Air, land, sea, space... and cyberspace? The development of military domains

Bryan James Nakayama
Department of International Relations, Mount Holyoke College, South Hadley, United States
Please direct all correspondence to bnakayam@mtholyoke.edu

Author Information

Bryan James Nakayama is a visiting lecturer in the Department of International Relations at Mount Holyoke College in South Hadley, Massachusetts.

Air, land, sea, space... and cyberspace? The development of military domains

Abstract

Why is cyberspace—an abstraction of information infrastructure—considered a military domain by the U.S. alongside the geographical spaces of air, land, sea, and orbital space? While puzzling, scholars working on cyberspace and international security have taken this state of affairs as a given even though other states, such as Russia, do not treat cyberspace in the same manner. In this paper, I resolve this question by first arguing that military domains should be understood as institutionalized social facts. Second, I theorize that domains are institutionalized in the U.S. military through a bottom-up process of domain advocacy by servicemembers. To demonstrate my theoretical claim, I present two case studies on the development of the air and cyberspace as domains, revealing the decisive role that domain advocacy played. A key implication of my argument is that the role of domains in warfare is not inevitable but rather contingent on domain advocacy.

Keywords

cyberspace, cyberwarfare, airpower, technology, military domain

Word Count

14488

Air, land, sea, space…and cyberspace? The development of military domains

Introduction

Why is cyberspace—an abstraction used to describe global information infrastructure—considered a domain of warfare by the U.S. military alongside the geographical spaces of air, land, sea, and orbital space?[1] This tension has not gone unnoticed by the U.S. military, in 2011 retired General Michael Hayden wrote that "the other domains are natural, created by God, and this one is the creation of man.… Are these differences important enough for us to rethink our doctrine?" [2] Regardless of this tension, treating cyberspace as a domain is a core feature of the U.S. approach to cyberwarfare, Deputy Secretary of Defense William Lynn III in 2010 hailed creation of U.S. Cyber Command (USCYBERCOM) as a critical step towards institutionalizing cyberspace as a military domain by laying the groundwork for a dedicated force structure and body of doctrine.[3] However, this outcome was neither inevitable nor obvious, in early 2011 two high ranking officials from the Department of Homeland Security disputed Lynn's premise that cyberspace was a domain, stating unequivocally that "cyberspace is fundamentally a civilian space—a neighborhood, a library, a marketplace, a school yard, a workshop—and a new, exciting age in human experience, exploration and development" it "is not a warzone."[4] More recently, Martin Libicki, contrasting the much greater significance of electronic warfare in the RF spectrum with cyberspace operations argues that it is unclear why cyberspace should be accorded the status of domain instead of the RF

[1] For the purpose of U.S. cyberspace operations, cyberspace is described in Joint Doctrine (JP 3-12) using a three-layer model: first, physical, which describes the cables, switches, computers, and other hardware infrastructure. Second, logical, the data and code that exists on and enables operation of the physical infrastructure. Lastly, the "cyber-persona" layer, "digital representations of an actor or entity identity in cyberspace." Joint Chiefs of Staff, *JP 3-12 Cyberspace Operations* (Chairman of the Joint Chiefs of Staff, 2018), I2-I4

[2] Michael V. Hayden, "The Future of Things "Cyber"," *Strategic Studies Quarterly* 5, no. 1 (2011): 4

[3] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (2010): 97–108

[4] Jane Holl Lute and Bruce McConnell, "OP-ED: A CIVIL PERSPECTIVE ON CYBERSECURITY," *Wired Magazine*, February 14, 2011, accessed February 22, 2012, `https://www.wired.com/2011/02/dhs-op-ed/`

spectrum.[5] This question lies at the center of a foundational debate over the effects of cyberspace on international security—whether it should be understood as a separate, unique, and highly consequential medium of conflict or if it is just a set of distinctive missions and/or capabilities.

In this paper I answer this question by accomplishing two tasks: first, conceptualizing domains as an institutional formation enabling comparison between cyberspace the "natural domains." Second, I present an argument that technologically mediated military domains—air, space, cyberspace—develop as institutional formations through bottom-up domain advocacy by military officers who seek to operationalize in organizational forms, doctrine, and technological capabilities a vision of a new domain-specific way of warfare. In order to demonstrate my argument, I provide two case studies, air and cyberspace, that draw on archival materials, doctrine, memoirs, and other documentary sources. A key implication of my argument is that the existence and role of technologically mediated military domains in warfare is contingent, how a domain is conceived and operationalized by a specific military is dictated by a social process rather than technological inevitability. Cross-national variation over the role of cyberspace in warfare exposes this contingency, whereas the U.S. focuses on cyberspace operations "within and through" information infrastructure, Russia focuses on information operations, integrating cyber and non-cyber capabilities.[6] U.S. Senator Mark Warner identified this difference as the reason why the U.S. failed to effectively anticipate and counter the Russian information operation campaign against the 2016 presidential election.[7] Ironically, during the 1990s the U.S. military emphasized a similar conception of information operations but the work of cyber-advocates led to the institutionalization of the cyberspace domain instead. Therefore, how a domain is envisioned by advocates not only impacts patterns of institutionalization but also how states interpret their threat environment. The argument

[5]Martin Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016), 156

[6]Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (New York, NY: Oxford University Press, 2018), 143; P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York, NY: Eamon Dolan Books, 2018)

[7]Mark Warner, *Warner Calls for Society-Wide Cyber Doctrine*, 2018, accessed December 14, 2018, `https://www.warner.senate.gov/public/index.cfm/2018/12/warner-calls-for-society`

that I develop in this paper not only addresses the puzzle of how cyberspace has become a military domain for the U.S. but also explains the roots of this cross-national variation. Overall, my argument in this paper is that domains should be understood as contingent institutional formations that are produced through bottom-up advocacy—in other words, militaries do not find and exploit domains, advocates make them.

Scholars working on international security have largely treated military domains as exogenous—taking the spatial divisions of warfare as inevitable. This is a significant oversight as the military domain is a fundamental organizing category of warfare which affects patterns in military organization, capabilities, and ways of warfare, for example Air Force/airpower/air, Navy/seapower/sea, and Army/landpower/land.[8] Furthermore, military domain status is part of the "common sense" of warfare, structuring grand strategy and informing the norms, treaties, and laws that govern the practices of interstate conflict.[9] As I will demonstrate in my case studies, the belief that aircraft served as a unique instrument and way of conducting war was deeply contested by early 20th century military leaders; likewise there is nothing about cyberspace, a concept to describe information infrastructure, that necessitated the logic of military conflict as opposed to an information assurance, counter-espionage, or covert/clandestine service approach. The institutionalization of a new military domain is a large-scale shift in the available levers of military power and the nature of the security environment, understanding how they come to exist is critical to understanding the relationship between technology and international security.

