDAA for Fiscal Year (FY) 2006 nor the NDAA for FY 2007 use the terms cyber or cyberspace. Information technology is only mentioned once in the 2006 version when referring to a "pilot program for best-value source selection for performance of information technology services."[46] In the FY 2007 NDAA, information technology (IT) is mentioned 12 times and over a wide range of topics. In each of these twelve cases, the focus of IT is the technology itself; IT

45. U.S. Congress, *H. Rept. 109-731: Report of the Activities of the Committee on Armed Services for the One Hundred Ninth Congress*, House Report H. Rept. 109-731 (Washington, D.C.: U.S. House of Representatives, December 15, 2006), accessed March 26, 2017, https://www.congress.gov/congressional-report/109th-congress/house-report/731/.
46. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2006*, January 6, 2006, p. 65. Accessed March 3, 2017, https://www.congress.gov/.

is not used as a pseudonym for what could be "cyberspace" as we understand it today. Section 1207, for example, authorizes the military to provide a wide range of educational material to foreign personnel for the purpose of training.[47] The term "information systems" is absent from the FY 2007 NDAA, but is mentioned twice in 2006, where both refer to the same provision, Section 806. That section relates to major acquisition programs and requiring "congressional notification of cancellation of major automated information systems."[48] The term "data" occurs 61 times between the 2006 and 2007 NDAA, and never refers to data residing on a computer, information system, or storage device. Rather, "data" is used in the traditional sense referring to elements such as data links, technical data for weapon systems, and data (information) regarding aircraft carriers.

The HASC Report to the 109th Congress uses the term IT only one time, and it refers to "the transfer of learning content and IT [being] subject to the Arms Control Act."[49] Terms such as "information systems" and "data," on the other hand, do not appear in the report. However, the annual report does mention "cyber-security" and "cyber attacks" one time each, though neither was used in referring to the cyberspace domain. In the first instance, cyber-security is nested within a long list of briefing requirements related to military applications of nuclear energy. The report notes that in addition to budget hearings, "the committee received several briefings on topics relating to the nuclear weapons complex…physical security concerns and cyber-security practices."[50] Finally, the Subcommittee on Strategic Forces included a provision in the annual report that subcommittee briefings included "adversarial information operations and *cyber attacks* as part of a threat-based defense review to complement the DOD's ongoing, capabilities-based Quadrennial Defense Review (QDR)."[51]

47. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2007*, October 17, 2006, p. 337. Accessed March 3, 2017, https://www.congress.gov/.
48. U.S. Congress, *NDAA for FY06*, p. 231.
49. U.S. Congress, *H. Rept. 109-731*, p. 31.
50. U.S. Congress, *H. Rept. 109-731*, p. 30.
51. U.S. Congress, *H. Rept. 109-731*, p. 68.

In summary, these documents suggest that the 109th Congress rarely acknowledged or paid much attention to cyberspace. They were concerned with acquisition programs, technical data, and technology transfers, but with nothing that signals an acknowledgment of the cyberspace domain or a particular understanding thereof. In fact, both mentions of "cyber," came from subcommittee hearings other than the threats and capabilities subcommittee, where cyber security and cyber attacks were tangential elements of the brief. In terms of a taxonomy, taxonomical observations regarding the 109th Congress are inconclusive. Ample evidence to suggest that cyberspace was, at most, on the far periphery of their understanding, but there is simply insufficient data to build a clear taxonomical assessment.

110th Congress

In the 110th Congress, the HASC renamed the UTC to include "terrorism"; the committee would now be called the Subcommittee on Terrorism, Unconventional Threats and Capabilities (TUTC). The Chairman of the TUTC subcommittee for the 110th Congress was Mr. Adam Smith, who was elected along with Ranking Member "Mac" Thornberry to oversee the subcommittee. Roles and responsibilities for the TUTC remained largely the same as the 109th Congress, with two additions. "Science and technology policy" and "homeland defense and consequence management programs within the committee's jurisdiction" were both added to the existing subcommittee roles.

The 110th Congress passed the 2008 and 2009 NDAAs during the 2007-2008 congressional cycle. Neither NDAA mentions the word cyberspace, but "cyber" begins to emerge during the FY 2008 NDAA. The occurrence of the term "cyberspace" was used to modify the FY 2000 NDAA to change an annual DoD report on Chinese national defense capabilities. Congress amended the FY 2000 NDAA "by adding at the end the following new paragraph: 'Developments in China's asymmetric capabilities, including efforts to acquire, develop, and deploy

cyberwarfare capabilities.'"[52] Three additional mentions of "cyber" were all linked to security risks to the nuclear weapons complex, where the term appeared in tandem with general security "to address the physical and cyber security threats" at individual nuclear sites.[53] Finally, section 1804 of the 2008 NDAA requires the Secretary of Defense to deliver a report to Congress detailing a potential response to a wide variety of scenarios:

> The plan shall provide for response to the following hazards: Nuclear detonation, biological attack, biological disease outbreak/pandemic flu, the plague, chemical attack-blister agent, chemical attack-toxic industrial chemicals, chemical attack-nerve agent, chemical attack-chlorine tank explosion, major hurricane, major earthquake, radiological attack-radiological dispersal device, explosives attack-bombing using improvised explosive device, biological attack-food contamination, biological attack-foreign animal disease and cyber attack.[54]

Instead of providing a framework of "nuclear, biological, chemical, and natural disaster," the Congress explicitly spelled out four types of chemical attack, four types of biological attacks, a plague, etc. Then, to top off the list, the HASC tosses in "cyber attack."

Both NDAAs discussed the terms "information technology" and "information system," which occur 76 times across a wide range of usage such as "IT investment," "IT services," "information systems networks." Also, the Congress acknowledged the Department of Defense (DoD) would need to turn to the private sector to begin bridging the technology gap that had opened between industry and the government. To that end, Section 881 required the DoD to establish a clearinghouse which aimed to enhance "internal data and communications systems of the [DoD] for sharing and retaining information regarding commercial technology priorities and needs, technologies available to meet such priorities and needs, and ongoing research and development directed toward gaps in such technologies."[55] Section 881 is one of the first instances

52. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2008*, January 28, 2008, p. 405. Accessed March 3, 2017, https://www.congress.gov/.
53. U.S. Congress, *NDAA for FY08*, p. 578.
54. U.S. Congress, *NDAA for FY08*, p. 497.
55. U.S. Congress, *NDAA for FY08*, p. 261.

where the HASC acknowledged the widening gap of technological sophistication within the private sector compared to the DoD. That specific direction carried with it a tacit understanding of how cyberspace was beginning to transform commercial industry and potentially other countries' military capabilities, which created a change in the security environment DoD was directed to respond to.

