What's in a Name? Metaphors and Cybersecurity

Jordan Branch

Abstract For more than a decade, the United States military has conceptualized and discussed the Internet and related systems as "cyberspace," understood as a "domain" of conflict like land, sea, air, and outer space. How and why did this concept become entrenched in US doctrine? What are its effects? Focusing on the emergence and consolidation of this terminology, I make three arguments about the role of language in cybersecurity policy. First, I propose a new, politically consequential category of metaphor: *foundational metaphors,* implied by using particular labels rather than stated outright. These metaphors support specific ways to understand complex issues, provide discursive resources to some arguments over others, and shape policy contestation and outcomes. Second, I present a detailed empirical study of US military strategy and doctrine that traces the emergence and consolidation of terminology built on the "cyberspace domain." This concept supported implicit metaphorical correspondences between the Internet and physical space, yielding specific analogies and arguments for understanding the Internet and its effects. Third, I focus on the rhetorical effects of this terminology to reveal two important institutional consequences: this language has been essential to expanding the military's role in cybersecurity, and specific interests within the Department of Defense have used this framework to support the creation of US Cyber Command. These linguistic effects in the United States also have implications for how other states approach cybersecurity, for how international law is applied to cyber operations, and for how International Relations understands language and technological change.

> Cyberspace: A new universe, a parallel universe created and sustained by the world's computers and communication lines.
>
> —*Cyberspace: First Steps* [1991][1]

> Strategic Initiative 1: DoD [the US Department of Defense] will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.
>
> —DoD Strategy for Operating in Cyberspace [2011][2]

The Internet has generated, even for powerful states, fundamentally new security vulnerabilities, including commercial espionage, data breaches, intrusions into government networks, threats to physical infrastructure, and online election interference.

1. Benedikt 1991, 1.
2. DoD 2011, 5.

International Organization 75, Winter 2021, pp. 39–70

doi:10.1017/S002081832000051X

Yet the Internet is also seen as a source of opportunities, including for militaries—a virtual space for carrying out actions remotely that previously required crossing boundaries physically, enabling "force projection without the need to establish a physical presence in foreign territory."[3] This potential was demonstrated on the day of the 2018 US midterm elections, when a US military operation reportedly shut down Internet access at an organization in Russia believed to be behind election interference and disinformation. According to one US official, "We showed what's in the realm of the possible"—that is, the ability and willingness to use cybersecurity tools within another state's borders.[4]

How did we get here, where the US government is carrying out self-described "offensive military operations" inside Russian territory? What explains the policies and institutional changes that US officials—and those in other states, reacting to US actions—have pursued in response to cybersecurity concerns? In other words, how do policymakers understand these rapidly evolving threats and opportunities, and how are states adapting to face them? Answering these questions requires looking beyond the material features of technologies or the structure of geopolitical competition. Although threats or attacks on hardware create pressure for a policy response—and the US operation was itself a reaction to Russian interference—the *form* of that response is underdetermined by material or strategic circumstances and thus is also shaped by ideational factors, including the effects of language itself. Focusing specifically on changes in cybersecurity terminology used by state officials, in this article I make three arguments: theoretical, empirical, and explanatory.

First, I propose a novel addition to theories of language and policy. I distinguish between, on the one hand, explicitly stated analogies and metaphors and, on the other, *foundational metaphors*, constituted by using particular terms as labels. Foundational metaphors implicitly connect otherwise distinct conceptual fields, reframing policy problems and solutions and shaping the rhetorical resources available for political contestation. This approach builds on existing International Relations (IR) literature—including constructivist scholarship on language,[5] theories emphasizing argument and rhetoric,[6] and research joining IR with Science and Technology Studies[7]—and suggests new, generalizable mechanisms by which language shapes outcomes.

Second, through an extensive study of primary documents, I provide the first comprehensive empirical account of the cybersecurity language used by the US military.

3. Joint Chiefs 2018, xii.

4. Ellen Nakashima, "US Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," *Washington Post,* 27 February 2019; David E. Sanger and Nicole Perlroth, "US Escalates Online Attacks on Russia's Power Grid," *New York Times,* 15 June 2019.

5. Kratochwil 1989; Krebs 2015; Milliken 1999; Onuf 1989, 2013; Raymond 2019; Sandholtz 2008; Schmidt 2008.

6. Crawford 2002; Krebs and Jackson 2007; Risse 2000.

7. Fritsch 2011; Herrera 2006; Mayer, Carpes, and Knoblich 2014; McCarthy 2017.

After several decades of evolving terminology, by the late 2000s US doctrine defined cybersecurity in terms of threats and opportunities "in cyberspace." Simultaneously, cyberspace was defined as a "warfighting domain," suggesting that it is as militarily important as land, sea, air, and outer space. The combination of "cyberspace" with "domain" has constituted a foundational metaphor implying that the Internet and related systems have created a virtual space within which actions take place.

Third, I explain how this foundational metaphor, implicit in "cyberspace domain," has reshaped US policy and institutions in two ways. First, as state agencies have competed for cybersecurity resources and responsibilities, this language has reinforced the military's arguments for a dominant role. Second, in contestation within the military, the metaphor has supported a specific institutional solution: US Cyber Command. These changes have altered policy outcomes, including the nature and frequency of US military cybersecurity operations. Moreover, creating a command for "cyberspace" has effects beyond the United States, as Cyber Command operates across borders and as other states emulate—or challenge—US concepts, strategies, and institutions. These linguistic and ideational factors are largely overlooked by the prevailing approach to cybersecurity in IR, which has productively emphasized technical and strategic aspects.[8] Focusing on the rhetorical consequences of foundational metaphors implicit in terminological labels reveals new connections between language and policy outcomes, including identifying why language is so consequential in a complex field like cybersecurity.[9]

Metaphor Theory and Cyberspace

Metaphors involve "understanding and experiencing one kind of thing in terms of another,"[10] a transfer of meaning that is especially important for thinking through new or complex phenomena.[11] Metaphors, however, are not simply evocative comparisons. Instead they have complex effects through their *entailments*: follow-on concepts or ideas that reshape thinking, decision making, and practical outcomes.[12] IR studies have explored the effects of metaphorical language, demonstrating that

8. E.g., Buchanan 2016; Choucri 2012; Demchak and Dombrowski 2011; Gartzke 2013; Kello 2017; Lindsay 2013; Rid 2013; Valeriano and Maness 2015. A wider array of approaches has also emerged, relating cybersecurity to Internet governance (DeNardis 2014; Raymond and DeNardis 2015), securitization (Hansen and Nissenbaum 2009), Science and Technology Studies (Dunn Cavelty 2018), norm development (Finnemore and Hollis 2016), history (Healey 2013; Warner 2012), territoriality (Herrera 2007; Lambach 2020; Sheniak 2014), and language (Dunn Cavelty 2013; Lawson 2020; Lupovici 2016).

9. Following Raymond (2019, 36), I combine constitutive and causal claims, addressing first how it has been possible to construct cybersecurity threats in specific ways and then why certain institutional and policy responses have followed.

10. Lakoff and Johnson 1980, 5.

11. Lakoff 1992, 205.

12. Gibbs 2008; Lakoff and Johnson 1980; Lakoff 1992; Semino 2008.

even instrumentally deployed analogies have pervasive, often unintended policy consequences.[13]

In addition to analogies and metaphors that are used consciously, other metaphors operate on a deeper level. These *conceptual metaphors* are "systematic sets of correspondences … across conceptual domains" that "reflect conventional patterns of thought."[14] In this article I introduce a new category, *foundational metaphors*: conceptual metaphors constituted by using particular terms as labels. Like other conceptual metaphors, they provide "mental models [that] guide our thoughts without us really being aware of them"[15]—reinforcing specific assumptions, suggesting particular analogies and discouraging others, and limiting which arguments can be made convincing. Foundational metaphors, however, specifically emerge when something is labeled with a term with connotations that imply answers to foundational questions: What defines this as a "thing"? What are its fundamental characteristics? To what other things is it similar? Whether chosen deliberately or intuitively, the label itself is often presented by speakers as commonsensical, or not needing to be explained.[16] Nonetheless, whether anyone is aware of it or not, metaphorical correspondences can emerge.[17]

Unlike explicitly stated metaphors (or analogies), foundational metaphors' correspondences are implied by the connotations of terminology—yet either type of metaphor could draw the same correspondences. Because foundational metaphors are implicit, identifying them requires multiple steps: noting that a particular label is consistently used,[18] examining the range of metaphorical correspondences *potentially* implied, and then analyzing surrounding texts to see which of those correspondences—if any—are guiding the entailed descriptions, arguments, and explicit analogies and metaphors. The content of a foundational metaphor is shaped, as well as revealed, by surrounding language. For example, explicitly stated metaphors and implicit foundational metaphors often work in conjunction, each structuring the meaning of the other.

I focus on rhetoric and argument, where foundational metaphors play a powerful and distinct role.[19] Rhetorical contestation takes place at all levels of international

13. Khong 1992; also Bousquet 2009; Drulák 2006; Lawson 2014; Onuf 2013, chapter 3.

14. Semino 2008, 5. On conceptual metaphor theory, see Lakoff and Johnson 1980.

15. Larsson 2017, 7–8.

16. This takes no position on whether speakers or audiences believe the implicit metaphorical correspondences *are* true or commonsensical. Instead, following Semino's discursive metaphor theory, we can analyze texts' metaphorical content, including how prevalent metaphors "come to represent the 'commonsense' or 'natural' view." Semino 2008, 33.

17. Many metaphors are "not noticed as being metaphorical." Lakoff and Johnson 1980, 27.

18. Determining how "consistently" and by whom is difficult. A foundational metaphor *exists* when a speaker uses a term with metaphorical implications, observable in surrounding text. That metaphor is *consequential* when it is used widely in a community. See footnote 26.

19. Focusing on rhetoric sidesteps the contested argument that metaphors directly shape thought. Semino, for example, argues that while we are not "completely blinkered and straitjacketed by the metaphors we conventionally use … in some cases we may be," supporting a "weak version of the Sapir-Whorf hypothesis." Semino 2008, 33.

politics,[20] and even "rational" actors need to use acceptable "normative reasoning" to convince others.[21] In such arguments, language can be deployed to remove opponents' discursive resources—not changing their minds, but denying them the "rhetorical commonplaces" needed to convince audiences.[22] Metaphorical language in contestation ranges from intentional deployments to unconscious choices. Historical analogies, for example, are often selected instrumentally by decision makers (albeit from those resonant within a community).[23] By contrast, invoking foundational metaphors by using particular terminology is rarely so instrumental. Speakers may reach for a term because they believe it "works" as a label rather than because they think it will directly support their arguments. In fact, opposing arguments often use the same terminology and draw on the same foundational metaphors, the entailments of which then frame debate. Yet not all arguments are as readily supported by the metaphors implied by shared terms—foundational metaphors can make certain arguments more convincing.

As with other linguistic processes, foundational metaphors are simultaneously a resource, constraint, and context for political interaction.[24] Like "dominant narratives" in foreign policy, these metaphors "do not fully smother contestation but channel it,"[25] setting boundaries for which arguments count as legitimate. The point at which terminology comes to be at least provisionally settled—that is, presented as unproblematic and commonsensical—constitutes an important critical juncture.[26] Contestation and argument continue, but within different bounds.