[8]Erik Heftye, "Multi-Domain Confusion: All Domains Are Not Created Equal," 2017-07-10, May 26, 2017, https://thestrategybridge.org/the-bridge/2017/5/26/multi-domain-confusion-all-domains-are-not-created-equal; F.G. & Davies M.C. Hoffman, "Joint Forces 2020 and the Human Time: Time for a New Conceptual Framework," *Small Wars Journal*, 2013, accessed July 10, 2017, http://smallwarsjournal.com/jrnl/art/joint-force-2020-and-the-human-domain-time-for-a-new-conceptual-framework; Joseph S Nye Jr, *Cyber power* (Cambridge, MA: Belfer Center for Science / International Affairs, 2010), 4; Joseph S Nye Jr, "Nuclear Lessons for Cyber Security?," *Strategic Studies Quarterly* 5, no. 4 (2011): 31-32

[9]Michael Hayden argues that "domain" is a perceptual schema. Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York, NY: Penguin, 2016), 128. Martin Libicki highlights that domain status implies strategic theory. Libicki, *Cyberspace in Peace and War*, 165-166. Barry Posen highlights how the "command of the commons"—air, space, and sea—is a core part of U.S. hegemonic strategy. Barry R. Posen, "Command of the Commons," *International Security* 28, no. 1 (2003): 5–46

So as to accomplish two tasks that I outlined—conceptualizing "domain" and providing an explanation for the development thereof—the paper will unfold in the following fashion: first, I will demonstrate that scholarship which exogenizes the domain status of cyberspace obfuscates important dynamics by ignoring how and why the U.S. treats cyberspace as a medium of conflict. Instead of treating domains as a pre-existing space that the U.S. military operationalizes, I propose that they should be understood as institutionalized social facts thereby enabling a deeper assessment of the role of cyberspace in international security. Then, I explain my theory of domain development wherein I claim that domains are institutionalized by military domain advocates, working from the bottom-up. Following that, I demonstrate my theory of domain development with two cases—air and cyberspace. For both, I reveal how patterns in their institutionalization were a contingent consequence of domain advocacy. I conclude the paper by identifying key avenues for further research into military domains and substantive implications.

Domains and the Limits of Exogenizing Cyberspace

Despite its frequent usage and foundational importance "domain" as a concept is little discussed both within U.S. Department of Defense documentation and scholarship on international security.[10] This lacuna is reflected in the literature on cyberspace and international security, which has not addressed the role that the U.S. military has played in *making* cyberspace a military domain. Literature that directly addresses cyberspace as a domain has only focused on the normative question of whether it is beneficial for the U.S. military to treat cyberspace as a domain, instead of explaining *why* cyberspace is considered a domain of warfare.[11] This is because cyberspace, as a potential

[10] The *DOD Dictionary of Military and Associated Terms* provides definitions for the "air domain," "cyberspace," "land domain," and "maritime domain" but not "domain" itself. Department of Defense, *DOD Dictionary of Military and Associated Terms*, Joint Electronic Library, February 1, 2018, 12, 137, 200, accessed March 10, 2018, `http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf`

[11] Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*; Hayden, "The Future of Things "Cyber""; Martin Libicki, "Cyberspace is a not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society* 8, no. 1 (2012): 321–336; Martin Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist," *Strategic Studies Quarterly* 14, no. 1 (Spring 2014): 23–39; Libicki, *Cyberspace in Peace and War*; Thomas Rid, *Cyber War Will Not Take Place* (New York, NY: Oxford University Press, 2013)

arena of inter-state interaction, is naturalized within the cyberspace and security literature. As Christopher Whyte notes: "a core assumption of cyber conflict scholars" is that "dynamics of digital politics diverge... because of the exogenous determinants of such effects."[12] The assumption that cyberspace, a concept for describing information infrastructure, is naturally a security arena serves as one of the core assumptions of the cyber-security literature.[13] By viewing cyberspace in this manner, existing literature cannot grapple with consequential cyber-international security dynamics such as cross-national variation in the role of cyberspace vis-a-vis information warfare and why warfare in cyberspace rose to prominence for the U.S. military. My approach deepens our understanding of cyber-international security dynamics both by demonstrating why cyberwarfare overtook information warfare and by placing cyberspace into a comparative framework.

The literature on cyberspace and international security is roughly divided into two competing camps—revolutionists and evolutionists—both of which naturalize the role of cyberspace as a domain for international security.[14] Revolutionists argue that cyberspace upends traditional security dynamics because of its unique complexity which empowers revisionist actors, undermines deterrence, and creates the potential for powerful asymmetric attacks against major powers deeply dependent on cyberspace.[15] The revolutionary literature draws attention to reactive dynamics—asking how states will manage the challenges imposed by cyberspace—thereby obfuscating the

[12]Christopher Whyte, "Dissecting the Digital World: a Review of the Construction and Constitution of Cyber Conflict Research," *International Studies Review* 20, no. 3 (2018): 521

[13]Scholars outside of security studies have considered the role that politics have played in the constitution of cyberspace. For example, Laura Denardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge, Massachussetts: MIT Press, 2009); Laura Denardis, *Global War for Internet Governance* (New Haven, CT: Yale University Press, 2014); Daniel R McCarthy, *Power, information technology, and international relations theory: The power and politics of US Foreign policy and internet* (London, UK: Palgrave Macmillan, 2015)

[14]I borrow this framing from Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404; Lucas Kello, *The Virtual Weapon and International Order* (New Haven, CT: Yale University Press, 2017); Valeriano, Jensen, and Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*

[15]Susan W. Brenner, *Cyberthreats and the Decline of the Nation-State* (New York, NY: Routledge, 2014); Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York, NY: Ecco, 2011); Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: MIT Press, 2012); Kello, *The Virtual Weapon and International Order*; Dennis F. Poindexter, *The New Cyberwar: Technology and the Redefinition of Warfare* (New York, NY: McFarland, 2015); Gabriel Weimann, *Terrorism in Cyberspace: The Next Generation* (Washington, DC: Woodrow Wilson Center Press, 2015)

critical empirical question of how cyberspace has come to be treated as a medium of conflict. While these authors have prospectively identified important potential challenges, cyberspace is not independent of human activity and militaries play a core role in defining how cyberspace, as a sphere of conflict, will alter security. By placing cyberspace into a comparative framework, my argument enables clearer assessment of whether cyberspace revolutionizes international security.

Opposed to the revolutionists are the evolutionists who argue that cyberspace and cyber-capabilities have not and are unlikely to revolutionize security dynamics. Largely working from an empirical basis, these scholars have argued that the actual effects of attacks are modest, cyber-capabilities are just new means for old missions, and that existing conceptual constructs—with some modification—are able to adequately explain cybersecurity dynamics.[16] Taking a broader view, others have argued that far from destabilizing security, cyber-competition between states has been defined by restraint and caution.[17] However, if the effects of cyberspace on security have thus far been modest it sharpens the core question as to why the U.S. military treats cyberspace as equivalent in significance to the air, land, and sea.