During the 110th Congress, the House Armed Services Committee (HASC) also used its annual report to the house to highlight the fact that DoD needed to adapt to a changing context with respect to cyberspace. They noted that "during a dedicated hearing on June 20, 2007, the [TUTC] became aware of significant confusion surrounding the roles and missions of the military services, particularly with respect to the development and employment of capabilities such as unmanned aerial systems, tactical airlift, *and cyberwarfare*."[56] The term "cyber" appeared six times in H. Rep. 110-942, where "cyber" was used to discuss cybersecurity threats to the U.S. nuclear enterprise as well as "cybersecurity enabling network centric operations."[57]

Another "first" for the HASC during the 110th Congress was the way in which the term 'data' was presented. In prior house reports and NDAAs, the term "data" was simply a convenient euphemism for "information regarding," as seen in aforementioned instances such as "technical data for weapon systems." However, in H. Rep. 110-942, the term "data" is also used to in a more contemporary sense to refer to computer data. For example, the HASC took action on several issues "as a result of holding hearings and briefings on bandwidth and large data management."[58] The notion that warfare would also be fought by leveraging the cyberspace domain was beginning to catch hold in the HASC.

---

56. U.S. Congress, *H. Rept. 110-942: Report of the Activities of the Committee on Armed Services for the One Hundred Tenth Congress*, House Report H. Rept. 110-942 (Washington, D.C.: U.S. House of Representatives, January 3, 2009), p. 66. My emphasis. Accessed March 27, 2017, https://www.congress.gov/110/crpt/hrpt942/CRPT-110hrpt942.pdf.
57. U.S. Congress, *H. Rept. 110-942*, p. 152.
58. U.S. Congress, *H. Rept. 110-942*, p. 109.

The most attention given to cyberspace as a distinct domain came during a hearing from the TUTC on April 1st, 2008, at a hearing titled "Holistic Approaches to Cybersecurity Enabling Network-Centric Operations." As part of his opening remarks, Ranking Member Thornberry expressed the need for a more holistic look at cyberspace when he noted that "cyber issues are indicative of some of the future security issues we are all going to face…[The TUTC] has spent a fair amount of time looking at information technology the Pentagon was trying to procure, including information assurance. We have gotten to the point where I believe cyber is a domain of warfare and, therefore, deserving of our attention."[59] Witnesses at the hearing were asked to testify primarily about network-centric warfare, intellectual property theft, and international competitors such as China and Russia. To that end, most follow-on questions from members of the subcommittee were oriented at understanding the nature of what they perceived would be potential warfare in cyberspace.

In summary, the two NDAAs and the house report produced by the 110th Congress show that the Congress was beginning to pay attention to notions of a cyberspace domain. Whereas previously the HASC, through the threats and capabilities (TC) subcommittee, was generally concerned with computer programs and information technology as support elements, they were also beginning to see cyberspace as distinctive. Accordingly, the TC began holding hearings to receive testimony from think tanks and defense experts alike. Cyberspace was acknowledged to require specific oversight, or at least attention, but it was not a priority of congressional governance overall. Based on the way the HASC and the TC were beginning to discuss cyberspace, my assessment of their perspective on cyberspace at this juncture is *axiomatic*.

---

59. U.S. Congress, *UTC Hearing: Holistic Approaches to Cybersecurity Enabling Network-Centric Operations*, House Report (Washington, D.C.: U.S. House of Representatives, April 1, 2008), accessed March 31, 2017, https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg45255/html/CHRG-110hhrg45255.htm.

111th Congress

The HASC only made minor changes to the Subcommittee on Terrorism, Unconventional Threats and Capabilities (TUTC) subcommittee during the 111th Congress. Adam Smith continued to chair the subcommittee in 2009, before resigning and being replaced by Ms. Sanchez; HASC Republicans elected Mr. Miller to be the ranking member.[60] The TUTC jurisdiction was virtually unchanged.[61] During this period, the DoD released the 2010 Quadrennial Defense Review, which specifically addressed DoD's intent to organize, train, and equip forces to operate in the cyberspace domain in concert with more traditional warfighting domains.[62] Of note, U.S. Cyber Command also stood up on June 3rd, 2010, which became a focus area for congressional oversight during the FY 2011 NDAA.

The 111th Congress, through the HASC, wrote and passed the NDAAs for FY 2010 and FY 2011. When compared to the 110th Congress, two observations stand out with respect to cyberspace. The first is simply the number of times "cyber" is mentioned in the FY 2010 and 2011 NDAAs compared with the past two years. In the previous congressional cycle, the HASC used the term "cyber" just four times, and only in the FY 2008 NDAA; three of those were in the same subsection.[63] In contrast, the 111th Congress referred to "cyber" *115 times*, with great interest on "cyber warfare capabilities," "cyber events," "cyber attack," and "cyber operations personnel." Additionally, "information technology" or "information systems" appear 113 times in the legislation proposed by the 111th

60. U.S. Congress, *H. Rept. 111-710: Report of the Activities of the Committee on Armed Services for the One Hundred Eleventh Congress*, House Report H. Rept. 111-710 (Washington, D.C.: U.S. House of Representatives, January 3, 2011), p. 23. Accessed March 27, 2017, https://www.congress.gov/111/crpt/hrpt710/CRPT-111hrpt710.pdf.
61. Unchanged other than to remove "and oversight," from their "force protection policy" function—ostensibly because the subcommittee exercised an oversight function by default and so the HASC found the description redundant.
62. The publication date was February 1st, 2010. See Department of Defense, *Quadrennial Defense Review Report: 2010*, February 2010, accessed March 27, 2017, https: //www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf
63. Section 3123, pg. 578.

Congress, an increase of roughly 25 percent over the previous congressional cycle.

Two exemplars typify how the HASC understood cyberspace during the 2009–1010 cycle. The first occurs in Section 931 of the FY 2011 NDAA, where the HASC mandated a "strategy for organizing the research and development bodies of the DoD to develop leap-ahead cyber operations capabilities."[64] In clarifying what they meant by "cyber operations capabilities," the HASC noted that it referred to "the range of capabilities needed for computer network defense, computer network attack, and computer network exploitations…including technical as well as non-materiel solutions."[65] In Section 931, *Computer networks* was one of their primary considerations. The second occurs in Section 935 of the same NDAA, where the 111th Congress asked the DoD to report on any DoD progress to defend the department itself along with the defense industrial base.[66] In this section, the Congress requested a comparative assessment of the degree of dependency on cyberspace of "potential United States adversaries, nations with advanced cyber warfare capabilities, and the United States on networks that can be attacked through cyberspace."[67] Here again, the computer networks emerge as the primary consideration in a cyberspace attack.

In summary, the two NDAAs produced by the 111th Congress' House Armed Services Committee (HASC) demonstrate that cyberspace was gaining increasing attention. The Congress began to see cyberspace not only as a distinct phenomenon but also as a warfighting domain. Accordingly, the Threats and Capabilities subcommittee began holding hearings to discuss the impact of cyberspace on U.S. power projection, DoD and industrial base networks, and network warfare. In general, the lexical choice of Congress when discussing cyberspace, as evidenced in the Report to the House and in the two NDAAs still

64. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2011*, January 7, 2011, p. 244, accessed March 3, 2017, https://www.congress.gov/.
65. U.S. Congress, *NDAA for FY11*, p. 245.
66. U.S. Congress, *NDAA for FY11*, p. 204.
67. U.S. Congress, *NDAA for FY11*, p. 204.

takes an *axiomatic* approach. However, the HASC, and especially the Threats and Capabilities subcommittee, tends to depart from an axiomatic understanding and use a commoditized framework when they discuss cyber warfare or cyber capabilities. Limited evidence suggests that the more they think hard about cyberspace, the more they resort to *commoditized* language.