Metaphorical language is everywhere in cybersecurity, as designers, users, and policymakers rely extensively on analogies and metaphors—including terminology no longer even considered metaphorical (desktop, virus, firewall). Existing studies have focused on the effects, often unintended, of instrumental analogies and metaphors.[27] For example, the analogy to Pearl Harbor explicitly emphasized the

20. Crawford 2002, 13.
21. Sandholtz 2008, 103.
22. Krebs and Jackson 2007, 42, 45.
23. Khong 1992.
24. The effects of foundational metaphors can be distinguished from other linguistic processes by two elements. First, here *metaphors* implicitly connect otherwise distinct concepts, defining a narrower scope of meaning making than narratives, norms, or rules. Second, the importance of *implicit* meanings differentiates this from securitization (Buzan, Wæver, and de Wilde 1998) or instrumentally using a label—for example, *combatant*—with explicit legal or normative consequences (Kinsella 2005). Yet foundational metaphors often work alongside other processes: narratives or stories, for example, help define policy problems, but "the framing of problems often depends upon metaphors underlying the stories." Schön 1993, 138. Among the diverse ways in which social facts shape contestation, foundational metaphors are distinguished by being metaphors implicit in shared terminology.
25. Krebs 2015, 5.
26. It is difficult to set a threshold on *how widely* a term must be accepted. Nonetheless, when multiple sides to an ongoing debate use the same terminology—implying the same metaphorical correspondences—that community's language has at least provisionally been settled. While never permanent, language often remains stable for identifiable periods.
27. E.g., studies suggesting "cyber analogies": Goldman and Arquilla 2014; Greathouse 2014; Karas, Moore, and Parrott 2008; Manjikian 2015, 2016; Nye 2011; Perkovich and Levite 2017. For analysis:

possibility of a catastrophic attack on infrastructure to promote specific preventive measures, but it also unintentionally minimized the threat of continuous low-level intrusions and espionage.[28] Likewise, the "threat representations" that decision makers instrumentally deploy to support their arguments also shape perceptions in unintended ways.[29] Foundational metaphors, implicit in terminology, have received far less attention.

The word *cyberspace* implies a metaphor between the Internet (and related systems) and some kind of space.[30] This implicit correspondence follows a common pattern: something "relatively abstract, complex, unfamiliar, subjective, or poorly delineated" (global computer networking) is understood by reference to something "concrete, simple, familiar, physical and well-delineated" (physical space).[31] Yet space can be understood and defined in various ways, and identifying the specific spatial metaphor implied by a community's use of *cyberspace* requires examining the associated arguments and analogies, especially when they form a coherent whole.[32] Although the implication that cyberspace is a "place" is almost never meant literally, implicit metaphors nonetheless shape discussion.

Where, then, did *cyberspace* originate? Author William Gibson coined the word in the early 1980s, noting later that "it seemed evocative and essentially meaningless."[33] Yet there was a meaning embedded in the term itself, in its designation as a type of *space*—reinforced by the spatial language used to describe this "consensual hallucination."[34] Within a few years *cyberspace* had been adopted in the media and by technology companies, and by the mid-1990s it was widely used to describe *where Internet users were,* metaphorically.[35] It was deployed in explicitly political arguments, such as the 1996 "Declaration of the Independence of Cyberspace,"[36] as well as in late-1990s legal debates about regulating online activity—in which opposing arguments shared the metaphorical framework that online activity occurred "in cyberspace."[37]

Betz and Stevens 2013; Dunn Cavelty 2013; Graham 2013; Lapointe 2011; Lawson 2012; Libicki 2012; Stevens 2016.

28. Critical discussions: Gartzke 2013; Goldman and Arquilla 2014; Lawson 2020; Stevens 2016.

29. Dunn Cavelty 2013 is closest to my approach, examining language both "setting the linguistic rules of the game and … used instrumentally" (118). I focus on metaphors implied by terminology *used* by decision makers, rather than the *creation* of available "threat representations."

30. Karas, Moore, and Parrott 2008; Lapointe 2011. Betz and Stevens note that "cyberspace" may represent cybersecurity's "ur-metaphor." Betz and Stevens 2013, 149.

31. Semino 2008, 6.

32. Larsson 2017, 28. The next section demonstrates this in the US case with *cyberspace* and *domain*.

33. Mueller 2017a, 418.

34. Gibson 1984, 69; Edwards 1996, 308.

35. Edwards 1996, 19–20; Rid 2016, 219–20.

36. Barlow uses cyberspace terminology but draws on nonterritorial images ("a standing wave in the web of our communications"). Barlow 1996. The elasticity of *possible* metaphorical correspondences reinforces the point: identifying the foundational metaphor constituted by a term requires looking to the surrounding text(s).

37. E.g., Goldsmith 1998; Johnson and Post 1996; Lessig 1999. Commentary: Blavin and Cohen 2002; Cohen 2007; Hunter 2003; Lemley 2003; Yen 2002.

The popularity of a spatial term like *cyberspace* was in part predictable. Spatial metaphors are often used to understand abstract concepts,[38] and they have been widely applied to online activities.[39] Yet the embrace of this specific term was also, in part, coincidental.[40] Many technologists had been interested in *cybernetics* and thus were likely to find the *cyber* prefix appealing.[41] In the early 2000s, however, the term largely disappeared from popular and academic discourses.[42] Yet it was exactly in this period that *cyberspace* increasingly appeared in US military language, where the term has since become ubiquitous.[43]

In short, *cyberspace* is more than just a catchy word. In the specific context of US security policy and military doctrine it has been an essential component of terminology—and implicit metaphors—used to conceptualize the political and security implications of information technology. These metaphors have provided the foundation for specific arguments and policies deployed by the US government to manage cybersecurity threats. As other states have emulated, challenged, or resisted US actions, the language and policy of the United States have played a significant role in shaping the global response to cybersecurity issues.[44]

US Doctrine and the "Cyberspace Domain"

Since computer security first arose as a policy issue, US decision makers have used an evolving set of terms. By the late 2000s, however, US military doctrine had come to rely almost exclusively on cyberspace-based terminology, further specifying that computers and networks constitute a "domain" of warfare. This dual conceptual framework has changed little in the past decade and is now deeply rooted in how the US military talks about, and organizes for, cybersecurity. To uncover this pattern, I draw on a comprehensive reading of public and declassified cybersecurity documents. They were not read for an exact count of terms, or to identify the first or last use of a particular word or phrase. Instead, I survey trends in dominant

38. Lakoff and Johnson 1980, 17.

39. E.g., Internet users describe their actions spatially. Maglio and Matlock 1998; Matlock et al. 2014. See also Cohen 2007, 212; Hunter 2003; 444; Larsson 2017, 29.

40. Contingent origins do not preclude path-dependent effects: for example, the QWERTY keyboard. David 1985.

41. Rid 2016. This helps explain why "cyberspace" was adopted over other authors' terms (e.g., "the other plane," in Vinge 1981, a novella influential among technologists; Rid 2016, 206) or Gibson's "the matrix," which appears more often than "cyberspace" in his novels. Hunter 2003, 473.

42. The Google Books Ngram Viewer shows a post-2000 decline. Wagner 2019, 61. See also Betz and Stevens 2013, 150; Graham 2013, 178.

43. Even *cyber* has come to refer to computers and networks in this community. Healey 2013, 280; but see Futter 2018 and Lupovici 2016. This has eclipsed Arquilla and Ronfeldt's 1993 influential discussion of "cyberwar," in which *cyber* referred to "information-related principles." With roots in *cybernetics*, *cyber* could also suggest control or governance. Arquilla and Ronfeldt 1993, 57; Lindsay 2017, 494; Rid 2016, 3. Yet "historical" or "etymological" origins of metaphors often matter less than current uses. Semino 2008, 18.

44. Dunn Cavelty and Egloff 2019, 44.

terminology and implied foundational metaphors (identified in surrounding texts). Focusing on this level of language reveals broad patterns that cut across variation in documents' arguments, author intent, or drafting processes.[45]

In the 1980s, cybersecurity was rarely addressed in major national security statements; when it was, documents discussed the security of "telecommunications" and "information systems."[46] The terminology changed by the mid-1990s, especially at the Department of Defense (DoD), where "information warfare" dominated.[47] This was a broad concept: the definition in an influential 1995 Air Force document includes not only computer-network attack and defense but also all operations targeting information, from propaganda to the physical destruction of informational hardware.[48] "Joint Vision 2010," released by the Joint Chiefs of Staff in 1996, reflects a similar emphasis on information warfare and operations.[49] Neither document uses "cyberspace" or cyber-prefixed terms.

At the same time, "cyberspace" began to appear in other government documents as something *within* which things happen. For example, a 1995 National Security Agency (NSA) document is titled "SIGINT and INFOSEC in Cyberspace,"[50] and in 1997 an outgoing NSA official argued that cyberspace is a distinct site of espionage and conflict akin to territorial spaces: "Almost every type of action that occurs in the physical world will have a corollary in cyberspace," and "The Future of Warfare is Warfare in Cyberspace."[51] Yet these documents continued to use "information warfare" language as well.

Published in 2000, the Joint Chiefs' "Joint Vision 2020" reveals an evolution of information-warfare terminology, while setting the stage for the important later shift to "cyberspace domain." Like its 1996 predecessor, this document continues to use information-based terms rather than "cyberspace." Yet it now defines information as a "domain of operations," noting that "operations within the information domain will become as important as those conducted in the domains of land, sea, air, and space."[52] In contrast, earlier documents had sometimes proposed an *area* or *realm* of conflict in which information plays a special role,[53] but the terminology was inconsistent and had not included the word *domain*. (While it is impossible to prove the complete absence of a term or usage, it is suggestive that the *DoD*

45. Diverse approaches study ideas through documents. E.g., Builder 1989; Raymond 2019; Semino 2008. Contemporary documents are more useful than later interviews, given the tendency to project vocabulary backwards. Although accessing *all* relevant documents is impossible (especially with classification), I reviewed an extensive sample covering all *types* of US military documents, classified and unclassified: memos, vision documents, strategies, doctrines, etc. The quoted documents are representative of overall trends.
46. White House 1984.
47. Warner 2015.
48. US Air Force 1995.
49. Joint Vision 2010, Joint Chiefs of Staff, 1996. On file with author.
50. National Security Agency 1995.
51. Black 1997.
52. Joint Chiefs 2000, 72.
53. E.g., US Air Force 1995, 8.

Dictionary—which collates terms from military documents—starts defining "domains" in 1999).[54]

In the mid-2000s, US military language took a decisive shift, joining *domain* with *cyberspace*—a combination that would prove crucial. For example, the Joint Chiefs' 2004 "National Military Strategy" uses *cyberspace* as a framework to understand the new domain ("The Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains").[55] Soon thereafter, other documents consistently deploy cyberspace language in place of information terms. The Joint Chiefs' classified "National Military Strategy for Cyberspace Operations" from 2006 explicitly defines cyberspace—not information—as a domain and argues that "treating cyberspace as a domain establishes a foundation to understand and define its place in military operations."[56] Finally, a 2008 memo from the Deputy Secretary of Defense officially defines cyberspace as a "global domain" in doctrine,[57] a definition subsequently adopted across DoD documents.

The metaphorical correspondences implied by cyberspace terminology provided a consistent conceptual framework for discussing this new nonphysical domain—in other words, *cyberspace* gave *domain* a particular meaning. The earlier information-based terminology was ambiguous, with diverse connotations, and the relationship between information and physical spaces was never clarified. For example, the "Joint Vision" document from 2000 argues that information has a "multidimensional definition": "domain of operations" *and* "target, weapon, resource."[58] Given that information was essential to military operations long before the Internet,[59] is the "information domain" actually new? Which aspects are new and require new strategies or tactics? These questions were difficult to address with information-based terminology.