This question has been partially addressed by scholars through the lens of securitization, by examining the rhetorical construction of cyber-threats and discourse over critical infrastructure.[18]

[16]Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–481; Ben Buchanan, *Cybersecurity Dilemma: Network Intrusions, Trust and Fear in the International System* (New York, NY: Oxford University Press, 2017); Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (2013): 41–73; Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24, no. 2 (2015): 316–348; Nadiya Kostyuk and Yuri M. Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?," *Journal of Conflict Resolution*, 2017, 1–31, doi:10.1177/0022002717737138; Lindsay, "Stuxnet and the Limits of Cyber Warfare"; Travis Sharp, "Theorizing cyber coercion: The 2014 North Korean operation against Sony," *Journal of Strategic Studies* 40, no. 7 (2017): 898–926; Rid, *Cyber War Will Not Take Place*; Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2017): 72–109

[17]Brandon Valeriano and Ryan C Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York, NY: Oxford University Press, 2015); Valeriano, Jensen, and Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*

[18]Myriam Dunn Cavelty, *Cyber-security and threat politics: US efforts to secure the information age* (London, UK: Routledge, 2007); Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, no. 53 (2009): 1155–1175; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-threats," *Journal of Information Technology and Politics* 10, no. 1 (2013): 86–103

There is also a growing body of historical literature but that has largely been either descriptive or limited in scope to specific capabilities, individuals, or time periods.[19] These studies have made substantial contributions in understanding the evolution of strategy and specific capabilities but they have failed to explain why cyberspace came to be viewed as equivalent to the geographic domains in strategy and tactics. In my case studies, I provide a focused account of the evolution of the U.S. military understanding of cyberspace by tracing the relationship between domain conceptions of cyberspace and organizational development. This paper contributes to this growing body of empirical scholarship by providing both a theory that explains why cyberspace has come to be treated as equivalent to air, land, and sea as well as an empirical account that provides a focused comparison between the development of the air and cyberspace domains.

In order to grapple with these unresolved questions, I treat military domains, not as spaces that come to be exploited by a military, but rather as an institutional formation of specialized organizations, doctrine, service identity, and technological capabilities premised on a vision of a spatially distinct way of war. This definition is useful for two reasons: first, the U.S. and other great powers structure militaries around the basic spatial divisions of air, land, and sea—with separate service branches for orbital space and cyberspace being debated.[20] Domain-specific warfare is intimately connected to institutional formations: a major military domain will have a dedicated highly autonomous military organization. This can be seen in U.S. President Donald Trump's call to create a "Space Force" that is "separate but equal" to the Air Force, arguing only that a dedi-

[19] Ronald J. Deibert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (New york, NY: Penguin, 2013); Fred Kaplan, *Dark Territory: The Secret History of Cyberwar* (New York, NY: Simon / Schuster, 2016); Jason Healey, *A Fierce Domain: Conflict in Cyberspace 1986-2012* (Baltimore, MD: The Atlantic Council, 2013); Shane Harris, *@War: The Rise of the Military-Internet Complex* (New York, NY: First Mariner Books, 2015); Brian M Mazanec, *The Evolution of Cyber War: International Norms for Emerging-technology Weapons* (Lincoln, NE: University of Nebraska Press, 2015); Kim Zetter, *Countdown to Zero Day* (New York, NY: Crown, 2014)

[20] During the Republican primary for the 2016 election, candidate Marco Rubio advocated for the creation of a separate Cyber Department.Gizmodo Staff, "The 2016 Presidential Candidates' Views on Cyber Warfare," *Gizmodo*, March 1, 2016, accessed March 2, 2016, `https://gizmodo.com/the-2016-presidential-candidates-views-on-cyber-warfare-1760899365` Likewise, the Israeli IDF studied and ultimately rejected the potential for a Cyber Branch. John Ahronheim, "IDF Decides Not to Have a Cyber Command Department," January 1, 2017, accessed July 22, 2017, `https://www.jpost.com/Israel-News/IDF-decides-not-to-have-a-cyber-command-department-477169`

cated service department could ensure "American dominance in space."[21] Second, understanding domains in this way allows for meaningful comparisons between cyberspace and the geographic domains by drawing attention to comparative trends in strategy, tactics, doctrine, organizational autonomy, capabilities acquisition, and socialization. Understanding a domain in this fashion reveals that how they are understood by militaries is contingent; USCYBERCOM historian William Nolte, reflecting on the U.S. military experience with cyberspace, notes that "domains are not self-defining."[22] Consequently, a key implication of this approach is that the role of technologically mediated domains—air, orbital space, and cyberspace—in warfare is contingent on how they are institutionalized.

Theory of Domain Development

In order to explain the contingent development of new technologically mediated domains, I argue that they are the consequence of a bottom-up process of domain advocacy by military officers who seek to institutionalize their domain vision of spatially distinct warfare in organization, doctrine, and capabilities. A new domain, therefore, does not pre-exist military exploitation, rather, it is the outcome of a long-term process which has two stages: first, the advocates succeed in developing what I term a support domain which is a semi-autonomous military institutional formation responsible for spatially distinct activity in support of operations in another domain. For example, orbital space and cyberspace are currently institutionalized as support domains. Second, a strategic domain, which is a highly autonomous institutional formation, such as a service department responsible for practicing a spatially distinct way of warfare. Air, land, and sea because of their powerful service departments, distinct training, and bodies of doctrine are strategic domains. These two stages mark the progress of domain advocates in advancing their domain vision—a cluster of

[21] William Harwood, *Trump Directs Pentagon to create military Space Force*, CBS News, June 18, 2018, accessed June 20, 2018, `https://www.cbsnews.com/news/trump-space-force-pentagon-create-military-space-force-national-space-council-meeting-2018-06-18/`

[22] William M. Nolte, "Anticipating Cyberspace Security: NSA's Experience 1992-1997," *Cryptologic Quarterly*, 2012, 47

beliefs that undergirds doctrine and organizational structure. Domain visions center on the belief that an emerging domain-enabling technology allows for the pursuit of a new and distinct way of warfare that breaks with the role and capacity of extant security institutions. Therefore, a domain vision is not a rational assessment of the potentials and limits of a domain-enabling technology, but rather a belief system about the potentials of a spatially distinct way of warfare. The prospective nature of domain visions are what drive contingency in domain institutionalization.

The domain vision plays a crucial role in the institutionalization of a new domain by providing the foundation for a distinct organizational culture. This culture plays two important roles: first, realizing the domain vision through the creation of organizational forms and doctrine motivates the visionary advocacy of the domain advocates. Rather than a cool-headed technological assessment, a domain vision for the advocates is a prophetic dream to be realized. Second, the domain vision has a binding effect for the advocates by defining relationships with other domains and services, providing a shared worldview, as well as generating a common language and assumptions thereby forming a shared orthodoxy about the role of the new domain.[23] This shared orthodoxy serves to distinguish the domain advocates from their parent service and drives the desire for a new and autonomous organizational structure and body of doctrine.