112th Congress

During the 112th Congress, elected to the 2011–2012 congressional cycle, the HASC renamed the threats and capabilities subcommittee to the Subcommittee on Emerging Threats and Capabilities (ETC). The ETC's rules of jurisdiction also changed rather significantly; the ETC now had oversight and governance over:

> Defense-wide and joint enabling activities and programs to include: Special Operations Forces; counter-proliferation and counter-terrorism programs and initiatives; science and technology policy and programs; information technology programs; homeland defense and Department of Defense-related consequence management programs; related intelligence support; and other enabling programs and activities to include *cyber operations*, strategic communications, and *information operations*.[68]

Mr. Thornberry of TX was elected as the subcommittee Chair, working in concert with the Ranking Member Jim Langevin of RI. Consistent with the U.S. House jurisdictional rules, which now specifically highlighted cyberspace operations, the subcommittee would continue paying more and more attention to cyberspace.

The 112th Congress enacted two provisions during their congressional cycle which underscores a continued affirmation of cyberspace as a distinct domain. The first was under Section 954 of the FY 2012 National Defense Authorization Act (NDAA), where the HASC affirmed that "that the [DoD] has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests."[69] This provision was made subject to the same legal structure that governed kinetic capabilities, as

68. U.S. Congress, *H. Rept. 111-710*, p. 17. My Emphasis.
69. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2012*, December 31, 2011, p. 255, accessed March 3, 2017, https://www.congress.gov/.

well as the War Powers Resolution. The second was in the FY 2013 NDAA, where the HASC for the first time committed an entire Subtitle to "Cyberspace-Related Matters."[70] Subtitle D encapsulated Sections 931 through 956, and included everything from the "next-generation host-based cyber security system," to "collection and analysis of network data flow," to newly-mandated "quarterly cyber operations briefings."[71]

Section 940 of the FY 2013 NDAA also included a Sense of Congress on U.S. Cyber Command. Sense of Congress language is important to DoD in that, while short of creating a law, it provides the DoD an unambiguous perspective from the Legislature on where they think the DoD should focus their attention.[72] In particular, the Congress noted that "there is a serious cyber threat to the national security of the United States and the need to work both offensively and defensively to protect the networks and critical infrastructure of the United States."[73] Section 940 lays out a perspective that U.S. Cyber Command, whose primary focus is the cyberspace domain, has the primary responsibility to protect networks and infrastructure.

Another instance in the FY 2013 NDAA which elucidates the 112th Congress perspective of cyberspace occurs in Section 244, which requires a report on cyber and IT investments for the U.S. Air Force.[74] Specifically, the USAF was asked to submit a report on its investment strategy with respect to "cyber science and technology," and include "near-, mid-, and far-term science and technology priorities of the Air Force with respect to cyber and

70. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2013*, January 2, 2013, p. 11. Accessed March 3, 2017, https://www.congress.gov/.
71. U.S. Congress, *NDAA for FY13*, p. 11-12.
72. Article1, Section 8, of the U.S. Constitution gives the Legislature sole authority over creating and maintaining the U.S. Armed Forces. In this light, Sense of Congress language is a means by which the Legislature can exercise their oversight role and still allow the DoD some latitude to follow Congressional direction without incurring a legal burden. To that end, the DoD is always responsive to SoC language in the NDAA and in acting on SoC language with the same energy determination as though it were, in fact, law. This is partly because the Congress can always come back in a later year and write more onerous legislation if they deem the military to be shirking. The DoD ignores SoC language to its peril.
73. U.S. Congress, *NDAA for FY13*, p. 259.
74. U.S. Congress, *NDAA for FY13*, p. 57.

information-related technologies and the resources…projected to address these priorities. [Additionally, provide] strategy to transition the results of the science and technology priorities into weapon systems, including cyber tools."[75] The Congress' focus within the cyber portfolio as seen here was concentrated on IT and tools.

In the FY 2012 NDAA, the HASC also enacted a pilot program that demonstrates an expanded view of "computer and network data" than was discussed by the 110th Congress. Under this pilot program, the Under Secretary of Defense for Intelligence was directed to "demonstrate a [network] enterprise-wide query and correlation capability through the Defense Intelligence Information Enterprise program."[76] According to the Section 945, the purpose of the program was to demonstrate whether or not DoD had the capability for enterprise-wide data correlation across multiple users, multiple sites, and a large volume of data. Specifically, the HASC mandated that the demonstration support "complex, simultaneous queries by a large number of users and analysts across numerous, large distributed data stores with response times measured in seconds."[77] In Section 945, Congress is trying to develop an understanding of DoD's capability to deal with "big data," a capability inherent in the modern context of cyberspace.[78] Section 945 demonstrates the next iteration of the Congress's conception of data within cyberspace, which shifted from simple "small data environment" to a more modern comprehension.[79]

In addition, the 112th Congress used the term "data," as it relates to a cyber-based information commodity, with remarkable frequency during this cycle compared to previous years. One can just follow the term "data center" juxtaposed with "data link," beginning at the 109th Congress to observe how

75. U.S. Congress, *NDAA for FY13*, p. 57.
76. U.S. Congress, *NDAA for FY12*, p. 244. Note also the relationship of *Information Enterprise* to cyberspace at large.
77. U.S. Congress, *NDAA for FY12*, p. 254.
78. For a more thorough exposition of "Big Data," see Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Mariner Books, 2014).
79. Mayer-Schönberger and Cukier, *Big Data*, p. 13-14.

congressional concern for data links—a mainstay of congressional concern for two decades due to its impact on complex modern battlefields—was eclipsed by data centers. During the 109th Congress, data links were mentioned eleven times, whereas "data center" was never mentioned either in the NDAA or in the HASC Report to the House; the same holds true for the 110th Congress. However, in the 112th Congress data center and data links were *both* mentioned 23 times. By the 113th Congress, "data link" only appears 9 times across both NDAAs, and exclusively within funding tables at the end of the authorization bill. Data centers, on the other hand, were referenced 39 times during the 113th Congress and mostly within the text of the legislation.