By labeling this new domain "cyberspace," however, it could be designated as a domain *and nothing else*. Cyber warfare involves "operating within or through [cyberspace]," while information operations aim broadly to "influence adversary decisions."[60] Essential to this discursive effort was the particular spatial metaphor implied by the combination of *cyberspace* with *domain*. While each term has diverse possible meanings, when used together their definitions are narrowed. Without this further specification, *cyberspace* could imply various types of space: political territory, postmodern "space of flows," notional space of ideas, or others. Likewise, *domain*'s multiple etymologies—ranging from mathematics to medieval

54. Joint Chiefs of Staff, n.d.
55. Joint Chiefs 2004, 18.
56. Joint Chiefs 2006, ix.
57. Specifically, cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." US Strategic Command 2009, 8.
58. Joint Chiefs 2000, 72.
59. Joint Chiefs 2000, 61.
60. Alexander 2007, 60.

political authority over land—imply diverse metaphorical correspondences. Because the two terms are deployed together in US military documents, however, the metaphorical implications of each are narrowed down to a correspondence between the cyberspace domain and the four physical spaces within which the military already operates.[61] This is evident in the geographic or territorial analogies deployed in surrounding texts: "terrain," "high ground," "borders," "failed state," "ungoverned frontier," and so on.[62] These explicit comparisons reveal the characteristics of the implicit spatial metaphor and they are simultaneously made more convincing by it.[63]

The foundational metaphor implied by *cyberspace domain* allowed convincing parallels to be drawn to physical spaces. Broad objectives "in cyberspace" can be framed with available concepts: for example, the 2006 Joint Chiefs document states that a key "strategic goal" is "to ensure US military strategic superiority in cyberspace" just as in air, sea, land, and space.[64] The rhetorical power of that statement follows from the metaphor implied by the terms: here is a new space, created by computers and networks, into which existing goals can be translated.

DoD documents subsequently argue repeatedly that cyberspace is a domain, distinct from the four physical domains but similar in that the US military needs to operate within it. For example, a 2009 "Cyber Warfare Lexicon" defines a host of cyber-prefixed terms as the versions of "real world" phenomena taking place "in cyberspace."[65] Especially after 2010, the dual shift in terminology—deploying the "cyberspace" label and then calling it a "domain"—becomes pervasive in high-profile documents. The Pentagon's 2011 "Strategy for Operating in Cyberspace," for instance, frames cyberspace as a domain within and through which the US and its adversaries act.[66] Although this document actively argues that cyberspace should be treated as an operational domain, it simply asserts that there is something called "cyberspace" within which things happen.[67] This terminology was taken up

61. Separating out land, sea, and air was a long-standing organizational principle of the US military, institutionalized in the National Security Act of 1947. But it was only when this "new" space appeared that a label (i.e., "domain") was needed—the 1947 act simply distinguishes among "operations on land," "operations at sea," and "air operations." See Heftye 2017 and Nakayama 2019. Thus "domain" does not appear until the late 1990s. The eventual designation of *one label* for land, sea, air, space, *and* cyberspace may have been more important than the term "domain" itself—which has not been officially defined in Joint Chiefs of Staff, n.d. See also Allen and Gilbert 2009, 2.

62. Betz and Stevens 2013; Lapointe 2011; Manjikian 2010.

63. Implied characteristics can contradict explicit definitions. For example, US military publications define cyberspace in terms of hardware. See footnote 57; Dunn Cavelty 2013, 108. Yet those texts' spatial analogies present cyberspace instead as a "space between the hardware components … where interaction happens." Dunn Cavelty 2013, 107. The implicit metaphor, not the formal definition, often frames further arguments and proposed solutions.

64. Joint Chiefs 2006, 13. Note that these statements often discuss actions or goals "in cyberspace" without using "domain." In this community, "cyberspace" alone has come to embody the combined meaning of "cyberspace domain."

65. US Strategic Command 2009; Cartwright 2010.

66. DoD 2011.

67. See epigraph.

throughout the US military, as service branches used cyberspace-domain language to analogize to their existing practices and concepts.[68]

By the mid-2010s, the idea of cyberspace as a domain of warfare was fully entrenched in US military language.[69] For example, while the DoD's 2011 cybersecurity strategy explicitly argues that cyberspace *should* be treated as an operational domain, the 2015 and 2018 revisions simply assume that cyberspace *is* a domain and discuss how to operate in it.[70] This terminology was not only directed at external audiences; it also informed internal DoD discussions. Classified memos use the same foundational metaphor, including, for example, a 2010 secret instruction on "counterintelligence activities in cyberspace"[71] and a 2013 document on "Human Intelligence (HUMINT) Activities in Cyberspace."[72] A 2012 Presidential Decision Directive authorizing offensive cyber operations also addresses threats and actions "in cyberspace."[73] Finally, internal Pentagon communications about disrupting the Islamic State's online presence discuss the need to "counter the Islamic State of Iraq and the Levant (ISIL) in Cyber Space."[74]

This terminology has become both stable and ubiquitous, demonstrating its rhetorical power and its ability to fit logically with existing military concepts and ideas. In other words, at this point there is little contestation among military authors about the language to be used; the arguments are entirely about how to apply the cyberspace-domain concept to improve strategies and tactics. This framework's persistence for more than a decade is striking, given the incentives to propose new terms. Military documents often note the importance of language,[75] and promoting new or different terminology can be one way to contribute to strategy or doctrine.[76] Since at least 2010, however, efforts to innovate have continued to discuss the "cyberspace domain."[77]

While scholarly attention usually focuses on contested aspects of language and policy, the consolidation of terminology—and implicit foundational metaphors—can be equally important. Contestation continues, but the available rhetoric has been transformed. Tracing these linguistic processes reveals new aspects of cybersecurity policymaking.

68. US Army 2010; US Air Force 2011; US Navy 2012; US Coast Guard 2015.
69. The pattern is clear in document series: for example, the 1997–2014 Quadrennial Defense Reviews (QDRs) shift from using no cyberspace terminology to consistently discussing cyberspace as a domain.
70. DoD 2011, 2015, 2018.
71. DoD 2010a, 1.
72. DoD 2013.
73. White House 2012.
74. US Cyber Command 2016.
75. Cartwright 2010, 1; US Army 2010, i.
76. In author interviews, officials repeatedly mentioned new terminology being motivated by the desire to "make one's mark" in a new position.
77. E.g., DoD 2018; Joint Chiefs 2018.

Metaphors and Institutional Change

In the mid-2000s, significant intrusions into US government and corporate networks intensified pressure on policymakers to respond.[78] Yet the nature of that response was far from preordained and was shaped by the foundational metaphor implicit in cyberspace-domain terminology. This metaphor gave particular arguments more weight and made it possible to present certain institutional solutions as commonsensical. In other words, language has not driven policy directly, nor has it entirely constrained how speakers or audiences think. Instead, explicit and implicit linguistic framings have made some propositions more resonant with existing ideas, arguments, and interests, strengthening those positions in political contestation.

A critical juncture occurred in the late 2000s, with concurrent changes in US doctrine, institutions, and outcomes. The shift to an exclusive reliance on cyberspace-domain terminology allowed an implied foundational metaphor to be deployed—both instrumentally and unintentionally—to support particular institutional and policy changes, at two levels of contestation. First, as state agencies have competed for cybersecurity responsibilities and resources, this language has been successfully used to argue for increasing the role of military over civilian institutions.[79] Second, within the military, it supported the creation of US Cyber Command, a single organization for military operations "in cyberspace." The resulting institutional changes have had significant downstream effects, including enabling an increase in offensive cybersecurity actions by the US military. Given the ambiguity of many cybersecurity tasks—which could be framed in terms of commerce, law enforcement, homeland security, or national defense—these outcomes were not simply the most effective or "rational" responses.

Policy outcomes in cybersecurity emerge out of numerous processes, of course, many of which interact with the rhetorical effects of language. For example, DoD funding procedures can make it difficult to "mainstream" solutions to new problems, that is, to add a new task across existing organizations.[80] Overcoming that challenge by creating a new organization, however, depends on the availability of rhetorical resources to support such an institutional change. Similarly, while the militarization of cybersecurity may reflect general post-9/11 trends,[81] the metaphors implied by cyberspace-domain language have made it possible to present this as a commonsense solution. Finally, although institutional and policy shifts have coincided with broader contextual changes—technical innovation, more skilled adversaries, turnover and

78. David E. Sanger, "Pentagon Puts Cyberwarriors on the Offensive, Increasing the Risk of Conflict," *New York Times,* 18 June 2018.

79. I do not address broader, state-versus-society contestation regarding the respective cybersecurity roles of the state vis-à-vis corporations, civil-society groups, individuals, etc. See Coles-Kemp, Ashenden, and O'Hara 2018; Dunn Cavelty 2013; Dunn Cavelty and Egloff 2019; Hansen and Nissenbaum 2009; McCarthy 2018. On language see Kamis and Thiel 2015; Stevens 2016, 184.

80. As noted regarding cybersecurity by former Defense Secretary Carter 2019, 340.

81. Brooks 2016.

learning among policymakers—the effects of those factors are, on their own, indeterminate. For example, given that there is rarely a single optimal policy, learning alone cannot explain which specific solution is chosen.[82] Instead, how officials revise strategies, respond to adversaries, and understand novel threats have all been framed by the terms, rhetoric, and ideas that predominate within the military cybersecurity community—including the metaphors implicit in *cyberspace domain*. At key moments, bureaucratic competition over cybersecurity has been shaped by this language—probabilistically, not deterministically—as cyberspace-domain terminology favored certain arguments over others.

DoD officials have actively used this framework to denote cybersecurity as a military rather than civilian concern, attempting to close the controversy around the nature of the problem and its solution. The early-2000s shift from *information warfare* to *cyberspace domain*—with its implied spatial metaphor—made it rhetorically easier to present cybersecurity activities taking place in something analogous to air, land, sea, and outer space, all of which involve nonmilitary issues and concerns but, simultaneously, are spaces in which the military legitimately operates.[83] For example, in 2010 the Deputy Secretary of Defense wrote in *Foreign Affairs* that "the Pentagon has formally recognized cyberspace as a new domain of warfare … just as critical to military operations as land, sea, air, and space."[84] Officials at other agencies "were as much surprised by the article as some foreign audiences,"[85] and they immediately protested this designation.[86] Information-warfare concepts had not inspired such a direct reaction, but the cyberspace-domain framework suggested a more expansive—and bureaucratically threatening—claim.

This language supports military arguments, while also having an intrinsic appeal to military actors. As Michael Hayden (retired Air Force general and former NSA and CIA director) put it in 2011: "Like everyone else who is or has been in a US military uniform, I think of cyber as a domain. It is now enshrined in doctrine: land, sea, air, space, *cyber*. It trips off the tongue, and frankly I have found the concept liberating."[87]

That Hayden finds this language "liberating" reflects how the implied spatial metaphors are simultaneously useful in policy arguments *and* appealing as a metaphorical framework for understanding a complex and challenging area.[88] As noted earlier, they allow policymakers to apply existing ideas to new problems. The relevant questions are then straightforward (How do known strategies apply "in cyberspace"?) and

82. Although cyberspace terminology and metaphors have been *rhetorically effective*—making certain policies easier to promote—the resulting policies are not necessarily *objectively effective*.
83. Dunn Cavelty 2013, 113; Manjikian 2015, 3.
84. Lynn 2010, 101–102. See also Alexander 2007.
85. Hayden 2016, 130.
86. E.g., Lute and McConnell 2011.
87. Hayden 2011, 4; see also Libicki 2012. Hayden's 2016 memoir makes similar points.
88. Lambach 2020; Stevens 2016, 74. This suggests studying *positive affect* in cybersecurity, adding to research on negative emotions like fear. Betz and Stevens 2013, 149; Dunn Cavelty 2012, 116; Lawson 2020.

less likely to require entirely new concepts or models. The ability to draw from other domains has been essential to military staffing, since many senior cybersecurity positions were initially filled by individuals who began in traditional "kinetic" operations.[89] In short, this terminology was adopted because it intuitively fit as much as because it was instrumentally useful.