Domain advocates refine and advance their domain vision by debating and crafting doctrine as well as building alliances with senior officers and civilian leaders to achieve organizational and doctrinal autonomy. However, domain advocates are only successful under certain conditions: first, the domain advocates begin as mid- or low-level officers utilizing the domain-enabling technology before a formal military unit to operate the technology in warfare has been created. The status of domain advocates as mid- and low-level officers means that they have greater freedom in conceptualizing the uses of a domain-enabling technology because they are not as indebted to their parent service as senior officers. Military hierarchies provide prescriptive guidelines over

[23]Carl H Builder, *The Masks of War: American Military Styles in Strategy and Analysis* (Baltimore, MD: Johns Hopkins University Press, 1989); David E. Johnson, *Fast Tanks and Heavy Bombers: Innovation in the U.S. Army 1917-1945* (Ithaca, NY: Cornell University Press, 1998), 54

all aspects of their member's lives and possess a pyramidal structure whereby promotion and advancement only occur internally within a single service branch which places a premium on officers conforming to a service's orthodoxy.[24] Therefore, senior officers of a service department have a deep allegiance to their service's domain conception of warfare, Carl Builder demonstrates that the organizational identity of a service department, Air Force, Army, and Navy, is founded on both the service's domain conception of war.[25] Therefore, lower-level officers are freer to develop and advance a radically new way of warfare within and through a new space. For the advocates, generating increasingly autonomous organizations and independent bodies of doctrine is imperative for realizing their domain vision.

Second, the senior officers of the service must have an ambivalence towards the role and status of the domain-enabling technology during the early stages of development—by "ambivalence" I meant that the senior leadership does not exert tight control over the activities of the domain advocates. This is critical because if senior officers seek tight control over the development and use of the technology, it will bind the domain-enabling technology into the existing service conception of war resulting in the sticky institutionalization of a support domain. Of course, senior officers will be interested in the new technology and may integrate it into existing doctrine but there is a difference between rhetoric and intense interest/guidance. Senior officer ambivalence is decisive during the period of development preceding the institutionalization of a support domain, this is because after the advocates have succeeded in creating a semi-autonomous spatially distinct military organization they are both less beholden to senior leadership and able to garner greater legitimacy for their domain vision. For example, the Air Force, Army, and Navy repeatedly jockeyed over space technologies in the decade preceding the Sputnik launch. One consequence of this jockeying

[24]Samuel P. Huntington, *The Common Defense: Strategic Programs in National Politics* (New York, NY: Columbia University Press, 1961), 404-407; William A Lucas and Raymond H. Dawson, *The Organizational Politics of Defense* (Pittsburgh, PA: ISA, 1974); Stephen Peter Rosen, "New Ways of War: Understanding Military Innovation," *International Security* 13, no. 1 (1988): 136-141; Harvey Sapolsky, "On the Theory of Military Innovation," *Breakthroughs* IX, no. 1 (2000): 37

[25]Builder, *The Masks of War: American Military Styles in Strategy and Analysis*

is that the Air Force senior leadership articulated orbital space as an extension of the air domain—Aerospace. This combined with intense service leader interest meant that space advocates were bound to their parent service's conception of space as a support domain.[26] This has had the consequence that the institutionalization of space as a support domain has remained sticky. Whereas ambivalence allows the domain advocates to influence the perceived role of the domain-enabling technology in warfare as they develop employment concepts and bodies of doctrine. Overall, the institutionalization of a domain vision by domain advocates is necessarily a bottom-up process because the development of a new domain necessitates the creation of organizational forms and bodies of doctrine which support a new and distinct conception of war.[27]

Case Studies: Air and Cyberspace

In order to demonstrate that military domains are institutionalized domain visions developed through advocacy rather than spaces discovered and operationalized by the U.S. military, I present two case studies—air and cyberspace. Before proceeding to the case studies, I first discuss the rationale behind selecting these cases. Second, I proceed to the air case study which examines the period from 1909-1947, revealing that an organizationally independent air force was the consequence of Army air advocates seeking to institutionalize their vision of strategic air warfare. Third, I reveal that the development of cyberspace into a domain was accomplished by U.S. Air Force advocates, who nurtured and drove forward the institutionalization of cyberwarfare against a dominant emphasis on information warfare.

[26]Dwayne Day, "Invitation to Struggle: The History of Civilian-Military Relations in Space," in *Exploring the Unknown: Selected Documents in the History of the U.S. Civil Space Program Volume II: External Relationships*, ed. John Logsdon et al. (Washington, D.C.: NASA History Office, 1996), 233–270; Stephen M. Rothstein, "Ideas as Institutions: Explaining the Air Force's Struggle with its Aerospace Concept" (PhD diss., The Fletcher School of Law and Diplomacy, 2006)

[27]This is not to imply that military organizations are stodgy and resistant to change, Kimberly Zisk and Benjamin Jensen have both demonstrated how militaries are capable of internally driven change. Benjamin Jensen, *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford, CA: Stanford Security Studies, 2016); Kimberly Zisk, *Engaging the Enemy: Organization Theory and Soviet Military Innovation, 1955-1991* (Princeton, NJ: Princeton University Press, 1993)

Case Construction

I selected air and cyberspace for three reasons: first, air represents a hard case for my theoretical claim that domains are institionalized social facts won through advocacy rather than an exogenous factor in the conduct of warfare because if domains were exogenous features of the global security environment then we should expect that the rise of the air domain as an institutional formation would be the consequence of rational assessment of the security environment or technology. Cyberspace is an easy case because of its abstract and constructured nature, treating information infrastructure as a military domain equivalent to geographic spaces is not an obvious outcome. Second, these two case studies each demonstrate a stage in the development of a new domain—the air is currently a strategic domain because the Air Force is a highly autonomous service department dedicated to a spatially distinct form of warfare whereas cyberspace is currently a support domain as USCYBERCOM is a semi-autonomous functional command that based on an infrastructural conception of cyberspace. Finally, these cases provide a useful contrast between the development of technologically-mediated geographic domains and the human-built geographical domain of cyberspace revealing the extent to which the rise to prominence of cyberspace was the consequence of visionary advocacy rather than the "discovery" of cyberspace by militaries.

In constructing the case studies I draw primarily on archival and other primary sources such as published doctrine, service journal articles, congressional testimony, memoirs, and organizational histories where available. These sources allow me to evaluate the motives of domain advocates, the attitude of senior officers towards the domain-enabling technology, and the institutionalization of a domain vision in doctrine and organization. In order to demonstrate that domain advocates were determinative in evolving organization and doctrine for a new domain, I reconstruct the temporal sequencing of the development of organizational forms and the domain vision. I expect that organizational developments won by the advocates should lag the evolution of the domain vision. Likewise, doctrine over time should increasingly conform to the domain vision

as advocates gain greater control over its formulation. However, if there is evidence that senior officers repeatedly asked the advocates to explore specific ideas or that doctrinal concepts were developed through close attention to technological evaluations then that will serve to disprove my theory.

Air

The air is a strategic domain with all major great powers maintaining sizable standing forces for independent strategic warfare within and through the air. In the following case, I first chart the development of doctrine and organization from the acceptance of the first aircraft by the War Department in 1909 to the activation of the semi-autonomous General Headquarters–Air Force in 1935 which institutionalized the air as a support domain. Due to the ambivalence of War Department leadership, over this period the first Army aviators developed a domain vision that aircraft provided a fundamentally new and distinct way of war. Second, I show how the advocates utilized alliances to institutionalize this new way of warfare in organization, doctrine, and capabilities culminating in the creation of the Department of the Air Force in 1947.