Mentions of cyberspace elements throughout the 112th Congress increasingly married congressional understanding of cyberspace to information technology (IT). From a purely numerical perspective, the rates of occurrence for the term "cyber," just between 111th and 112th Congressional cycles, is telling. In the 111th Congress, the House Armed Services Committee (HASC) used the term cyber 39 times, whereas their use jumps over 300% during the next two years to 127 times. With respect to the way in which the HASC, or more specifically the ETC, understood cyberspace, the second semi-annual report to the House is telling. During this cycle, the ETC committee "devoted substantial attention to cyber operations and information technology" to ensure the DoD "defends its networks."[80] Furthermore, the HASC reported that they had "included several legislative provisions related to information technology [and] cybersecurity…in H.R. 4310."[81]

80. U.S. Congress, *H. Rept. 112-359: Second Semiannual Report of the Activities of the Committee on Armed Services for the One Hundred Twelfth Congress*, House Report H. Rept. 112-359 (Washington, D.C.: U.S. House of Representatives, December 30, 2011), p. 86, accessed March 27, 2017, https://www.congress.gov/112/crpt/hrpt359/CRPT-112hrpt359.pdf.
81. H.R. 4310 was the FY 2013 NDAA. See U.S. Congress, *H. Rept. 112-744: Fourth Semiannual Report of the Activities of the Committee on Armed Services for the One Hundred Twelfth Congress*, House Report H. Rept. 112-744 (Washington, D.C.: U.S. House ofRepresentatives, June 29, 2012), p. 124. Accessed March 27, 2017, https://www.congress.gov/112/crpt/hrpt744/CRPT-112hrpt744.pdf

In summary, the 112th Congress spent considerable energy discussing cyberspace and various functions within the domain. Their lexical use when discussing cyberspace writ large also shifted to a firmly *commoditized* understanding of the domain and its technological manifestations. Taken as a whole, the ends for which cyberspace operations occur, as understood by the 112th Congress, was to protect networks and infrastructure.[82]

113th Congress

During the 113th Congress, the HASC made one change to the Threats and Capabilities subcommittee jurisdiction, which was to also grant the subcommittee oversight over intelligence policy. According to the new jurisdictional rules, the subcommittee on Intelligence, Emerging Threats and Capabilities (IETC) would now be responsible for "intelligence policy…national intelligence programs (excluding national intelligence space programs), and DoD elements that are part of the Intelligence Community."[83] Overall the 113th Congress continued to use language consistent with a commoditized understanding of cyberspace.

From simply the rate of occurrence, an increase in Congress' use of the terms "cyber" and "cyberspace" is probably the most noteworthy from a textual analysis standpoint. The 113th Congress' uses "cyber" in the FY 2014 and FY 2015 NDAAs 196 times and the term "cyberspace" 24 times, more than doubling its use in the 112th Congress.[84] From a linguistic cognition standpoint, however, the number of occurrences must also be paired with the way in which they used the term, which in 2013 remained commoditized. Cybersecurity still

82. The networks and infrastructure themselves are immaterial, but they are used to support capabilities that reside on networks or are supported by infrastructure. "Networks" becomes a euphemism for commodities therein.
83. U.S. Congress, *H. Rept. 113-309: First A nnual Report of the Activities of the Committee on Armed Services for the One Hundred Thirteenth Congress*, House Report H. Rept. 113-309 (Washington, D.C.: U.S. House of Representatives, December 27, 2013), p. 24. Accessed March 27, 2017, https://www.gpo.gov/fdsys/pkg/CRPT-113hrpt309/pdf/CRPT-113hrpt309.pdf.
84. "Cyberspace" occurs 11 times in the previous two NDAAs combined.

emerged alongside IT.[85] In addition, the HASC created the position of Principal Cyber Advisor to advise the Secretary of Defense on cyber activities, whose primary function was to supervise "cyber activities related to…[DoD] *networks*, including oversight of policy, resources…and *technology*."[86] With respect to cyber test ranges, the HASC mandated an executive agent to assume roles and responsibilities which included "developing and maintaining a comprehensive list of cyber and information technology ranges."[87] Other than an observable shift in rate of occurrence for the cyber-specific terms, the 113th Congress HASC continued along the lines of the 112th Congress and used comparable lexical choices in their legislation and reports to the full chamber.

In summary, the 113th Congress continued to reflect a *commoditized* understanding of cyberspace. Use of the term "cyber" increased 150% over the previous congressional cycle, and the HASC use of the term "cyberspace" more than doubled. Otherwise, no significant lexical shifts were evident in either the FY 2014 or FY 2015 NDAA or the two annual HASC reports to the U.S. House of Representatives.

114th Congress

The 114th Congress is the final congressional cycle covered in this analysis. Of the 19 members elected to the threats and capabilities subcommittee, only six were also elected to the ETC subcommittee during the 109th Congress. Of those six, only one was elected the subcommittee every year.[88] Also of note, in 2015 the HASC removed the intelligence portfolio from the threats and capabilities subcommittee and changed its jurisdiction back to what it was during the 112th Congress. Given the perspectives which rotated

85. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2015*, December 26, 2013, p. 992. Accessed March 3, 2017, https://www.congress.gov/.
86. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2014*, December 26, 2013, p. 160. My emphasis. Accessed March 3, 2017, https://www.congress.gov/.
87. U.S. Congress, *NDAA for FY15*, p. 740.
88. This was Mr. John Kline, of Minnesota. Incidentally, Mr. Kline is no longer on the ETC, having retired from Congress in January of 2017. Mr. Kline also served 25 years in the USMC and retired with the rank of Colonel.

through the threats and capabilities subcommittee since 2005, lexical cognitive theory suggests that the authorization bills and annual report would demonstrate a shift in understanding with respect to cyberspace.

An analysis of documents produced by the 114th HASC demonstrates an every-increasing interest cyberspace within the committee. The term "cyber" alone appeared 436 times in the two authorization acts, more than doubling its rate of occurrence in the 113th Congress. Additionally, language surrounding data centers still continued to outnumber language surrounding data links. The HASC also used terminology in the legislation that had previously only appeared in committee hearings and witness testimony. For example, the term "cyber domain" appeared for the first time in the FY 2016 NDAA under Section 1086.[89] During the 110th Congress, then Ranking Member Thornberry had alluded to his perspective of cyberspace as a "domain of warfare," but that notion had yet to appear in an authorization bill or in reports to the U.S. House.[90] In the FY 2016 NDAA, Section 1086 in pertained to "reform and improvement of personnel security, insider threat detection and prevention, and physical security."[91] However, within subparagraph (a)(1)(D), the HASC displayed an understanding of the cyber domain with respect to enterprise systems and "information technology capabilities."[92]

In the FY 2017 NDAA, the HASC acted to change contract provisioning and remove elements of IT from contracting guidance which previously mandated that contracts be awarded under the "lowest price technically acceptable" (LPTA) provision. Section 813 revised the defense acquisition regulation supplement, stating that "to the maximum extent practical," the DoD was now to *avoid* using LPTA provisions for certain procuring certain goods and services. Nestled above personal protective equipment and professional training was the following

89. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2016*, November 25, 2015, p. 281. Accessed March 3, 2017, https://www.congress.gov/.
90. U.S. Congress, *Holistic Approaches to Cybersecurity*.
91. U.S. Congress, *NDAA for FY16*, p. 281.
92. U.S. Congress, *NDAA for FY16*, p. 281.

exception regarding cyberspace: "*information technology services*, cybersecurity services, systems engineering and technical assistance services, advanced electronic testing, audit or audit readiness services, or other knowledge-based professional services."[93] The focus in Section 813, as in other instances, demonstrates the HASC focus on a range of cyberspace commodities such as IT and technical services. Lexical choices here and throughout the congressional cycle demonstrates a commoditized understanding which is reinforced throughout both NDAAs as well as their annual committee report.