While few argue that the military should play no role in cybersecurity, the DoD's gradual expansion of its remit is potentially reshaping US civil-military relations, which are defined by such "haggling over prerogatives."[90] Beyond the core problem of civilian control—formally settled in the United States—factors like the balance of funding affect how power within the state is distributed and whom the public perceives to be "in charge" in a particular policy area.[91] Contestation thus affects the relative primacy of civilian goals, the choice of solutions to new problems, and how problems are defined to begin with—especially with novel or ambiguous issues. If the military's definition of cybersecurity problems comes to be accepted as commonsensical and beyond debate, that definition will frame which solutions are in or out of bounds.[92] The recent expansion of the military's role thus represents an important shift in how the US government approaches cybersecurity.[93]

Within the Defense Department as well, there has been competition over cybersecurity roles and resources.[94] Diverse elements within the DoD have attempted to claim cybersecurity as "their" issue area, with the Air Force most prominent among the service branches. In the 1990s, for example, Air Force documents argued that the "information realm" was most similar to air,[95] and in 1995 it created one of the first "true combat" units for information attack.[96] A decade later, Air Force officials drew on emerging cyberspace language to propose an Air Force Cyber Command, describing its core mission as "to fly and fight in the Air, Space, and Cyberspace."[97]

Yet it was officials advocating for a joint approach, particularly within the Office of the Secretary of Defense, who successfully deployed the cyberspace-domain framework. Had the discussion simply been about cyberspace—that is, had

89. Healey 2013, 55; Libicki 2012, 332.
90. Brooks 2019, 387.
91. Ibid., 386.
92. Using cyberspace-domain language to present a significant military role in cybersecurity as *commonsensical* has been essential. For example, former CYBERCOM commander Keith Alexander argued, on the appropriate role of the military: "[the US Constitution] says that the purpose of the Union is to provide for the common defense. There is no parenthetical that says 'except in cyberspace.'" Clarke and Knake 2019, 94.
93. Healey 2013; Warner 2012. While DoD certainly had a hand in the creation of the Internet, the importance of that is contested and for decades other interests dominated Internet structure and governance. Townes 2012.
94. I focus here on *institutional interests and arguments*; on the role of specific individuals see Kaplan 2016 and Nakayama 2019.
95. US Air Force 1995, 8; Hayden 2016, 127.
96. Healey 2013, 35; Healey 2017; Nakayama 2019.
97. Lani Kass, "A Warfighting Domain," Presentation, AF Cyberspace Task Force, 26 September 2006. On file with author.

cyberspace not been designated as a domain—Air Force arguments could have been more convincing: cyberspace is complex, and operating there shares features with maneuvering in air and space more than with acting on land or sea. Framing cyberspace as *one of five domains*, however, implies that each domain, while distinct, shares certain characteristics (i.e., those making it a domain), supporting the need for parallel organizations. This fits better with building a joint force for cybersecurity than with subsuming cyberspace under the Air Force, a service already dedicated to a "traditional" domain.[98] In 2008, Air Force Cyber Command's permanent activation was denied.

Instead, in 2009 the relevant tasks were newly combined in US Cyber Command, one of the most significant organizational changes in US cybersecurity policy in the last two decades.[99] Creating an independent command for both defensive and offensive cyberspace operations represents a combat-focused "military paradigm" that favors specific "legal and policy choices,"[100] supported rhetorically by the foundational metaphor implied by cyberspace-domain terminology. Unfortunately, the explicit analogies that have followed (e.g., maneuver or deterrence in cyberspace), while succinct and evocative, may compromise key cybersecurity goals.[101] Military institutions are always guided by more than official mandates or rational decision-making processes, and foundational metaphors shape outcomes in ways similar to organizational procedures or service "personalities."[102]

While distinct from the service branches, Cyber Command has been tightly linked to another military organization: the National Security Agency (NSA). Its commander is "dual hatted" as NSA director, and both headquarters are at Fort Meade. These connections reflect the Command's need to coordinate with NSA signals-intelligence activities—and, even more, to draw on NSA resources and expertise.[103]

98. In 2019 space operations were upgraded from an Air Force command to a stand-alone Space Force, a move similarly promoted with "domain" language. For example, in 2017 the future head of Space Force argued that "space is … a war-fighting domain and we need to treat it as such." Anthony Capaccio, "US Air Force Space Chief Sees Final Frontier as Battleground," *Bloomberg,* 17 October 2017. Available at <https://www.bloomberg.com/news/articles/2017-10-17/u-s-air-force-space-chief-sees-final-frontier-as-battleground>. "Domain" favors the separation, not merging, of roles.

99. Healey 2013, 73–75. Cyber Command was operational in 2010 and elevated to a unified combatant command in 2018.

100. Hollis and Ohlin 2018, 441.

101. A point made by, among others, Betz and Stevens 2013; Dunn Cavelty 2012, 119; Heftye 2017; Lapointe 2011, 16; Lawson and Middleton 2019, 14–15; Libicki 2012; Stevens 2016.

102. E.g., Builder 1989.

103. Linking the two could be presented to the Joint Chiefs as "offering NSA's resources to enhance DOD cyber-combat power at little cost to the services." Hayden 2016, 143. While this practical explanation is convincing, the rhetorical effects of language may have played some role. Kaplan (2016, 219–20) notes that NSA declassified a host of cybersecurity documents in 2012, once Cyber Command was operational and PPD-20 (White House 2012) had authorized offensive cyber operations. Included were the mid-1990s NSA documents discussed earlier, which do not use "domain" but do discuss "cyberspace" (NSA 1995; Black 1997)—suggesting at least the possibility that NSA sought to demonstrate its own lineage "in cyberspace." Yet such a rhetorical move was unlikely to succeed: by 2012 cyberspace-domain language was well established as a rhetorical resource to support Cyber Command's assertion of a combat role in this "war-fighting domain."

Nonetheless, the Command is organizationally separate, with authority to conduct combat operations rather than espionage. This distinction has enabled actions that would have been extremely unlikely to emerge from an intelligence organization, including Cyber Command's recent uptick in "offensive operations."[104] Revealing capabilities by engaging in attack or disruption runs contrary to the goal in intelligence collection to keep capabilities secret—and thus usable—for as long as possible. Overall, both organizations have likely seen advantages as well as disadvantages to this arrangement.[105] Thus, while the dual hat can certainly be read as NSA "winning" a bureaucratic battle, the expansion of Cyber Command's combat-oriented activities —supported by the DoD's dominant cyberspace-domain language—suggests a limited NSA victory at best.[106]

Cyberspace-domain language provided essential rhetorical tools for those advocating for the new command. For example, the 2009 memo establishing Cyber Command emphasizes various threats "in cyberspace" and the need "to secure freedom of action in cyberspace."[107] In 2010, the Deputy Secretary of Defense argued that, because "the military must be able to defend and operate within [cyberspace] … the Defense Department needs an appropriate organizational structure."[108] Which institutional solution is deemed "appropriate," of course, is conditioned by how problems are framed—here, entirely in terms of operating "in cyberspace," making Cyber Command the correct solution. The Command's mission statement also draws on implicit spatial metaphors: the Command will "ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."[109] In later documents and testimony related to Cyber Command, cyberspace-domain language continues to be essential to further argument—and goes largely unremarked.[110]

Even when recent statements explicitly emphasize new threats—requiring new responses—discussion continues to rely on the same terminology and spatial analogies. For example, the 2018 "Command Vision" outlines a significant shift in strategy toward a more offensive posture through "defending forward" and "persistent engagement," repudiating the more reactive 2011 strategy.[111] Cyberspace-domain language helps to legitimize the new posture—including potentially controversial elements like "operating outside our borders, being outside our networks."[112] Operating in another state's territory could be interpreted as a form of aggression,

104. Kaplan argues that, once Cyber Command was operational, offensive operations "emerged as a consuming, even dominant, activity at Fort Meade." Kaplan 2016, 211.

105. Sulmeyer 2017.

106. Some connection between Cyber Command and NSA will almost certainly persist. While discarding the dual hat has long been discussed (Kaplan 2016, 257; Sulmeyer 2017), the arrangement represents a "sticky" institutional design—who wants to be the first *non*-dual-hatted NSA director or CYBERCOM commander?

107. Secretary of Defense 2009.

108. Lynn 2010, 101–102.

109. DoD 2010b.

110. E.g., Alexander 2011, 2013.

111. Schneider 2019; Smeets and Lin 2018; US Cyber Command 2018.

112. Nakasone 2019a, 7.

or raise concerns about possible escalation.[113] Those concerns, however, are undercut by arguments drawing on spatial metaphors. For example, in 2019 Paul Nakasone, the head of Cyber Command, wrote:

> We must "defend forward" in cyberspace, as we do in the physical domains. Our naval forces do not defend by staying in port, and our airpower does not remain at airfields. They patrol the seas and skies to ensure they are positioned to defend our country before our borders are crossed. The same logic applies in cyberspace.[114]

The Command's new posture thus involves activity "in cyberspace" analogous to uncontroversial actions in the physical domains. Of course, the idea that these all follow the "same logic" depends on the underlying foundational metaphor that connects cyberspace to physical spaces, especially to global commons like the high seas.[115]

Nakasone's statement, moreover, operates at multiple levels of contestation simultaneously. It explicitly defends Cyber Command's new proactive posture. It justifies the Command as the military's centralized cybersecurity organization—if the high seas have the Navy and airspace has the Air Force, cyberspace requires Cyber Command. Finally, it implicitly promotes the broader role of the military: civilian agencies do not contest the DoD securing physical domains, so why should they protest the "same logic" applied to cyberspace? All three arguments rely on the metaphor implied by *cyberspace domain*.

Within the US military, this language appears to be firmly consolidated. It was first explained and advocated, then officially declared as doctrine, and finally taken as given. Cyberspace-domain terminology continues to justify the existence of Cyber Command and, at the same time, the institutionalization of this language in the Command's mission—and even its name—makes it increasingly difficult for an alternative framework to replace it. In fact, while discursive communities outside the government have long resisted this terminological framework—*domain*, *cyberspace*, even the *cyber* prefix[116]—the military's terms and implied foundational metaphors have spread into broader discussions across the federal government.[117] This terminology continues to shape policy outcomes, not just rhetoric: the 2019 National Defense Authorization Act expanded Cyber Command authorities to respond to a wide array of threats "in cyberspace," resulting in a significant increase in offensive actions.[118]

113. Though Kreps and Schneider 2019 suggest that escalation fears may be misplaced.
114. Nakasone 2019b, 12.
115. Rhetoric also used by Hayden 2016, 132.
116. Rid and Buchanan 2018, 7.
117. E.g., the report from the "Cyberspace Solarium Commission," led by elected officials and including multiple federal agencies, closely tracks DoD language. King and Gallagher 2020.
118. NDAA 2019, section 1642. Chesney 2019; Clarke and Knake 2019; Sanger and Perlroth, "US Escalates Online Attacks."