Acquisition to Support Domain: 1909-1935

While there was little enthusiasm in the War Department General Staff for aircraft at the beginning of the 20th century, the first Army aviators came from a world where aircraft were viewed as a revolutionary technology. This belief was expressed through the popularity of "scientific romances" such as Jules Verne's 1886 *Clipper of the Clouds* or Orson Welles' 1907 *The War in the Air* that dramatized the potentials of aircraft.[28] The popularity of aircraft literature was representative of a broader belief in technological modernity during this period—the preceding fifty years had seen the rise and expansion of the railroads, the beginning of electrification, incandescent lighting, wireless

[28]Benjamin Foulois and C.V. Glines, *From the Wright Brothers to the Astronauts: The Memoirs of Benjamin D. Foulois* (New York, NY: McGraw-Hill, 1968), 43. Also see: Tami Davis Biddle, *Rhetoric and Reality in Air Warfare* (Princeton, NJ: Princeton University Press, 2002), 13

telegraphy, the internal combustion engine, and photography; technologies which were reshaping the lives of the rapidly urbanizing populations in the western world. The aircraft—engaging in heavier-than-air flight—was a potent symbol of the inexorable advance of technology and western civilization.[29]

The first aircraft was delivered to the Aeronautical Division of the Army Signal Corps in 1909 following a lengthy lobbying process by the Wright Brothers to overcome the reluctance of the War Department General Staff.[30] The Aeronautical Division had little power and few resources because it was the smallest unit of the smallest Army corps. The role of the Signal Corps managed communications and conducted reconnaissance in service of the infantry and the Aeronautical Division was an ad-hoc unit created in 1907 to explore military ballooning.[31] The Wright aircraft was procured by the Aeronautical Division because of senior officer disinterest in the aircraft—it was viewed as a curiosity as opposed to a potentially game-changing technology.

This ambivalence meant that the first aviators recruited to operate the Wright aircraft were granted a large degree of freedom in their activities. Benjamin Foulois, the first Army pilot, recalled that this his orders were: "You are to evaluate the airplane. Just take plenty of spare parts—and teach yourself to fly."[32] This ambivalence of the General Staff continued through 1911 when Henry Arnold, the second Army pilot, began flying; he reports that "in general . . . our purpose had to be a vague one. . . of developing the airplane into a military weapon as best we could, for we certainly received few, if any, suggestions from the War Department."[33] The main Army doctrinal statement—the Field Service Manual—reflected this ambivalence and the 1910 edition merely

[29]Robert Wohl, *A Passion for Wings: Aviation and the Western Imgination 1908-1918* (New Haven, CT: Yale University Press, 1994), 8-14

[30]Tom D. Crouch, *The Bishop's Boys: A life of Wilbur and Orville Wright*, New York, NY, 2003, 331; Charles Chandler and Frank Lahm, *How Our Army Grew Wings: Airmen and Aircraft Before 1914* (New York, NY: The Ronald Press Company, 1943), 148

[31]Brig. Gen. James Allen, "Report of the Chief Signal Officer," in *Annual Report of the Secretary of War*, vol. II (Washington, DC: Government Printing Office, 1908), 179–215; R. Earl McClendon, *Autonomy of the Air Arm* (Washington, DC: Air Force History / Museums Program, 1996), Appendix A

[32]Foulois and Glines, *From the Wright Brothers to the Astronauts: The Memoirs of Benjamin D. Foulois*, 2

[33]Henry Harley Arnold, *Global Mission* (New York, NY: Harper & Brothers, 1949), 31

noted that the "flying machine is used as the commander directs."[34] During this period of free experimentation, the early air advocates developed reconnaissance techniques and tested the offensive utility of aircraft which allowed them to cultivate a daredevil aura and a distinct set of interests.[35] The advocates, leveraging their experimentation, demonstrated the efficacy of aircraft during field maneuvers in 1912 and the 1913 Field Service manual integrated their strategic and tactical reconnaissance techniques.[36]

The early air advocates began to develop a domain vision by realizing a distinctive identity and set of interests during this period. They described their unique perspective and identity, derived from operating aircraft, as "airmindedness" which denoted a belief that military aviation would serve a critical role in the future of warfare.[37] The Army air advocates were sharply critical of their non-airminded commanding officers and Henry Arnold claims that this led to "a feeling that [Army pilots] should be commanded at the top by men who understood flying."[38] The perception of poor leadership generated a sense of resentment amongst the Army pilots, culminating in a series of courts-marshal of pilots for insubordination.[39] The distinctive "airminded" culture of the Army aviation advocates laid the basis for a domain vision and led them to seek greater autonomy in defining the conditions of their operation.

Despite the freedom to experiment and sense of distinctiveness among aviation advocates Army aviation concepts remained simplistic at the beginning of WWI, Arnold wrote "we had

[34]War Department Office of the Chief of Staff, *Field Service Regulations: United States Army* (Washington, DC: Government Printing Office, 1910), 54

[35]Chandler and Lahm, *How Our Army Grew Wings: Airmen and Aircraft Before 1914*, 196; Arnold, *Global Mission*, 31-32

[36]Foulois remarked that "we proved that airplanes could replace the calvary and could prevent surprise mass attacks by providing information on enemy troop buildups and movements much faster than ever before." Foulois and Glines, *From the Wright Brothers to the Astronauts: The Memoirs of Benjamin D. Foulois*, 101-102; Juliette A. Hennessy, *The United States Army Air Arm, April 1861 to April 1917* (Washington, DC: Office of Air Force History, 1985), 110; War Department Office of the Chief of Staff, *Field Service Regulations: United States Army* (Government Printing Office, 1913), 58

[37]"Airmindedness" is used extensively to describe allies and malign foes in memoirs. See: Arnold, *Global Mission*; Chandler and Lahm, *How Our Army Grew Wings: Airmen and Aircraft Before 1914*

[38]Arnold, *Global Mission*, 46

[39]ibid., 42-46

no theories of aerial combat, or of any air operations except armed reconnaissance."[40] Despite these limitations, on the eve of American entry into the war Congress, appropriated $ 640 million dollars to build up the Air Service-American Expeditionary Forces. The buildup was in response to a request by French Prime Minister Alexandre Ribot. [41] While this was a massive infusion of funding, aircraft, and personnel the WWI Air Service was operated on a largely ad-hoc basis because of the youth and inexperience of the officer corps drawn from the Army aviators. The relative freedom of the Army aviators in operating the Air Service in World War I reflected the secondary and contested role that aircraft had in the conduct of the war, Army aviators proposed operations to senior officers who generally constrained rather than encouraged their activities. They were granted limited opportunities to pursue operations outside of battlefield support.[42]

While Air Service officers were constrained in their activities, they began to elaborate a domain vision with theories of strategic bombing and air superiority, initially borrowing from British and Italian contacts.[43] While attempts to implement strategic bombing campaigns failed during the war, the work of William "Billy" Mitchell on the role of air superiority would ultimately be most influential on the development of the post-war air domain vision. Extending his battlefield experience, he argued that the "the only defense against an air force is another air force" and that "an air force can act either over the land or the water, and if adequately organized, trained, and equipped, can defend the United States from aerial attack and from naval attack." What was unique about aircraft for Mitchell was that the extension of the sphere of military activity in the air enabled actions irrespective of surface geography—the air enabled action across all surface environments thereby providing a radically new method of waging war.[44] This vision of air warfare portrayed

[40] Arnold, *Global Mission*, 52

[41] Foulois and Glines, *From the Wright Brothers to the Astronauts: The Memoirs of Benjamin D. Foulois*, 140-158

[42] *Passim* "Early History of the Strategical Section," Edgar Gorrell, Record Group 120, Gorrell's History of the American Expeditionary Forces Air Service 1917-1919, Series B, Volume 6, NARA-College Park, 371-401.