In summary, an analysis of the Report on the Activities of the HASC for the 114th Congress along with the two Defense Authorization Acts exhibits a *commoditized* understanding of cyberspace. Congressional concern with how warfare will be conducted in and through cyberspace remained readily apparent, as was their concern for institutional challenges required to marshal corresponding military forces. As such, the rates of occurrence for terms like "cyber," "cybersecurity," and associated derivations continued climbing during the 114th Congress. The 114th Congress became increasingly locked into a commoditized view of cyberspace instead of shifting to a different perspective.

Summary: U.S. Congress, 2005–2016

Given a theory of lexical cognition, a test case involving the U.S. Congress predicts that the Congress will never coalesce around a perspective of cyberspace reflected in a single taxonomical category. With respect to individual occurrences of words like cyber, cybersecurity, information technology, and information system, one could argue that many stand-alone instances were less about cyberspace *per se* than about the technology itself. However, when taken holistically, dominant trends in thought emerge through Congress' lexical use within each congressional cycle. Conventional wisdom holds that from 2005–2016, the Congress should shift relatively predictably between multiple

93. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2017*, December 23, 2016, p. 272. My emphasis. Accessed March 3, 2017, https://www.congress.gov/.

points of view. Evidence from the 109th to the 114th Congress suggests that this is not the case, and, that the opposite proved true. The Congress began with almost no perceptible cognitive inclination towards cyberspace and then progressed increasingly towards a commoditized framework, where it remains today.

Empirical Summary

These two complementary case studies do not support a theory of lexical cognition. Common thought patterns may be influenced by words, language and discourse, but thoughts must be bound by something with a higher degree of agency than a lexical framework. Even if the three acts of the mind remain closely related to language, we still have to look elsewhere for a higher degree of agency relating to mental frames. In the cases of GEN Alexander and the U.S. Congress, neither behaved in ways consistent with lexical theory. By studying their perceptions of cyberspace through their use of language over time, it becomes apparent that in both cases something other than discourse significantly influenced their mental frames.

By the time GEN Alexander retired he had almost exclusively discussed cyberspace in terms which were distinctly commoditized. However, when he retired from the DoD, the evidence suggests that GEN stopped comprehending cyberspace solely based on its commodities and began to understand the domain in a more axiomatic sense. In addition, conventional wisdom surrounding lexical cognition predicts that the U.S. Congress would not coalesce around a singular perspective. If that was true, the primary legislative products produced by the House Armed Services Committee would reflect a shifting perspective over time with a loose understanding of cyberspace. However, evidence from the HASC shows that the opposite was true. The Congress progressed from a point where they did not even use the term “cyberspace” to an understanding of cyberspace that was firmly and consistently commoditized.

Chapter 5

Conclusions

A theory of cyberspace rests on a collective understanding of what cyberspace *is*, and just from the following example we can see that the way the Air Force understands cyberspace recently resulted in a significant organizational change. At the time of this writing, the USAF just announced its intent to move the 24 AF (Air Forces Cyber) from under Air Force Space Command and relocate it under Air Combat Command (ACC). Since the 25 AF moved under ACC in 2014, the 24 AF transition allows a single Major Command (MAJCOM) to focus on developing and employing capabilities supporting cyber and intelligence missions.[1] Moving Numbered Air Forces between MAJCOMs presumes more than an efficiency drill. It presumes, at the very least, that the relationship between cyberspace and intelligence forces will be enhanced, which will improve the AF's overall combat effectiveness. A general perception did, in fact, lead to a specific action.

History is replete with similar examples of how a nation's understanding of a specific technology shaped how it developed and employed the capability in warfare. The Battle of Britain is a good example of this very phenomenon because the British and German Air Forces both understood RADAR in different ways. Both Germany and Britain knew that radio waves reflected off solid objects, but Britain's Watson-Watt and Roe turned RADAR into a "Radio Direction-Finding" system.[2] This "RDF" system gave skilled operators the chance to identify range, bearing, force strength, and altitude for an incoming German bomber force.[3] Hugh Dowding built the RDF into an early warning system that

1. The 25 AF was previously known as the Air Force Information, Surveillance, and Reconnaissance Agency, and retains preeminence in AF intelligence services.
2. Stephen Bungay, *The Most Dangerous Enemy* (Aurum Press Ltd., Great Britain, 2015), p. 61.
3. Bungay, *The Most Dangerous Enemy*, p. 61.

allowed the Royal Air Force's (RAF) Fighter Command to gain an operational advantage over the Luftwaffe and win the Battle of Britain.

Functioning properly, the British air defense system allowed the RAF a two-minute on-station advantage against the Luftwaffe, which allowed Fighter Command to achieve an altitude advantage and coordinate all their efforts into a single air defense sector. Adolf Galland, the preeminent Luftwaffe fighter pilot, would later write that "from the beginning the British had an extraordinary advantage, never to be balanced out at any time during the whole war, which was their radar and fighter control network and organization."[4] If the Battle of Britain had been lost, America would have been unable to use Britain as a forward staging base for U.S. armies and supplies. The Battle of Britain was therefore a "necessary precondition for all the later successes."[5] The British perception of RADAR within a larger early warning and command and control system proved to be a pivotal element to Allied success in WWII.

Given that future warfare in an "information age" context will necessarily involve the use of cyberspace, then the DoD's perception of cyberspace will influence how future wars are fought and won. In section two I discussed how perception about a phenomenon determines how we act about it because of the intervening function of mental frames. This study has not sought to address *how* actions preceded from mental frames, but rather *whether* language has the highest degree of agency in how frames are constituted to begin with. Conventional wisdom suggests that linguistic cognition has a high degree of agency within that process, and many theorists, such as Benjamin Worf, proposed that language was the dominant agent. My research shows that not to be the case; words and language still exercise agency within the cognitive process but they are not preeminent.

4. Bungay, *The Most Dangerous Enemy*, p. 68.
5. Bungay, *The Most Dangerous Enemy*, p. 388.

Core Findings

Contrary to theories of lexical cognition, words and language do not appear to be dominant agents in shaping a person's mental frames. GEN Alexander made numerous public statements as the Commander of USCYBERCOM, and they all show a cyberspace understanding that is firmly commoditized. Not only was his perspective consistent, but it helped to shape USCYBERCOM's three core missions which continue unchanged to this day. When GEN Alexander retired, lexical cognition would predict that he would continue discussing and thinking about cyberspace along commoditized lines for a significant period. Instead of maintaining his previous perspective, the evidence suggests he quickly began discussing cyberspace in terms which were more axiomatic or even at times utilitarian.