Counterfactuals and Comparisons

How might different language have led to different outcomes? Without the foundational metaphor implied by the combination of *cyberspace* with *domain*, cybersecurity debates would have played out differently. Essential here is the *conjunction* of the two terms and how that specified and strengthened the particular metaphorical implications that emerged: namely, that the Internet has created a virtual space with territorial features, within which military ideas, strategies, goals, and actions apply. Without the specification as a domain, cyberspace could have continued to be associated with a wide range of spatial ideas and implications—in fact, before the military adopted this term, its most prominent political uses were explicitly nonterritorial.[119]

Without the combined term, arguments for increasing the military's cybersecurity role would have lacked a powerful rhetorical resource, and counterarguments by other agencies might have been more successful. Consider, for example, a published back-and-forth between officials from the DoD and the Department of Homeland Security (DHS).[120] In response to the DoD's assertion that cyberspace constituted a "domain of warfare," the DHS officials first deployed a nonspatial concept: "cyber-ecosystem—not just technology, but also policy, procedure, practice, and law."[121] Yet the *cyberspace* term could not be ignored, so the DHS response also tried to redefine it: "cyberspace is fundamentally a civilian space." But land, sea, air, and space are "civilian spaces" and "warfighting domains" *at the same time*. Thus "domain" specifies exactly what the DoD means by "cyberspace" and makes it possible to undermine counterarguments that use cyberspace language. Without this ability to set the terms of the debate (literally), the DoD position would have lacked a key rhetorical advantage it has enjoyed against civilian agencies' arguments.

We can also ask what might have happened if Gibson had not coined the specific term *cyberspace* to begin with. It is certainly possible that a different term implying a spatial metaphor could have emerged and become widely adopted.[122] If combined with *domain* (or the like), another spatial term could in theory have constituted similar rhetorical resources.[123] Yet not every candidate term with spatial connotations would have worked as effectively. For one, "cyberspace" does not just connote a space, it literally contains the word *space*. And the term is syntactically efficient: speaking about events or actors "in cyberspace" is more succinct than many alternatives.[124] Without the specific word *cyberspace,* it is unlikely that arguments

119. E.g., Barlow 1996.

120. The DoD case was prominently argued in *Foreign Affairs* by Lynn 2010, with a response in *Wired* by Lute and McConnell 2011.

121. Lute and McConnell 2011.

122. Lakoff and Johnson (1980, 17) note the prevalence of spatial metaphors.

123. I remain agnostic about how essential the specific term *domain* has been (rather than early alternatives like *realm*). The crucial step was consistently applying *a single label* to land, sea, air, space, *and* cyberspace (see footnote 61).

124. Compare, for example, "operating in the information domain/realm" with "operating in cyberspace."

supporting the role of military actors and interests in this domain would have been so convincing.

Without cyberspace-domain language, nonspatial terms and implicit foundational metaphors might have become more prominent in these cybersecurity debates. For example, when "the Internet" is used as an overall label for networking and computing,[125] it can imply a set of metaphorical correspondences to *networks* rather than *spaces*.[126] The resulting emphasis on network features (e.g., nodes and connections) rather than operating in a virtual space yields different interpretations of cybersecurity problems and solutions.[127] Biological terms and metaphors like *ecosystem*, similarly, might be more prevalent in the absence of cyberspace-domain language, yielding different rhetorical resources.[128] While these and other terminologies have come in and out of use,[129] few have become as firmly consolidated within a community—and thus as consequential—as the US military's use of *cyberspace domain*.

The effects of the DoD's cybersecurity language are further illustrated by comparing how different terminology has worked within other agencies—and by considering how those terms could have altered outcomes at DoD. For example, since its creation in 2002, DHS has not characterized cyberspace as a spatial domain but has instead discussed cybersecurity in terms of protecting *critical infrastructure*. More than a description of Internet hardware, "critical infrastructure" implies a metaphorical correspondence between the Internet and other communication and transportation systems. The terminology first became prominent in a 1997 presidential commission report that focused on "cyber" threats to civilian infrastructure, without framing them as threats *within* digital spaces and without using "cyberspace" at all.[130] Although later DHS documents occasionally use the term, it is not discussed as a *domain* and the metaphor of actions in a virtual space is absent.[131]

The contrast between DHS and DoD language has had observable consequences. The two have reacted differently to major cybersecurity incidents, with each organization's response guided not only by its mission but also by its foundational metaphors. In 2016, as evidence of Russian interference in US elections surfaced, the

125. Recalling that the word *internet* originally referred only to "internetworking" projects like ARPANET.

126. E.g., "Internet governance" literature largely avoids spatial language and metaphors, focusing instead on network-type characteristics like "control points." DeNardis 2014; Raymond and DeNardis 2015.

127. Lambach 2020, 7–8. For example, this suggests historical analogies to communication networks like the telegraph, with distinct security (Gartzke and Lindsay 2015) or legal implications. Goldsmith 1998.

128. On biological metaphors in general, see Betz and Stevens 2013; Dunn Cavelty 2013, 110; Lapointe 2011. *Ecosystem* has been suggested by analysts (Osenga 2013, 49–51) and policymakers (Lute and McConnell 2011).

129. E.g., "information superhighway" was used to argue for federal investment in the early Internet. Blavin and Cohen 2002, 269–70.

130. White House 1997. See Braman 2014, 49; Collier and Lakoff 2008; Warner 2012.

131. E.g., DHS 2003; DHS 2011, D-2. See Futter 2018. The core difference between DHS and DoD definitions of *cyberspace* is the DoD's use of *domain*—the two definitions are otherwise nearly identical. US Strategic Command 2009, 8; DHS 2011, D-2.

DHS largely stayed within the frame of monitoring, preventing, and mitigating direct attacks on election infrastructure.[132] The department's institutional response was then to reorganize its relevant components as the Cybersecurity and Infrastructure Security Agency (CISA). The DHS Secretary argued that this change "allows us to confront the threats of today."[133]

The Pentagon's response to 2016 election interference, on the other hand, has involved a command whose mission is entirely framed in terms of operating "in cyberspace," defined as a military domain. Russian actions are thus labeled as "cyberattacks," and threats to the territory and sovereignty of the United States.[134] In March 2018 comments on Russian interference, for example, the head of Strategic Command argued that "Cyberspace needs to be looked at as a warfighting domain … and if somebody threatens us in cyberspace, we need to have the authorities to respond."[135] The response by US Cyber Command has then focused on operating proactively "in cyberspace" to prevent or disrupt future interference, including the 2018 election-day operation discussed earlier.

How would the two organizations respond differently if their terminologies and metaphors were reversed? If the DoD were to use *critical infrastructure* as a cybersecurity framework,[136] its response to foreign interference would likely be framed by its existing definition of "critical infrastructure protection" in general: "Actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc."[137] None of this is about defending those "assets" by operating in adversaries' territory and interfering with their corresponding systems. Actions like the 2018 cyberattack on Russian sources of election interference would not easily fit in this frame, making them more difficult to present as commonsensical and proportionate responses.

Likewise, DHS would pursue different policies if it relied on spatial terminology and metaphors. While using "domain" would be unlikely—since that term emerged from a specific context at DoD—a spatial model that DHS could conceivably draw on is an analogy to border protection (one of "six overarching homeland security missions").[138] This would place less emphasis on vulnerability and resilience in core infrastructure and more on preventing intrusions at network locations analogous to territorial boundaries (i.e., away from election hardware itself).[139] Yet DHS's

132. E.g., DHS 2016, 2018.
133. DHS 2018. Clarke and Knake argue that it was "just a reorganization of things that were already in DHS." Clarke and Knake 2019, 171.
134. E.g., Carter 2019, 341.
135. Sanger, "Pentagon Puts Cyberwarriors on the Offensive."
136. As to *why* it does not, see the discussion on the close "fit" that spatial terminology provided with military concepts and staffing.
137. DoD 2020.
138. "Mission." Homeland Security. Available at <https://www.dhs.gov/mission>.
139. Manjikian 2016.

long reliance on critical infrastructure language, which predates the department itself, appears to undermine other frameworks—just as DoD's cyberspace-domain terminology has, thus far at least, remained impervious to alternatives.

"Cyberspace" Beyond the United States

In this article I have analyzed how cybersecurity has been constructed by language, going beyond the focus in existing literature on technical and strategic aspects. In particular, foundational metaphors, implied by widely used terminology, have shaped arguments, policy responses, and institutional changes. In US military doctrine and strategy, the *cyberspace domain* label has constituted a set of underlying spatial metaphors since the mid-2000s—providing instrumental rhetorical tools and, simultaneously, structuring the arguments, analogies, and policies brought to bear. This has shaped contestation within the US government, supporting militarization and the creation of a unified Cyber Command. In circumstances of rapid technological change, uncertain consequences, and novel vulnerabilities—conditions clearly present in cybersecurity—how issues are framed in terminology and then institutionalized can have significant effects. While I have focused on the United States, cybersecurity language and metaphors also shape contestation in other contexts.[140]

For one, US terms—and implicit metaphors—have appeared in documents from other states, particularly among US allies.[141] NATO documents have also drawn directly on US concepts,[142] and even US adversaries have, on occasion, used US language.[143] While the military, economic, and diplomatic power of the United States explains why US language has sometimes been emulated,[144] the consequences of that emulation result from the content of US terminology, including its implicit foundational metaphors.

Those consequences are evident in debates around how international law applies to cybersecurity—especially debates that have drawn directly on US language.[145] For example, the two *Tallinn Manuals* were written by a group of experts (largely from NATO states) seeking to codify how state practices reveal customary and

140. The following explores, briefly, linguistic processes and cybersecurity elsewhere, particularly international reactions to US terminology. Comparing terms and metaphors across languages has inherent challenges, including the mistranslation of words or divergent connotations. Giles and Hagestad 2013; Kamis and Thiel 2015; Zeng, Stevens, and Chen 2017.

141. E.g., UK Cabinet Office 2009. Emulation of US policy includes the very idea of releasing a "cybersecurity strategy." Kerttunen and Tikk 2019, 10.

142. NATO 2014, par. 72–73.

143. E.g., a 2015 Chinese strategy mentions "threats from such new security domains as outer space and cyber space." PRC 2015; see also Zeng, Stevens, and Chen 2017. This suggests the possibility that a single terminology could eventually serve as a "focal point" for international cybersecurity contestation. Farrell and Glaser 2017, 13.

144. Some other communities have thus been instrumentally motivated to adopt the cyberspace-domain framework, regardless of whether it provided the same institutional and intuitive "fit" that explains its uptake in the US military.