[43] Dr. J.L. Boone Atkinson, "Italian Influence on the Origins of the American Concept of Strategic Bombardment," *Airpower Historian* IV, no. 3 (1957): 145-146; Biddle, *Rhetoric and Reality in Air Warfare*, 54; George K. Williams, "'The Shank of the Drill': Americans and Strategical Aviation in the Great War," *Journal of Strategic Studies* 19, no. 3 (1996): 381–431

[44] "Principles underlying the use of an air force by the United States," William Mitchell, November 30, 1920, Pa-

the air as a distinct battlefield with the implication that an enemy air force could only be defeated in the air.

Advocates seized on post-WWI defense re-organization debates in order to advance this domain vision and were aided by the acting Chairman of the House Military Affairs Committee, Fiorello La Guardia, who had served in the WWI Air Service. La Guardia called hearings in 1919 to provide a forum for open discussion of aviation independence by the Army aviators.[45] In these hearings, the aviation advocates and War Department argued over two dimensions critical to the air domain vision: whether aircraft had a role beyond aiding the infantry and if that role necessitated organizational independence. William Mitchell argued in his testimony that "the principal mission of aviation is fighting hostile aviation" over land or sea. In order to pursue this mission, Mitchell claimed that an independent air force was necessary to provide specialized training and the flexibility to fight enemy air forces irrespective of surface terrain.[46] Secretary of War Newton Baker, representing the War Department position, argued that aircraft were merely new capability to pursue existing missions such as reconnaissance and artillery spotting and that the aircraft's greatest impact would be to "take over what the artillery now does" in supporting the infantry.[47] For Baker, this metaphor served as a powerful claim against autonomy remarking in his annual report that "nobody would think of suggesting that artillery should be a separate service." Notably, Baker supported his argument on two claims about technological utility: first, that air defense had become so sophisticated that aircraft had limited offensive utility; and second, that bombing was

pers of Billy Mitchell, Box: 31, Folder: Aeronautics–Separate Department Recommendations, Library of Congress Manuscript Division (hereafter LOC). A 1919 doctrinal manual by Army aviator William Sherman, "Tentative Manual for Employment of Air Service," similarly argues that maintaing air supremacy is a critical strategic function of aircraft. William Sherman, "55. Sherman: Tentative Manual for the Employment of Air Service 1919," in *The U.S. Air Service in World War I: Early Concepts of Military Aviation*, ed. Maurer Maurer, vol. II (Washington, DC: U.S. Government Printing Office, 1978), 315-384

[45]Rondall R. Rice, *The Politics of Air Power: From Confrontation to Cooperation in Army Aviation Civil-Military Relations* (Lincoln, NE: University of Nebraska Press, 2004), 16-17

[46]United States House of Representatives, *Hearings before the Committee on Military Affairs, House of Representatives, Sixty-sixth Congress, second session, United Air Service: General Discussionshe* (Washington, DC: Government Printing Office, 1919), 906-907. For other notable testimony from Benjamin Foulois and William Sherman see: ibid., 44, 81, 118-119

[47]ibid., 389

ineffective—bombing casualties in the AEF numbered 141. [48] This debate between the air advocates and the War Department was fundamentally a debate over whether the air was military domain—were aircraft a substantially different way of waging war or just another capability?

While these debates deepened the political and military acceptance that aircraft played a combat role, ultimately the preferred framework of the War Department shaped the 1920 National Defense Act, an Aviation Service subordinate to the strategic mission of the infantry on the line of the Army.[49] The new formal combat role of aircraft was further codified in the 1923 Field Service Regulations which expanded the use of aircraft to include offensive battlefield operations in coordination with other combatant arms.[50] The organizational expansion also came with two benefits for the aviation advocates. First, it provided a statutory strength of 1,514 officers and 16,000 enlisted, prior to the war the officers numbered in the dozens and enlisted personnel in the hundreds. Second, it stipulated that experienced pilots command aviation units, formally resolving a long-standing complaint of the aviation advocates.[51] Despite hewing to War Department views this act was a partial fulfillment of the aviators' domain vision, aircraft gained a formal combat role and advocates gained the ability to begin cultivating a distinct officer corps.

During the 1920s the air advocates continued to refine their domain vision—that air as a domain necessitated training and equipping for achieving air superiority—and the Air Service was renamed in the Air Corps in 1926.[52] At the beginning of the 1930s the advocates began to formulate a new domain vision that centered the role of precision strategic bombing of economic infrastructure instead of air superiority. Advocates at the Air Corps Tactical School called this "industrial-web theory" and argued "modern industrial nations are susceptible to defeat by inter-

[48] Secretary of War, *Annual Report of the Secretary of War* (Washington, DC: Government Printing Office, 1919), 71

[49] Biddle, *Rhetoric and Reality in Air Warfare*, 135-138; Robert Frank Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907-1960* (Maxwell AFB, AL: Air University Press, 1989), 35

[50] War Department Office of the Chief of Staff, *Field Service Regulations: United States Army 1923* (Washington, DC: Government Printing Office, 1923), 21-25

[51] Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907-1960*, 35

[52] The renaming also included the creation of an Assistant Secretary of War for the Air, but this had ambivalent effects. ibid., 40; Thomas H. Greer, *The Development of Air Doctrine in the Army Air Arm, 1917 to 1941* (Washington, DC: Office of Air Force History, 1985), 16

ruptions of this [industrial] web, which is built to permit the dependence of one section upon many or all other sections, and further this interruption is the primary objective for an air force."[53] The exact reasons for this shift in domain vision are under some dispute, while some have suggested that Italians such Giulio Douhet or Giovanni Caproni inspired the turn to the bomber-centric industrial-web theory, the evidence suggests that the turn owed to the prognostications of Air Corps Tactical School faculty.[54] This new domain vision had critical implications for how advocates would seek to institutionalize their domain vision: air superiority understood the air as a distinct battlefield where enemy forces had to be destroyed with fighter aircraft whereas industrial-web theory posited that the air allowed for bombers to directly target the capacity for a state to fight. [55]

At the same time, air advocates renewed their demand for organizational autonomy during the mid-1930s after Benjamin Foulois, the first pilot, became Air Corps Chief of Staff.[56] This coincided with a push inside the War Department to prepare for the newly developed RAINBOW war plans. Foulois took this opportunity to argue for the creation of a General Headquarters-Air Force (GHQ-AF) that would conduct independent air operations within the RAINBOW framework. Political space for realizing this increase in organizational autonomy opened because of the "Air Mail Crisis" in which multiple Army pilots died after being requisitioned to carry mail for the U.S. Postal Service leading public outcry and demands for reform.[57] Foulois and the domain advocates seized on this confluence of events and drove the creation of a semi-autonomous command and training structure for the Air Corps with a permanent GHQ-AF.[58] Foulois's successful drive for the GHQ-AF institutionalized the air as a support domain.