Lexical cognition also predicts that the U.S. Congress will not converge on a unified interpretation of cyberspace, but rather shift from one taxonomical approach to another. Shifting between understandings should occur as a function of lexical choices between members of congress serving from across the U.S. with different backgrounds. Furthermore, the high degree of turnover among members of the House Armed Services Committee (HASC) the subcommittee on Emerging Threats and Capabilities should serve to further preclude Congress's coalescence on any one taxonomy. The 109th Congress did not list cyberspace or any cyberspace component, such as cybersecurity, in the HASC oversight plan. Cyberspace was at best in the periphery of HASC oversight concerns throughout the 109th Congress. During the 110th and 111th Congresses, the HASC slowly came to acknowledge cyberspace as being a potential domain of conflict. Through the 114th Congress, the HASC focused increasingly on cyberspace to meet America's national security interests.

Lexical cognition would predict that GEN Alexander would be extremely slow to change such a firmly entrenched perspective of cyberspace, but that was

not the case. Likewise, a theory of lexical cognition would also predict that the U.S. Congress would not converge on a unified and yet unchanged perspective of cyberspace, but they have. In both cases, conventional wisdom, which holds that language has a dominant degree of agency in creating and maintaining mental frames, did not prove true. Given the taxonomical categories and empirical analysis presented above, the fact *that* GEN Alexander diverged from a commoditized perspective and the fact *that* the U.S. Congress converged on a commoditized perspective seems to hold true. The question that remains unsolved is *why*, which presumes that another factor or factors have greater agency than language in influencing mental frames.

Implications

The cognitive equation presented in a theory of lexical cognition, as outlined in section two of this thesis, can be summed up as language ∖ frame ∼ action, where language has a helical and reinforcing effect on cognitive frames to produce a distinct action. I have already indicated through the empirical assessments that language as an independent variable has insufficient agency to fully manipulate mental frames. However, the other half of the equation—cognitive frames leading to actions—remains highly relevant. My empirical analysis does nothing to test the mechanics of how cognitive frames lead to actions, but the research suggests that the second half of the equation holds true.

Actions do not emerge *ex nihlo*, and in both GEN Alexander and the U.S. Congress we can see evidence of a specific understanding, as *expressed* in language though not necessarily *shaped* by language, leading to predictable action. In GEN Alexander's case, the most obvious strategic result is found in the current momentum of U.S. Cyber Command being elevated to a full Unified Combatant Command.[6] The organization of the Senate Armed Services

6. Smith, "Cyberwarfare."

Committees is another example of how a particular understanding of cyberspace emerges with strategic consequences. Leaders in both chambers of the Legislature purport that cyberspace is a distinct domain, but their collective understanding is commoditized with an emphasis on Information Technology (IT) and data. This allows for herculean efforts in commodity management, but it does not advance Congressional awareness or oversight of the DoD's ability to achieve policy objectives through operations across *all* domains.

Until the end of the 114th Congress, cyberspace was included in the portfolios of the Threats and Capabilities Subcommittees in both the House and the Senate. By comparison, air, land, and maritime domains were accorded distinctive oversight and guidance by separate committees of jurisdiction. A notable change initiated by the 115th Congress is that the Senate Armed Services Committee stood up a new cyber*security* subcommittee. That change demonstrates the Senate's increased concerns over cybersecurity—which is surely an important variable within cyberspace proper—but the change reflects a commodity-dominant understanding of cyberspace rather than an understanding which is *domain*-dominant. Technology and data can be secured; domains can only be more or less effectively harnessed for an operational advantage.

Further Study

Even with the relative nascency of cyberspace, especially with respect to scholarly research, I was surprised to find that almost no one discussed cyberspace from an ontological perspective. Most works I surveyed fit more or less neatly into commodity, utilitarian, axiomatic, or perspective dependent understandings of cyberspace. This may be a function of the parameters placed on my taxonomical selection, but even so, a lack of ontological discussion is surprising because the companies and education centers surveyed are national front-runners in thinking deeply about cyberspace writ large. The only person

that seemed to wrestle with a deeper understanding of what cyberspace *is* was Damir Rajnovic, who at the time worked for CISCO.[7] Rajnovic researched worldwide perspectives on cyberspace and attempted to "produce an ontology of cyberspace using definitions of cyberspace created by multiple national governments and relevant international bodies."[8] Given the importance of cyberspace as a warfighting domain, further studies on domain distinctiveness are necessary precursors to developing theories of warfare in cyberspace. Without adequate theory, integrating cyberspace into a broader national strategy will be of limited value.

Another useful avenue of further study would be to determine the *degree* language influences cognitive frames. My research demonstrated that language and discourse were not *primary* agents, but language still influences mental frames. As referenced above, cognitive functions build from apprehension, judgment, and reasoning. Language is still required to communicate about cyberspace, build a collective understanding of it, and certainly to communicate or coordinate specific military effects in and through cyberspace.

Finally, with respect to methodology, a broader look into the Legislature may provide additional insights into how and why our national imperatives surrounding cyberspace have evolved the way they have. My analysis focused primarily on the House Committee on the Armed Services for reasons relating to time and scale. Logical expansions within the Legislature would the Senate Committee on the Armed Services, the Homeland Security subcommittee on cyberspace and infrastructure protection, and the Oversight and Government Reform subcommittee on information technology. With respect to analyzing perspectives of individual leaders within the Department of Defense, ADM Mike Rogers, who followed GEN Alexander as the Commander of USCYBERCOM, would be a prime candidate for a similar taxonomical assessment. Given that

7. Public information on Damir Rajnovic is rather limited. He worked for CISCO until around 2013, and now works as a liaison for Forum of Incident Response and Security Teams.
8. Damir Rajnovic, "Cyberspace – What Is It?," July 26, 2012, accessed April 17, 2017, https://blogs.cisco.com/security/cyberspace-what-is-it.

this analysis has been limited to available public presentations, conducting personal interviews with GEN (Ret.) Alexander, ADM Rogers, or similarly placed officials would allow for a more comprehensive assessment of language and cognition.

Bibliography

Alexander, Keith B. *CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. Cyber Command*, June 3, 2010. Accessed March 21, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/event/100603csis-alexander.pdf.

———. *General Alexander: Life After the NSA*. In collaboration with RSA 2015. May 5, 2015. Accessed March 23, 2017. https://www.youtube.com/watch?v=DWR9mJu15qo.

———. *Keynote Address by Keith Alexander*. In collaboration with Army Cyber Institute. December 20, 2016. Accessed March 25, 2017. https://www.youtube.com/watch?v=StiCssdBzVE.

———. *Statement Before the Senate Committee on Armed Services 12 March 2013*, March 12, 2013. Accessed March 22, 2017. https://www.armed-services.senate.gov/imo/media/doc/Alexander%2003-12-13.pdf.

———. *Statement Before the Senate Committee on Armed Services 27 February 2014*, February 27, 2014. Accessed March 22, 2017. https://www.armed-services.senate.gov/imo/media/doc/Alexander_02-27-14.pdf.