145. On cybersecurity language and international law see Boer 2017; Sauter 2015.

treaty-based international law of "cyber warfare" and "cyber operations."[146] The *Manuals* build on the spatial concepts in US cybersecurity language, even quoting from a US document that "international norms guiding State behavior … also apply in cyberspace," and defining terms like "cyber operations" and "cyberspace" very similarly to US terminology.[147] Yet the spatial metaphors implied by this terminology can complicate—maybe unnecessarily—the application of international law.[148]

Because the *Tallinn Manuals* discuss cybersecurity actions as occurring *in* or *through* cyberspace, nearly all issues are framed in terms of territorial sovereignty, defined as control over or independence of "a portion of the globe."[149] This is unproblematic for analyzing states' rights and responsibilities with regard to physical Internet infrastructure (states have a clear claim over hardware within their boundaries) or actions that involve physically crossing a border. Yet there is more to cybersecurity than direct control over hardware—one "point of leverage" over Internet activity[150] but a crude tool of Internet governance and rarely successful on its own.[151]

The *Tallinn Manuals*, therefore, also attempt to classify actions that rely exclusively on informational or nonphysical means, especially actions that intentionally cross state boundaries. This ranges from using "remote cyber operations" to effect damage inside another state[152] to sending "cyber weapons" through the infrastructure of a neutral party.[153] The spatial metaphor implied by cyberspace terminology has complicated this analysis, preventing consensus within the *Tallinn* group of experts: some treated cyberspace as a spatial extension of state territory (and thus subject to the same rules, metaphorically translated "into cyberspace"), while others treated cyber operations as informational actions that should not be understood through spatial analogies. With progress unlikely on any treaty-based international law for cybersecurity,[154] even nonbinding discussions like the *Tallinn* process will guide further developments in international law and norms, including by framing questions with largely unquestioned terms and implicit metaphors.[155]

146. Schmitt 2013, 2017. Although states do not see these manuals as binding and some analysts consider them irrelevant (e.g., Lucas 2016, 17), they serve as the first point of discussion and frame subsequent debate. Corn 2017; Raymond 2019, 206. Legal discourses are often shaped by "conceptual path dependence." Larsson 2017, 50.

147. Schmitt 2013, 3, 258. They have also drawn, implicitly, on language used by US officials (e.g., State Department lawyer Harold Koh 2012 on international law "in cyberspace"), itself reflecting earlier legal scholarship (footnote 37).

148. Although "domain" appears only rarely, the *Tallinn* discussions nonetheless draw on the US framing of cyberspace as a domain.

149. Schmitt 2013, 16; Schmitt 2017, 11. For example, the second edition begins by affirming: "The principle of State sovereignty applies in cyberspace." Schmitt 2017, 11. International legal debates often define "cyberspace with reference to territory." Manjikian 2015, 4. See also Mueller 2019.

150. Finnemore and Hollis 2016, 460.

151. DeNardis 2014; Lambach 2020, 13–14.

152. Schmitt 2017, 17–27.

153. That is, are "cyber weapons" munitions or information? Schmitt 2017, 553–62.

154. Hollis and Ohlin 2018.

155. Post-*Tallinn* discussions have continued to debate how law applies "in cyberspace" (e.g., *AJIL Unbound* 2017).

In other international settings, less dominated by US interests, the interactions across diverse languages, terminologies, and metaphors have been more complex. For example, in two UN cybersecurity bodies—the Group of Governmental Experts (GGE) and the more recent Open Ended Working Group (OEWG)—US language has not predominated. In consensus reports in 2013 and 2015 (hailed for demonstrating a surprising degree of international agreement), the GGE framed its work as developing norms regarding the use of "information and communication technologies" (ICTs) and the "conduct of ICT-related activities"[156]—not actions "in cyberspace." It is possible that agreement was enabled, albeit temporarily,[157] by the broad language being used: "ICT activities" favors neither the US cyberspace-domain concept nor the very different language of "information security" used by some other participating states, including Russia and China.[158]

Outside of international forums, there are other pathways by which US language may have global effects. For example, important aspects of Internet governance could be reshaped by an unintended correspondence between US terminology and authoritarian governments' Internet policies. The metaphors implied by cyberspace-domain language in US doctrine may inadvertently legitimize controls like China's "great firewall"—the US's spatial metaphors naturalize the idea of boundaries and state authority "in cyberspace." The Chinese government's claim of sovereignty over the Internet within its borders has even been justified with reference to the *Tallinn Manuals*.[159] In other words, the cyberspace-domain concept and the resulting spatial metaphors could implicitly support "Internet fragmentation," especially the "alignment" of Internet controls with state boundaries.[160]

Given that cybersecurity metaphors are likely to persist (it would be nearly impossible to avoid them entirely),[161] we should at a minimum be aware of how the metaphors implied by terminology shape arguments in policymaking—and in scholarship. Research in IR and Security Studies often uses cyberspace terminology, asking whether and how conflict, power, norms, deterrence, or other "traditional" security issues and concepts apply "in cyberspace."[162] Using other language may add new analogies, comparisons, and policy recommendations.[163] Or it could be helpful to

156. UNGA 2013, 2015.

157. In 2017 the GGE failed to yield a consensus report. See Henriksen 2019; Maurer 2020; Raymond 2020; Tikk and Kerttunen 2018.

158. Giles and Hagestad 2013; Tikk and Kerttunen 2018. *Information security* includes controlling Internet content alongside blocking malware or preventing network intrusions. While authoritarian governments' deployment of this concept is explained well by instrumental motivations, this article's framework suggests additional questions: What metaphors are implied by these terms? How do those metaphors fit with different interests? How might contestation around cybersecurity then be reshaped in countries where these terms predominate?

159. Zeng, Stevens, and Chen 2017, 449.

160. Mueller 2017b, 35. See also Mueller 2019.

161. Sauter 2015, 66.

162. E.g., Borghard and Lonergan 2017; Finnemore and Hollis 2016; Gartzke 2013; Kello 2017.

163. E.g., Gartzke and Lindsay 2015 on deception in communication networks, or Demchak and Dombrowski (2011, 35) on the Internet as a "substrate."

avoid conceptualizing the Internet and its effects as one "thing," by any name, and instead discuss it for what it is: a collection of actors, technologies, systems, institutions, problems, policies, effects, and so on.[164] Finally, one could use multiple terminologies simultaneously, and thus draw on diverse underlying metaphors.[165] While the "imperfections" of any particular metaphor are a possible constraint, they can also be "a source of creativity and innovation,"[166] especially when disparate metaphors are put in conversation with one another.

For IR in general, this study of terminology, metaphors, and their effects suggests two additions to how we analyze language and its consequences. First, it shows that examining *implicit* meanings and metaphors, not just explicitly made arguments, can be useful for understanding rhetorical processes and effects. Second, in addition to the customary focus on open contestation—arguments and analogies deployed instrumentally—we can look at what elements of language are *not* contested and what underlying ideas are then supported or precluded. To identify how language becomes consolidated, it is useful to trace it back to the point at which it was still unsettled—when terminology remained an open rather than closed controversy.[167] Both points apply outside of cybersecurity, especially to the politics of other new technologies.[168]

Quite a lot, it turns out, can be in a name. The labels and implicit metaphors that militaries, analysts, and even scholars use can reshape the technological environment, redefine the "terrains" of conflict, and determine what is and is not a "domain of warfare."

References

AJIL Unbound. 2017. Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0. Available at <https://doi.org/10.1017/aju.2017.58>.

Alexander, Keith B. 2007. Warfighting in Cyberspace. *Joint Forces Quarterly* 46:58–61.

Alexander, Keith B. 2011. Building a New Command in Cyberspace. *Strategic Studies Quarterly* (Summer):3–12.

Alexander, Keith. 2013. Commander, United States Cyber Command, Statement before the Senate Committee on Armed Services. 12 March. Available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-091.pdf>.

Allen, Patrick D., and Dennis P. Gilbert, Jr. 2009. The Information Sphere Domain: Increasing Understanding and Cooperation. In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 132–42. IOS Press.

164. Or a "bundle of mechanisms." Farrell 2012, 36.

165. For related suggestions, see Lawson and Middleton 2019, 16; Manjikian 2016.

166. Lawson 2020, 197.

167. Latour 1987.

168. For example, in legal and ethical debates about remote military operations, activists have instrumentally deployed terms like "killer robots," while militaries discuss "remotely piloted aircraft." Both labels are intended to frame the debate by suggesting specific metaphors—to dystopian scenarios or to the accepted use of aircraft in warfare. Yet even the widely used word *drone* may imply a set of unexamined metaphorical correspondences.

Arquilla, John, and David Ronfeldt. 1993. Cyberwar Is Coming! *Comparative Strategy* 12 (2):141–65.
Barlow, John Perry. 1996. A Declaration of the Independence of Cyberspace. Available at <https://www.eff.org/cyberspace-independence>.
Benedikt, Michael, ed. 1991. *Cyberspace: First Steps*. MIT Press.
Betz, David J., and Tim Stevens. 2013. Analogical Reasoning and Cyber Security. *Security Dialogue* 44 (2):147–64.
Black, William B. 1997. Thinking Out Loud About Cyberspace. *Cryptolog*. Available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-011.pdf>.
Blavin, Jonathan H., and I. Glenn Cohen. 2002. Gore, Gibson, and Goldsmith: The Evolution of Internet Metaphors in Law and Commentary. *Harvard Journal of Law and Technology* 16 (1):266–85.
Boer, Lianne J.M. 2017. "Spoofed Presence Does Not Suffice": On Territoriality in the Tallinn Manual. In *Netherlands Yearbook of International Law 2016: The Changing Nature of Territoriality in International Law*, edited by Martin Kuijer and Wouter Werner, 131–45. Asser.
Borghard, Erica D., and Shawn W. Lonergan. 2017. The Logic of Coercion in Cyberspace. *Security Studies* 26 (3):452–81.
Bousquet, Antoine. 2009. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*. Hurst and Company.
Braman, Sandra. 2014. Cyber Security Ethics at the Boundaries: System Maintenance and the Tallinn Manual. In *Proceedings: First Workshop on Ethics of Cyber Conflict*, edited by Ludovica Glorioso and Anna-Maria Osula, 49–58. NATO CCD COE.
Brooks, Risa. 2019. Integrating the Civil-Military Relations Subfield. *Annual Review of Political Science* 22:379–98.
Brooks, Rosa. 2016. *How Everything Became War and the Military Became Everything*. Simon and Schuster.
Buchanan, Ben. 2016. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Oxford University Press.
Builder, Carl H. 1989. *The Masks of War: American Military Styles in Strategy and Analysis*. Johns Hopkins University Press.
Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner.
Carter, Ash. 2019. *Inside the Five-Sided Box*. Dutton.
Cartwright, James E. 2010. Memorandum: Joint Terminology for Cyberspace Operations. Available at <https://nsarchive2.gwu.edu//dc.html?doc=2692112-Document-10>.
Chesney, Robert. 2019. CYBERCOM's Out-of-Network Operations. *Lawfare* 9 May. Available at <https://www.lawfareblog.com/cybercoms-out-network-operations-what-has-and-has-not-changed-over-past-year>.
Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. MIT Press.
Clarke, Richard A., and Robert K. Knake. 2019. *The Fifth Domain*. Penguin.
Cohen, Julie E. 2007. Cyberspace as/and Space. *Columbia Law Review* 107 (1):210–56.
Coles-Kemp, Lizzie, Debi Ashenden, and Kieron O'Hara. 2018. Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen. *Politics and Governance* 6 (2):41–48.
Collier, Stephen J., and Andrew Lakoff. 2008. The Vulnerability of Vital Systems: How "Critical Infrastructure" Became a Security Problem. In *Securing "the Homeland": Critical Infrastructure, Risk and (In)security*, edited by Myriam Dunn Cavelty and Kristian Søby Kristensen, 17–39. Routledge.
Corn, Gary. 2017. Tallinn Manual 2.0—Advancing the Conversation. *Just Security*. 15 February 2017. Available at <https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/>.
Crawford, Neta C. 2002. *Argument and Change in World Politics*. Cambridge University Press.
David, Paul A. 1985. Clio and the Economics of QWERTY. *The American Economic Review* 75 (2): 332–37.
Demchak, Chris C., and Peter J. Dombrowksi. 2011. Rise of a Cybered Westphalian Age. *Strategic Studies Quarterly* 5 (1):32–61.
DeNardis, Laura. 2014. *The Global War for Internet Governance*. Yale University Press.