[53] "Principles of War Applied to Air Force Action," Donald Wilson, 1933, IRIS 000157164, Call 248.101-2, AFHRA, 3.
[54] Atkinson, "Italian Influence on the Origins of the American Concept of Strategic Bombardment"; Biddle, *Rhetoric and Reality in Air Warfare*, 159-163 Donald Wilson, "Origin of a Theory for Air Strategy," *Aerospace Historian* 18, no. 3 (1971): 19–25
[55] "Air Force Principles," Donald Wilson, 1933, IRIS 000157164, Call 248.101-2, AFHRA, 3. See also: Biddle, *Rhetoric and Reality in Air Warfare*, 160-163
[56] Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907-1960*, 66
[57] ibid., 70
[58] ibid., 75; Rice, *The Politics of Air Power: From Confrontation to Cooperation in Army Aviation Civil-Military Relations*, 116-117

Strategic Domain 1935-1947

Following the creation of the GHQ-AF, the air advocates began to assertively lobby for the development of heavy bomber formations to operationalize their strategic bombing domain vision. First, air advocates built an alliance with George C. Marshall, shortly before his promotion to War Department Chief of Staff, by taking him on tours of air bases and production facilities.[59] Second, they had built support with President Roosevelt, leading him to support their domain vision over those existing the War Department. For example, William Mitchell cultivated a public friendship with Roosevelt during the early 1930s, helping him win the democratic nomination for president.[60] To demonstrate the utility of heavy bombers, they conducted "good will" flights to South America in order to demonstrate to President Roosevelt the potential value of heavy bombers in enforcing the Monroe Doctrine against fascist subversion in Latin America.[61] Together, these two lobbying efforts paid dividends following the 1938 Munich Crisis when Roosevelt began planning a massive increase in the production of military aircraft favoring Army air advocates' interests; Roosevelt purposefully hid his deliberations from the Secretary of War who preferred medium bombers and instead promoted heavy bombers based on guidance provided by air advocates.[62]

The organizational competencies of the GHQ-AF combined with the alliances cultivated during the late 1930s led to air advocates playing a central role in strategic planning for World War II.[63] In early 1941, air advocates drafted AWPD/1—the initial air war plan—which reflected "industrial-web theory." It contained three planks: first, the strategic bombing of "systems. . . vulnerable to air attack and to the continuance of war effort of Germany" which included transportation, oil

[59]Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907-1960*, 93

[60]Jeffrey S. Underwood, *The Wings of Democracy: The Influence of Air Power on the Roosevelt Administration 1933-1941* (College Station, Texas: Texas A&M University Press, 1991), 57

[61]ibid., 75, 103-122. Report of the Air Corps Board: Air Corps Mission Under the Monroe Doctrine, Air Corps Board, 1938, IRIS 00121165, Call 167.5-44, AFHRA.

[62]Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907-1960*, 100 Rice, *The Politics of Air Power: From Confrontation to Cooperation in Army Aviation Civil-Military Relations*, 150-153

[63]Donald Miller, *Masters of the Air: America's Bomber Boys Who Fought the Air War Against Nazi Germany* (New York, NY: Simon / Schuster, 2006), 52; Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907-1960*, 75, 108-109

infrastructure, and the capitol Berlin. Second, achieving air superiority through bombing Luftwaffe installations. And third, close air support for the final ground invasion.[64] Thus, the bomber played a central role in this vision of air war—demonstrating a commitment to independent strategic operations. The plan was approved by both the General Staff and the new Secretary of War, paving the way for operationalizing strategic air warfare.[65]

Full strategic autonomy was gained with the appointment of Henry Arnold, who led the newly named Army Air Forces, to the Joint Chiefs of Staff in March 1942. The Joint Chiefs had just been created to enable high-level strategic coordination between the service departments; the symbolic nature of Arnold's appointment was intentional.[66] While the Army Air Forces still coordinated with the Army Ground Forces, two dedicated strategic bombing units were also created: the 20th Air Force and the U.S. Strategic Air Forces in Europe operated independently of theater commands thereby finally giving the aviators the ability to conduct independent aerial warfare.[67] The rapidly expanding role of the Army Air Forces was doctrinally recognized in a 1943 doctrinal manual which stated "LAND POWER AND AIR POWER ARE CO-EQUAL AND INTERDEPENDENT FORCES; NEITHER IS THE ADJUNCT OF THE OTHER."[68]

Following the war, the creation of a fully autonomous Air Force was considered a fait accompli. Postwar debates were dominated by arguments over operational coordination in the soon to be created Department of Defense as opposed to whether aircraft had a worthwhile independent role.[69] The only objection came from the Navy, which feared Army and Air Force domination of the Department of Defense, however, these concerns were allayed and the 1947 National Security Act created a unified Department of Defense with co-equal Navy, Army and Air Force sub-

[64]"Munitions Requirements of the Army Air Forces," AWPD, 1941, IRIS 00118163, Call 145.82, AFHRA, 1-2
[65]Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907-1960*, 111
[66]ibid., 129
[67]Herman S Wolk, *Toward Independence: The Emergence of the U.S. Air Force* (Washington, DC: Air Force History / Museum Program, 1996), 6
[68]Emphasis in original. War Department General Staff, *FM 100-20*, (Washington, DC: Government Printing Office, 1943), 1
[69]Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907-1960*, 190-191; McClendon, *Autonomy of the Air Arm*, 102

departments.[70] Thus, the air was institutionalized as a strategic domain with a dedicated service department—the Air Force—through the work of aviation advocates advancing a domain vision of an independent strategic role for aircraft in warfare.

The institutionalization of the air as a strategic domain with the creation of an independent Air Force in 1947 was not the product of the air being a "natural domain." Rather, domain advocates, working over several decades to refine and operationalize a domain vision drove forward a series of doctrinal and organizational changes that articulated the air as a highly consequential medium of conflict. There is no evidence that technological assessments or a rational learning process directly led to the air being a strategic domain, rather, it was a political struggle by domain advocates that created the conditions whereby it was obvious that warfare in the air was a substantially different activity. This is not to claim that in absence of domain advocates the U.S. military would not have pursued aviation capabilities, rather, that the specific way of air warfare institutionalized in the U.S. was contingent—the domain vision shift from air superiority as the primary function of an air force to strategic bombing had significant implications for organization, doctrine, training, and capabilities acquisition. This shit was not the product of a natural evolution in aviation capabilities, but rather the conscious effort of domain advocates.