———. *Statement Before the Senate Committee on Armed Services November 3, 2015*. Washington, D.C., November 3, 2015. Accessed March 25, 2017. https://www.armed-services.senate.gov/imo/media/doc/Alexander_11-03-15.pdf.

Bailey, Richard. "Dilating Pupils: The Pedagogy of Cyberwar and the Encouragement of Strategic Thought." *Air and Space Power Journal* 7, no. 3 (2016): 5–25. Accessed November 8, 2016. http: //www.au.af.mil/au/afri/aspj/apjinternational/aspj_f/article.asp?id=185.

Berkeley. *Cybersecurity Policy Ideas for a New Presidency*, November 2016. Accessed March 16, 2017. https://cltc.berkeley.edu/files/2016/11/Center_ for_Long_Term_Cybersecurity.pdf.

Bungay, Stephen. *The Most Dangerous Enemy*. Aurum Press Ltd., Great Britain, 2015.

Chomsky, Noam. *Language and Mind*. 3rd ed. New York: Cambridge University Press, 2006.

CISCO. *Building an Architecture of Trust: The Network's Role in Securing Cyberspace*, January 2011. Accessed March 15, 2017. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/Architecture_of_Trust_WP.pdf.

Clearwater. *Clearwater IRM Analysis*. Accessed March 15, 2017. https://clearwatercompliance.com/wp-content/uploads/2015/07/Clearwater_IRM_Analysis_Data-Sheet-1.pdf.

———. *Healthcare Security Readiness*, March 2017. Accessed March 15, 2017. https://clearwatercompliance.com/wp-content/uploads/2017/02/Intel-Clearwater-Compliance-Healthcare-Security-Readiness-Program.pdf.

Committee on Armed Services: Oversight Plan for the 114th Congress, 2015. Accessed April 15, 2017. http://docs.house.gov/meetings/AS/AS00/20150114/102804/HMTG-114-AS00-20150114-SD002.pdf.

Committee on Armed Services: Oversight Plan for the 115th Congress, February 2, 2017. Accessed April 15, 2017. http://docs.house.gov/meetings/AS/AS00/20170202/105489/HMTG-115-AS00-20170202-SD001.pdf.

"Consolidated Appropriations Act, 2016." December 18, 2015. Accessed March 15, 2017. https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf.

"Cybersecurity 500 List of Top Cybersecurity Companies." Cybersecurity Ventures. March 1, 2017. Accessed March 15, 2017. http://cybersecurityventures.com/cybersecurity-500-list/.

Department of Defense. *Quadrennial Defense Review Report: 2006*, February 6, 2006. Accessed March 27, 2017. https://www.defense.gov/Portals/1/features/defenseReviews/QDR/Report20060203.pdf.

———. *Quadrennial Defense Review Report: 2010*, February 2010. Accessed March 27, 2017. https://www.defense.gov/Portals/1/features/defenseReviews/QDR/QDR_as_of_29JAN10_1600.pdf.

———. *Quadrennial Defense Review Report: 2014*, March 4, 2014. Accessed March 27, 2017. http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf.

Devitt, Michael, and Kim Sterelny. *Language and Reality: An Introduction to the Philosophy of Language*. Vol. 2nd ed. Cambridge, Mass: MIT Press, 1999.

Dudovskiy, John. "Ontology." 2016. Accessed April 18, 2017. http://research-methodology.net/research-philosophy/ontology/.

Ferris, Timothy. *The Mind's Sky: Human Intelligence in a Cosmic Context*. New York: Bantam Books, 1993.

Forsyth, Mark. *The Etymologicon: A Circular Stroll Through the Hidden Connections of the English Language*. Berkley trade pbk. ed. New York: Berkley Books, 2012.

Gleick, James. *The Information: A History, a Theory, a Flood*. 1st Vintage Books ed., 2012. New York: Vintage Books, 2011.

"IronNet Cybersecurity." Accessed March 24, 2017. https://ironnetcyber.com/.

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, N.J: Princeton University Press, 1976.

"Joint Publication 3-12 (Redacted): Cyberspace Operations." Accessed November 28, 2016. http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Kahneman, Daniel. *Thinking, Fast and Slow*. 1st ed. New York: Farrar, Straus / Giroux, 2011.

Kearns, Kate. *Semantics*. 2nd ed. Modern Linguistics Series. Basingstoke: Palgrave Macmillan, 2011.

Kegan, Robert, and Lisa Laskow Lahey. *Immunity to Change: How to Overcome It and Unlock Potential in Yourself and Your Organization*. Leadership for the Common Good. Boston, Mass: Harvard Business Press, 2009.

Kreeft, Peter. *Socratic Logic: A Logic Text Using Socratic Method, Platonic Questions & Aristotelian Principles*. Ed. 3.1. Edited by Trent Dougherty. South Bend, Ind: St. Augustine's Press, 2010.

Kuehl, Daniel T. "From Cyberspace to Cyber Power: Defining the Problem." In *Cyberpower and National Security*, 1st ed, by Larry K. Wentz, Stuart H. Starr, and Franklin D. Kramer, 24–42. Washington, D.C.: Potomac Books, 2009. Accessed November 28, 2016.

Kuhn, Thomas S. *The Structure of Scientific Revolutions*. Fourth edition. In collaboration with Ian Hacking. Chicago and London: The University of Chicago Press, 2012.

Libicki, Martin C. *Cyberspace in Peace and War*. Annapolis, Maryland: Naval Institute Press, 2016.

Liptak, Deborah A. "Information Warfare." *Searcher* 17, no. 9 (October 2009): 21–31. Accessed November 2, 2016. http://search.proquest.com.aufric.idm.oclc.org/docview/221111089/abstract/964AA14FC1C04CB2PQ/1.

Mayer-Schönberger, Viktor, and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Boston: Mariner Books, 2014.

Merchant, Nilofer. "Culture Trumps Strategy, Every Time." Harvard Business Review. March 22, 2011. Accessed November 2, 2016. https://hbr.org/2011/03/culture-trumps-strategy-every.

———. "Culture Trumps Strategy, Every Time." March 22, 2011. Accessed November 2, 2016. https://hbr.org/2011/03/culture-trumps-strategy-every.

"National Military Strategy for Cyberspace Operations (NMS-CO)." Accessed November 28, 2016. http: //www.dod.mil/pubs/foi/Reading_Room/Joint_Staff/07-F-2105_doc_1.pdf.

Obama, Barack H. "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment | Whitehouse.Gov." 2015. Accessed April 22, 2017. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian- malicious-cyber-activity.

Pérez, Efrén O., and Margit Tavits. "Language Shapes People's Time Perspective and Support for Future-Oriented Policies." *American Journal of Political Science*, January 1, 2017. Accessed February 1, 2017. http://onlinelibrary.wiley.com/doi/10.1111/ajps.12290/abstract.

Ponemon. *2014 Best Schools for Cybersecurity*. Research Report. Ponemon Institute. Accessed March 15, 2017. https://www.ponemon.org/local/ upload/file/2014%20Best%20Schools%20Report%20FINAL%202.pdf.