Department of Defense. 2010a. Instruction S-5240.23: Counterintelligence (CI) Activities in Cyberspace. 13 December. Available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-041.pdf>.
Department of Defense. 2010b. US Cyber Command Fact Sheet. 25 May. Available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-038.pdf>.
Department of Defense. 2011. Department of Defense Strategy for Operating in Cyberspace. Available at <https://nsarchive2.gwu.edu/dc.html?doc=2700131-Document-50>.
Department of Defense. 2013. Instruction S-3325.10: Human Intelligence (HUMINT) Activities in Cyberspace. 6 June. Available at <https://nsarchive2.gwu.edu//dc.html?doc=2692127-Document-19>.
Department of Defense. 2015. The Department of Defense Cyber Strategy. Available at <https://nsarchive2.gwu.edu/dc.html?doc=2692133-Document-25>.
Department of Defense. 2018. Summary: Department of Defense Cyber Strategy. Available at <https://nsarchive2.gwu.edu//dc.html?doc=4936880-Department-of-Defense-Summary-Department-of>.
Department of Defense. 2020. Critical Infrastructure Program Glossary. Available at <https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-Global-Security/Defense-Critical-Infrastructure-Program/cip_glossary/>.
Department of Homeland Security (DHS). 2003. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. Available at <https://www.dhs.gov/homeland-security-presidential-directive-7>.
Department of Homeland Security. 2011. Cybersecurity Strategy for the Homeland Security Enterprise. Available at <https://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf>.
Department of Homeland Security. 2016. Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security. 7 October. Available at <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national>.
Department of Homeland Security. 2018. Secretary Kirstjen M. Nielsen Remarks to the National Election Security Summit. 10 September. Available at <https://www.dhs.gov/news/2018/09/10/secretary-kirstjen-m-nielsen-remarks-national-election-security-summit>.
Drulák, Petr. 2006. Motion, Container and Equilibrium: Metaphors in the Discourse about European Integration. *European Journal of International Relations* 12 (4):499–531.
Dunn Cavelty, Myriam. 2012. The Militarisation of Cyber Security as a Source of Global Tension. In *Strategic Trends 2012: Key Developments in Global Affairs*, edited by Daniel Möckli, 103–24. ETH-Zurich.
Dunn Cavelty, Myriam. 2013. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review* 15:105–22.
Dunn Cavelty, Myriam. 2018. Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance* 6 (2):22–30.
Dunn Cavelty, Myriam, and Florian J. Egloff. 2019. The Politics of Cybersecurity: Balancing Different Roles of the State. *St. Antony's International Review* 15 (1):37–47.
Edwards, Paul N. 1996. *The Closed World: Computers and the Politics of Discourse in Cold War America*. MIT Press.
Farrell, Henry. 2012. The Consequences of the Internet for Politics. *Annual Review of Political Science* 15: 35–52.
Farrell, Henry, and Charles L. Glaser. 2017. The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine. *Journal of Cybersecurity* 3 (1):7–17.
Finnemore, Martha, and Duncan B. Hollis. 2016. Constructing Norms for Global Cybersecurity. *American Journal of International Law* 110 (3):425–79.
Fritsch, Stefan. 2011. Technology and Global Affairs. *International Studies Perspectives* 12 (1):27–45.
Futter, Andrew. 2018. "Cyber" Semantics: Why We Should Retire the Latest Buzzword in Security Studies. *Journal of Cyber Policy* 3 (2):201–16.
Gartzke, Erik. 2013. The Myth of Cyberwar. *International Security* 38 (2):41–73.
Gartzke, Erik, and Jon R. Lindsay. 2015. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies* 24 (2):316–48.

Gibbs, Raymond W. Jr., ed. 2008. *The Cambridge Handbook of Metaphor and Thought*. Cambridge University Press.
Gibson, William. 1984. *Neuromancer*. Ace Books.
Giles, Keir, and William Hagestad II. 2013. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In *2013 Fifth International Conference on Cyber Conflict*, edited by K. Podins, J. Stinissen, M. Maybaum, NATO CCD COE Publications. Available at <https://www.academia.edu/4187620/Divided_by_a_Common_Language_Cyber_Definitions_in_Chinese_Russian_and_English>.
Goldman, Emily O., and John Arquilla, eds. 2014. *Cyber Analogies*. Naval Postgraduate School.
Goldsmith, Jack L. 1998. The Internet and the Abiding Significance of Territorial Sovereignty. *Indiana Journal of Global Legal Studies* 5 (2):475–91.
Graham, Mark. 2013. Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities? *The Geographical Journal* 179 (2):177–82.
Greathouse, Craig B. 2014. Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? In *Cyberspace and International Relations Theory, Prospects and Challenges*, edited by Jan-Frederik Kremer and Benedikt Müller, 21–40. Springer.
Hansen, Lene, and Helen Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53 (4):1155–75.
Hayden, Michael V. 2011. The Future of Things "Cyber." *Strategic Studies Quarterly* 5 (1):3–7.
Hayden, Michael V. 2016. *Playing to the Edge: American Intelligence in the Age of Terror*. Penguin.
Healey, Jason. 2017. Claiming the Lost Cyber Heritage. Available at <https://www.airuniversity.af.edu/CyberCollege/Portal/Article/Article/1198929/claiming-the-lost-cyber-heritage/>.
Healey, Jason, ed. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Cyber Conflict Studies Association.
Heftye, Erik. 2017. Multi-Domain Confusion: All Domains Are Not Created Equal. *The Strategy Bridge*. Available at <https://thestrategybridge.org/the-bridge/2017/5/26/multi-domain-confusion-all-domains-are-not-created-equal/>.
Henriksen, Andres. 2019. The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity* 5 (1). Available at <https://doi.org/10.1093/cybsec/tyy009>.
Herrera, Geoffrey L. 2006. *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*. SUNY Press.
Herrera, Geoffrey L. 2007. Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. In *Power and Security in the Information Age*, edited by Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel, 67–93. Ashgate.
Hollis, Duncan B., and Jens David Ohlin. 2018. What If Cyberspace Were for Fighting? *Ethics and International Affairs* 32 (4):441–56.
Hunter, Dan. 2003. Cyberspace as Place and the Tragedy of the Digital Anticommons. *California Law Review* 91 (2):439–520.
Johnson, David R., and David Post. 1996. Law and Borders—The Rise of Law in Cyberspace. *Stanford Law Review* 48 (5):1367–402.
Joint Chiefs of Staff. 2000. Joint Vision 2020. *Joint Forces Quarterly* (Summer):57–76.
Joint Chiefs of Staff. 2004. The National Military Strategy of the United States of America. Available at <https://archive.defense.gov/news/Mar2005/d20050318nms.pdf>.
Joint Chiefs of Staff. 2006. The National Military Strategy for Cyberspace Operations. Available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf>.
Joint Chiefs of Staff. 2018. Joint Publication 3-12: Cyberspace Operations. 8 June 2018. Available at <https://nsarchive2.gwu.edu/dc.html?doc=4560063-Joint-Chiefs-of-Staff-Joint-Publication-3-12>.
Joint Chiefs of Staff. N.d. Joint Publication 1-02. The *Department of Defense Dictionary of Military and Associated Terms*. Older versions available at <http://webapp1.dlib.indiana.edu/virtual_disk_library/index.cgi/4240529/FID3171/ACDOCS/OLD_PUBS/JP1_02.PDF>; current version available at <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.

Kamis, Ben, and Thorsten Thiel. 2015. The Original Battle Trolls: How States Represent the Internet as a Violent Place. PRIF Working Paper No. 23. Peace Research Institute Frankfurt. Available at <https://www.hsfk.de/fileadmin/HSFK/hsfk_downloads/PRIF_WP_23.pdf>.
Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War*. Simon and Schuster.
Karas, Thomas H., Judy H. Moore, and Lori K. Parrott. 2008. Metaphors for Cyber Security. Sandia Report SAND2008-5381.
Kello, Lucas. 2017. *The Virtual Weapon and International Order*. Yale University Press.
Kerttunen, Mika, and Eneken Tikk. 2019. Strategically Normative. Norms and Principles in National Cybersecurity Strategies. Cyber Policy Institute, EU Cyber Direct. April.
Khong, Yuen Foong. 1992. *Analogies at War: Korea, Munich, Dien Bein Phu, and the Vietnam Decisions of 1965*. Princeton University Press.
King, Angus, and Mike Gallagher. 2020. *Cyberspace Solarium Commission*. Available at <https://www.solarium.gov/>.
Kinsella, Helen. 2005. Discourses of Difference: Civilians, Combatants, and Compliance with the Laws of War. *Review of International Studies* 31 (S1):163–85.
Koh, Harold Hongju. 2012. Remarks: International Law in Cyberspace. 18 September. Available at <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm>.
Kratochwil, Friedrich. 1989. *Rules, Norms, and Decisions: On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs*. Cambridge University Press.
Krebs, Ronald R. 2015. How Dominant Narratives Rise and Fall: Military Conflict, Politics, and the Cold War Consensus. *International Organization* 69 (1):1–37.
Krebs, Ronald R., and Patrick Thaddeus Jackson. 2007. Twisting Tongues and Twisting Arms: The Power of Political Rhetoric. *European Journal of International Relations* 13 (1):35–66.
Kreps, Sarah, and Jacquelyn Schneider. 2019. Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics. *Journal of Cybersecurity* 5 (1):1–11.
Lakoff, George, and Mark Johnson. 1980. *Metaphors We Live By*. University of Chicago Press.
Lakoff, George. 1992. The Contemporary Theory of Metaphor. In *Metaphor and Thought*, 2nd ed., edited by Andrew Ortony, 202–51. Cambridge University Press.
Lambach, Daniel. 2020. The Territorialization of Cyberspace. *International Studies Review*. 22 (3):482–506.
Lapointe, Adriane. 2011. When Good Metaphors Go Bad: The Metaphoric "Branding" of Cyberspace. Center for Strategic and International Studies. 9 September.
Larsson, Stefan. 2017. *Conceptions in the Code: How Metaphors Explain Legal Challenges in Digital Times*. Oxford University Press.
Latour, Bruno. 1987. *Science in Action: How to Follow Scientists and Engineers Through Society*. Harvard University Press.
Lawson, Sean. 2012. Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States. *First Monday* 17 (7), 2 July.
Lawson, Sean. 2014. *Nonlinear Science and Warfare: Chaos, Complexity, and the US Military in the Information Age*. Routledge.
Lawson, Sean. 2020. *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Routledge.
Lawson, Sean, and Michael K. Middleton. 2019. Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016. *First Monday* 24 (3), 4 March.
Lemley, Mark A. 2003. Place and Cyberspace. *California Law Review* 91 (2):521–42.
Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. Basic Books.
Libicki, Martin C. 2012. Cyberspace Is Not a Warfighting Domain. *I/S: A Journal of Law and Policy for the Information Society* 8 (2):321–36.
Lindsay, Jon. 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies* 22 (3):365–404.
Lindsay, Jon. 2017. Restrained by Design: The Political Economy of Cybersecurity. *Digital Policy, Regulation and Governance* 19 (6):493–514.

Lucas, George R. 2016. Emerging Norms for Cyberwarfare. In *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser, 13–33. Oxford University Press.
Lupovici, Amir. 2016. The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward. *International Studies Perspectives* 17 (3):322–42.
Lute, Jane Holl, and Bruce McConnell. 2011. Op-Ed: A Civil Perspective on Cybersecurity. *Wired*, 14 February.
Lynn, William J., III. 2010. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs* 89 (5):97–108.
Maglio, Paul P., and Teenie Matlock. 1998. Metaphors We Surf the Web By. *Proceedings of Workshop on Personalized and Social Navigation in Information Space* (1–9). Swedish Institute of Computer Science. Available at <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.49.6289&rep=rep1&type=pdf>.
Manjikian, Mary. 2010. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly* 54 (2):381–401.
Manjikian, Mary. 2015. *Confidence-Building in Cyberspace: A Comparison of Territorial and Weapons-Based Regimes*. Strategic Studies Institute and US Army War College Press.
Manjikian, Mary. 2016. *Deterring Cybertrespass and Securing Cyberspace: Lessons from United States Border Control Strategies*. Strategic Studies Institute and US Army War College Press.
Matlock, Teenie, Spencer C. Castro, Morgan Fleming, Timothy M. Gann, and Paul P. Maglio. 2014. Spatial Metaphors of Web Use. *Spatial Cognition and Computation* 14 (4):306–20.
Maurer, Tim. 2020. A Dose of Realism: The Contestation and Politics of Cyber Norms. *Hague Journal on the Rule of Law* 12: 283–305. Available at <https://doi.org/10.1007/s40803-019-00129-8>.
Mayer, Maximilian, Mariana Carpes, and Ruth Knoblich, eds. 2014. *The Global Politics of Science and Technology*. 2 vols. Springer.
McCarthy, Daniel R. 2017. *Technology and World Politics: An Introduction*. Routledge.
McCarthy, Daniel R. 2018. Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order. *Politics and Governance* 6 (2):5–12.
Milliken, Jennifer. 1999. The Study of Discourse in International Relations: A Critique of Research and Methods. *European Journal of International Relations* 5 (2):225–54.
Mueller, Milton. 2017a. Is Cybersecurity Eating Internet Governance? Causes and Consequences of Alternative Framings. *Digital Policy, Regulation and Governance* 19 (6):415–28.
Mueller, Milton. 2017b. *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*. Polity.
Mueller, Milton. 2019. Against Sovereignty in Cyberspace. *International Studies Review*. <https://doi.org/10.1093/isr/viz044>.
Nakasone, Paul M. 2019a. An Interview with Paul M. Nakasone. *Joint Forces Quarterly* 92 (1):4–9.
Nakasone, Paul M. 2019b. A Cyber Force for Persistent Operations. *Joint Forces Quarterly* 92 (1):10–14.
Nakayama, Bryan. 2019. Air, Land, Sea, Space … and Cyberspace? The Development of Military Domains. Unpublished paper.
National Defense Authorization Act (NDAA) for Fiscal Year 2019, Pub L. No. 115-232 132 Stat. 1636.
National Security Act of 1947, Pub L. No. 80-253 61 Stat. 495.
National Security Agency (NSA). 1995. SIGINT and INFOSEC in Cyberspace. *Cryptolog*. Available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-008.pdf>.
North Atlantic Treaty Organization. 2014. Wales Summit Declaration. 5 September. Available at <https://www.nato.int/cps/ic/natohq/official_texts_112964.htm>.
Nye, Joseph S. Jr. 2011. Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly* 5 (4):18–38.
Onuf, Nicholas G. 1989. *World of Our Making: Rules and Rule in Social Theory and International Relations*. University of South Carolina Press.
Onuf, Nicholas G. 2013. *Making Sense, Making Worlds: Constructivism in Social Theory and International Relations*. Routledge.
Osenga, Kristen. 2013. The Internet Is Not a Super Highway: Using Metaphors to Communicate Information and Communications Policy. *Journal of Information Policy* 3:30–54.
People's Republic of China. 2015. China's Military Strategy. Available at <http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm>.

Perkovich, George, and Ariel E. Levite, eds. 2017. *Understanding Cyber Conflict: Fourteen Analogies*. Georgetown University Press.
Quadrennial Defense Review (QDR). Available at <http://history.defense.gov/Historical-Sources/Quadrennial-Defense-Review/>.
Raymond, Mark. 2019. *Social Practices of Rule-Making in World Politics*. Oxford University Press.
Raymond, Mark. 2020. Social Practices of Rule-Making for International Law in the Cyber Domain. *Journal of Global Security Studies*. doi:10.1093/jogss/ogz065.
Raymond, Mark, and Laura DeNardis. 2015. Multistakeholderism: Anatomy of an Inchoate Global Institution. *International Theory* 7 (3):572–616.
Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford University Press.
Rid, Thomas. 2016. *Rise of the Machines: A Cybernetic History*. W.W. Norton.
Rid, Thomas, and Ben Buchanan. 2018. Hacking Democracy. *SAIS Review* 38 (1):3–16.
Risse, Thomas. 2000. "Let's Argue!" Communicative Action in World Politics. *International Organization* 54 (1):1–39.
Sandholtz, Wayne. 2008. Dynamics of International Norm Change: Rules Against Wartime Plunder. *European Journal of International Relations* 14 (1):101–31.
Sauter, Molly. 2015. Show Me on the Map Where They Hacked You: Cyberwar and the Geospatial Internet Doctrine. *Case Western Reserve Journal of International Law* 47 (1):63–78.
Schmidt, Vivien A. 2008. Discursive Institutionalism: The Explanatory Power of Ideas and Discourse. *Annual Review of Political Science* 11:303–26.
Schmitt, Michael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press.
Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
Schneider, Jacquelyn G. 2019. Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy. *Lawfare*. 10 May. Available at <https://www.lawfareblog.com/persistent-engagement-foundation-evolution-and-evaluation-strategy>.
Schön, Donald A. 1993. Generative Metaphor: A Perspective on Problem-Setting in Social Policy. In *Metaphor and Thought*. 2nd ed, edited by Andrew Ortony, 137–63. Cambridge University Press.
Secretary of Defense. 2009. Memorandum: Establishment of a Subordinate Unified US Cyber Command Under US Strategic Command for Military Cyberspace Operations. 23 June. Available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf>.
Semino, Elena. 2008. *Metaphor in Discourse*. Cambridge University Press.
Sheniak, Amit. 2014. The Emergence of the State in the Online Frontier: A Theoretical and Historical Comparison. *Dado Journal for Operational Art* 3:10–45.
Smeets, Max W.E., and Herbert Lin. 2018. A Strategic Assessment of the US Cyber Command Vision. In *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Herbert Lin and Amy Zegart, 81–104. Brookings Institution Press.
Stevens, Tim. 2016. *Cyber Security and the Politics of Time*. Cambridge University Press.
Sulmeyer, Michael. 2017. Much Ado About Nothing? Cyber Command and the NSA. *War on the Rocks* 19 July. Available at <https://warontherocks.com/2017/07/much-ado-about-nothing-cyber-command-and-the-nsa/>.
Tikk, Eneken, and Mika Kerttunen. 2018. Parabasis: Cyber-diplomacy in Stalemate. NUPI Policy Brief 5/2018.
Townes, Miles. 2012. The Spread of TCP/IP: How the Internet Became the Internet. *Millennium* 41 (1):43–64.
United Kingdom Cabinet Office. 2009. Cyber Security Strategy of the United Kingdom. Available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf>.
United Nations General Assembly (UNGA). 2013. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/68/98. 24 June. Available at <https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98>.
United Nations General Assembly. 2015. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. 22 July. Available at <https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174>.

United States Air Force. 1995. Cornerstones of Information Warfare. Available at <https://catalog.hathitrust.org/Record/101681332>.
United States Air Force. 2011. Air Force Doctrine Document 3-12: Cyberspace Operations, Incorporating Change 1 (30 November). Available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-060.pdf>.
United States Army. 2010. Cyberspace Operations Concept Capability Plan 2016–2028. 22 February. Available at <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-033.pdf>.
United States Coast Guard. 2015. United States Coast Guard Cyber Strategy. Available at <https://nsarchive2.gwu.edu//dc.html?doc=2692134-Document-26>.
United States Cyber Command. 2016. Order: To Establish Joint Task Force (JTF)-ARES to Counter the Islamic State of Iraq and the Levant (ISIL) in Cyber Space. 5 May. Available at <https://nsarchive2.gwu.edu//dc.html?doc=3678213-Document-07-USCYBERCOM-to-CDRUSACYBER-Subj>.
United States Cyber Command. 2018. Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command. Available at <https://nsarchive2.gwu.edu//dc.html?doc=4421219-United-States-Cyber-Command-Achieve-and-Maintain>.
United States Navy. 2012. Navy Cyber Power 2020. Available at <https://nsarchive2.gwu.edu//dc.html?doc=2692124-Document-16>.
United States Strategic Command. 2009. The Cyber Warfare Lexicon. 5 January. Available at <https://nsarchive2.gwu.edu//dc.html?doc=2692102-Document-1>.
Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.
Vinge, Vernor. 1981. *True Names*. Dell.
Wagner, Ben. 2019. Constructed "Cyber" Realities and International Relations Theory. In *Science, Technology, and Art in International Relations*, edited by J.P. Singh, Madeline Carr, and Renee Marlin-Bennett, 60–70. Routledge.
Warner, Michael. 2012. Cybersecurity: A Pre-history. *Intelligence and National Security* 27 (5):781–99.
Warner, Michael. 2015. Notes on Military Doctrine for Cyberspace Operations in the United States, 1992–2014. *The Cyber Defense Review*, 27 August.
White House. 1984. National Security Decision Directive Number 145: National Policy on Telecommunications and Automated Information Systems Security. 17 September. Available at <https://fas.org/irp/offdocs/nsdd145.htm>.
White House. 1997. Critical Foundations: Protecting America's Infrastructures. Available at <https://fas.org/sgp/library/pccip.pdf>.
White House. 2012. Presidential Policy Directive/PPD-20: US Cyber Operations Policy. 16 October. Available at <https://nsarchive2.gwu.edu/dc.html?doc=2725521-Document-2-9>.
Yen, Alfred C. 2002. Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace. *Berkeley Technology Law Journal* 17 (4):1207–63.
Zeng, Jinghan, Tim Stevens, and Yaru Chen. 2017. China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty." *Politics and Policy* 45 (3):432–64.

Author

Jordan Branch is Assistant Professor of Government at Claremont McKenna College in Claremont, CA. He can be reached at jordan.branch@cmc.edu.

Acknowledgments

I thank the editors of *IO*, the anonymous reviewers, Jonathan Caverley, Peter Dombrowski, Helen Kinsella, Ron Krebs, Sean Lawson, Helen Lee, Jon Lindsay, Bryan Nakayama, Abe Newman, John Savage, Jacquelyn Schneider, Amit Sheniak, Max Smeets, Tim Stevens, the staff at the National Security

Archive, and the participants and audiences where earlier versions of this article were presented: the University of Wisconsin, the University of Minnesota, Cambridge University, the Norwegian Institute of International Affairs, the Naval War College, Yale University, King's College London, Marquette University, the University of Connecticut, Georgetown University, Santa Clara University, Claremont McKenna College, and the 2018 International Studies Association meeting.

Key Words

Cybersecurity; metaphor; language; United States; civil-military relations; information technology

Date received: May 13, 2019; Date accepted: July 6, 2020