Putnam, Hilary. *Mind, Language, and Reality*. His Philosophical Papers; v. 2. New York: Cambridge University Press, 1975.

Rajnovic, Damir. "Cyberspace – What Is It?" July 26, 2012. Accessed April 17, 2017. https://blogs.cisco.com/security/cyberspace-what-is-it.

"RSA Conference: About." Accessed March 23, 2017. http://www.rsaconference.com/events/us17/about.

Schein, Edgar H. *Organizational Culture and Leadership*. 4th ed. Jossey-Bass business & management series. San Francisco: Jossey-Bass, 2010.

Schelling, Thomas C. *Arms and Influence*. New Haven, CT: Yale University Press, 2008.

Smith, Antoinette. "Cyberwarfare: What are we doing today?" U.S. Air Force. September 20, 2016. Accessed March 23, 2017.

http://www.af.mil/News/ArticleDisplay/tabid/223/Article/949919/cyberwarfare-what-are-we-doing-today.aspx.

Smith, Merritt Roe, and Leo Marx, eds. *Does Technology Drive History?: The Dilemma of Technological Determinism*. Cambridge, Mass: MIT Press, 1994.

Sproul, R. C., and Keith A. Mathison. *Not a Chance: God, Science, and the Revolt Against Reason*. Grand Rapids, Michigan: Baker Books, 2014.

"The National Military Strategy of the United States of America." Accessed November 28, 2016. http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf.

U.S. Congress. *H. Rept. 109-731: Report of the Activities of the Committee on Armed Services for the One Hundred Ninth Congress*. House Report H. Rept. 109-731. Washington, D.C.: U.S. House of Representatives, December 15, 2006. Accessed March 26, 2017. https://www.congress.gov/congressional-report/109th-congress/house-report/731/.

———. *H. Rept. 110-942: Report of the Activities of the Committee on Armed Services for the One Hundred Tenth Congress*. House Report H. Rept. 110-942. Washington, D.C.: U.S. House of Representatives, January 3, 2009. Accessed March 27, 2017. https://www.congress.gov/110/crpt/hrpt942/CRPT-110hrpt942.pdf.

———. *H. Rept. 111-710: Report of the Activities of the Committee on Armed Services for the One Hundred Eleventh Congress*. House Report H. Rept. 111-710. Washington, D.C.: U.S. House of Representatives, January 3, 2011. Accessed March 27, 2017. https://www.congress.gov/111/crpt/hrpt710/CRPT-111hrpt710.pdf.

———. *H. Rept. 112-123: First Semiannual Report of the Activities of the Committee on Armed Services for the One Hundred Twelfth Congress*. House Report H. Rept. 112-123. Washington, D.C.: U.S. House of Representatives, January 24, 2011. Accessed March 27, 2017. https://www.congress.gov/112/crpt/hrpt123/CRPT-112hrpt123.pdf.

———. *H. Rept. 112-359: Second Semiannual Report of the Activities of the Committee on Armed Services for the One Hundred Twelfth Congress*. House Report H. Rept. 112-359. Washington, D.C.: U.S. House of Representatives, December 30, 2011. Accessed March 27, 2017. https://www.congress.gov/112/crpt/hrpt359/CRPT-112hrpt359.pdf.

———. *H. Rept. 112-575: Third Semiannual Report of the Activities of the Committee on Armed Services for the One Hundred Twelfth Congress*. House Report H. Rept. 112-575. Washington, D.C.: U.S. House of Representatives, June 29, 2012. Accessed March 27, 2017. https://www.congress.gov/112/crpt/hrpt575/CRPT-112hrpt575.pdf.

U.S. Congress. *H. Rept. 112-744: Fourth Semiannual Report of the Activities of the Committee on Armed Services for the One Hundred Twelfth Congress*. House Report H. Rept. 112-744. Washington, D.C.: U.S. House of Representatives, June 29, 2012. Accessed March 27, 2017. https://www.congress.gov/112/crpt/hrpt744/CRPT-112hrpt744.pdf.

———. *H. Rept. 113-309: First A nnual Report of the Activities of the Committee on Armed Services for the One Hundred Thirteenth Congress*. House Report H. Rept. 113-309. Washington, D.C.: U.S. House ofRepresentatives, December 27, 2013. Accessed March 27, 2017. https: //www.gpo.gov/fdsys/pkg/CRPT-113hrpt309/pdf/CRPT-113hrpt309.pdf.

———. *H. Rept. 113-714: Second Annual Report of the Activities of the Committee on Armed Services for the One Hundred Thirteenth Congress*. House Report H. Rept. 113-714. Washington, D.C.: U.S. House ofRepresentatives, December 27, 2013. Accessed March 27, 2017. https: //www.gpo.gov/fdsys/pkg/CRPT-113hrpt714/pdf/CRPT-113hrpt714.pdf.

———. *H. Rept. 114-885: Report of the Activities of the Committee on Armed Services for the One Hundred Fourteenth Congress*. House Report H. Rept. 114-885. Washington, D.C.: U.S. House of Representatives, December 27, 2013. Accessed March 27, 2017. https://www.congress.gov/114/crpt/hrpt885/CRPT-114hrpt885.pdf.

———. *Information Technology and Cyber Operations: Modernization and Policy Issues in a Changing National Security Environment*. Washington, D.C., March 12, 2014. https://www.hsdl.org/?view&did=758299.

———. *National Defense Authorization Act for Fiscal Year 2006*, January 6, 2006. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2007*, October 17, 2006. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2008*, January 28, 2008. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2009*, October 14, 2008. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2010*, October 28, 2009. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2011*, January 7, 2011. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2012*, December 31, 2011. Accessed March 3, 2017. https://www.congress.gov/.

U.S. Congress. *National Defense Authorization Act for Fiscal Year 2013*, January 2, 2013. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2014*, December 26, 2013. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2015*, December 26, 2013. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2016*, November 25, 2015. Accessed March 3, 2017. https://www.congress.gov/.

———. *National Defense Authorization Act for Fiscal Year 2017*, December 23, 2016. Accessed March 3, 2017. https://www.congress.gov/.

——— . *UTC Hearing: Holistic Approaches to Cybersecurity Enabling Network-Centric Operations*. House Report. Washington, D.C.: U.S. House of Representatives, April 1, 2008. Accessed March 31, 2017. https://www.gpo.gov/fdsys/pkg/CHRG-110hhrg45255/html/CHRG-110hhrg45255.htm.

"U.S. Cyber Command Fact Sheet." September 30, 2016. Accessed March 23, 2017. http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.

Wendt, Alexander. *Social Theory of International Politics*. Cambridge studies in international relations 67. New York: Cambridge University Press, 1999.

Whorf, Benjamin Lee. *Language, Thought, and Reality: Selected Writings*. Cambridge, 1956. Accessed December 28, 2016. http://hdl.handle.net/2027/uc2.ark:/13960/t9n300r6z.