Cyberspace

In this case study, I reveal the institutionalization of the American conception of cyberspace as a domain founded on warfare within and through infrastructure.[71] The case study has one section that exposes the role of domain advocates in developing and advancing the cyberspace domain vision from the 1980s until the creation of USCYBERCOM, which signaled the institutionalization of cyberspace as a support domain. The institutionalization of cyberspace by advocates demonstrates the contingent nature of domains—during the 1990s the U.S. military initially focused on "information warfare" which integrated cyber and non-cyber capabilities akin to the contempo-

[70] Futrell, *Ideas, Concepts, Doctrine: Basic Thinking in the United States Air Force, 1907-1960*, 194
[71] Joint Chiefs of Staff, *JP 3-12 Cyberspace Operations*, I2-I4

rary Russian information operations. This case demonstrates that cyberspace as a domain was a contingent project and not an inevitability.

Acquisition to USCYBERCOM 1980s-2009

While computerized information networks have existed since the creation of the SAGE radar system in 1948, up until the 1980s these networks were treated as enabling infrastructure for general communication, information sharing, and C2 but not as a medium for military action.[72] The 1980s was a pivotal decade for two reasons: first, the TCP/IP standard was implemented which allowed flexible inter-networking across heterogeneous networks enabling the rapid growth and spread of civilian information infrastructure. Second, a rising belief that these technologies heralded the "Information Age" which was transforming society.[73] One of the beliefs of the "Information Age" was that computers and information networks created a virtualized space of interaction.[74] The term "cyberspace" was introduced by science fiction author William Gibson in his 1984 book *Neuromancer*, and it rapidly became a catchword for futurists anticipating the Information Age.[75]

Out of this milieu, members of the Joint Special Studies Group (JSSG), an ad-hoc intelligence analysis formation under the Joint Chiefs of Staff (JCS), began to experiment with disrupting Soviet submarine C2 networks. The key innovation of the group was the realization that they could "hack" into the C2 network and use it to disrupt Soviet submarine operations. JSSG members came to this conclusion by modeling the Soviet C2 network using their own information networks and using it to experiment with techniques to disrupt network traffic by acting through

[72]The partially de-classified NSA journal *Cryptolog*, service publications, and DOD reports from this time period demonstrate a concern with computer security and espionage but not military force. For example, Roger R. Schell, "Computer Security: the Achilles' heel of the electronic Air Force? (1979)," *Air & Space Power Journal* 27, no. 1 (January 2012): 158–192

[73]Academic contract researchers primarily developed these technologies. Jane Abbate, *Inventing the Internet* (Cambridge, MA: MIT Press, 2000)

[74]For example, the movie 1982 movie TRON, which depicted a fully virtual world inside of a computer. Or the 1983 movie War Games which showed a teenager hacking into NORAD and almost triggering a nuclear war.

[75]In *Neuromancer* a character describes cyberspace as "A consensual hallucination . . . A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity." William Gibson, *Neuromancer* (New York, NY: Berkley Publishing Group, 1989), 128. See also: Michael Benedikt, ed., *Cyberspace: First Steps* (Cambridge, MA: MIT Press, 1992)

network infrastructure—infrastructure as a medium. While little is publicly known about the JSSG, published accounts claim that the senior leadership within the JCS, DOD, and NSA were either opposed to or confused by the project. For example, [76]

Due to this reception, the work of the JSSG was not pursued further until the Gulf Wa when Michael McConnell, who had worked in the JSSG, led the Joint Intelligence Center (JIC). At the JIC he evaluated and refined methods to disable Iraqi air defense C2 systems using network attacks. While his more ambitious plans were stopped by theater commanders, he was able to conduct some rudimentary cyberattacks on Iraqi C2 systems.[77] After the Gulf War, McConnell would go on to lead the NSA but he did not continue extensive work on these capabilities due to the opposition of career NSA staff and the demands of adapting the NSA to the post-Cold War world.[78]

After the Gulf War three terms generally associated with the cyberspace as a domain were popularized. First, was "cyberwar" by John Arquilla and David Ronfeldt with their 1993 article "Cyberwar is Coming!" They argued that the Information Age created the grounds for the conduct of cyberwar and netwar—the former is warfare conducted by highly autonomous units, like the Mongol Horde, coordinated through superior intelligence processing and distribution; the latter, netwar, is a strategic struggle over societal narratives.[79] Second, was "Information War" which initially referred to the role that superiority in the collection, circulation, and use of information played on the battlefield during the Gulf War and was akin to Arquilla and Ronfeldt's "cyberwar." [80] However, this conception of information warfare would eventually be subsumed by the Rev-

[76]Bruce D. Berkowitz, *The New Face of War: How War Will Be Fought in the 21st Century* (New York, NY: Free Press, 2003), 57-59; Kaplan, *Dark Territory: The Secret History of Cyberwar*, 18, 26-27; Craig J. Wiener, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation" (PhD diss., George Mason University, 2016), 102

[77]Kaplan, *Dark Territory: The Secret History of Cyberwar*, 21-24

[78]McConnell was viewed as a reformer, but there is no evidence that it was these attacks that led to his appointment. NSA staff were suspicious of hacking for intelligence or "active SIGINT." ibid., 32-33

[79]John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy* 12, no. 2 (Spring 1993): 141–165; The earliest uses of "cyberwar" referred to robot warfare in science fiction and futurology. Lawrence Freedman, *The Future of War: A History* (New York, NY: PublicAffairs, 2017), 230-38.

[80]Popularized by: Alan D. Campen, *The First Information War: The Story of Communications, Computers, and In-*

olution in Military Affairs and was eclipsed by a conception of information warfare as warfare within and through the medium of information. Last, Counter-C2 Warfare was formalized by JCS Memorandum of Policy 30 as the military application of information warfare and called on service departments to develop a spectrum of capabilities to "decapitate the enemy's command structure from its body of combat forces."[81]

While McConnell's advocacy ended when he became Director of the NSA, an Air Force intelligence officer who had served in the Gulf War, Kenneth Minihan, began trying to replicate the JIC techniques at the Air Information Warfare Center under the Air Intelligence Agency (AIA).[82] He described the AIA as a "free form think tank" that "developed ideas and began to create capabilities for IW."[83] Based on this experimentation AIA advocates proposed integrating attacks through information infrastructure into war plans for a potential invasion of Haiti in 1995.[84] However, the actual attacks had to be conducted by another unit because the AIA, as an intelligence unit, did not have the authority to use force under U.S. law.[85] An officer at the Air Combat Command who was

telligence Systems in the Persian Gulf War (Fairfax, VA: AFCEA, 1992); See also: Michael Warner, "Reflections on Technology and Intelligence Systems," *Intelligence and National Security* 27, no. 1 (2012): 790. "Information war" was coined by Thomas Rona in 1976 as manipulating telemetry systems of enemy guided weapons. Thomas P. Rona, *Weapons Systems and Information War*, Defense Technical Information Center, 1976, accessed March 11, 2017, http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf

[81]Colin Powell, *Chairman of the Joint Chiefs of Staff Memorandum of Policy No. 30 (CMOP); Command and Control Warfare*, DTIC, March 8, 1993, 2, http://www.dtic.mil/docs/citations/ADA389344. Also, see Michael Warner, "Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014," *Cyber Defense Review*, August 27, 2015, accessed May 14, 2017, http://cyberdefensereview.army.mil/The-Journal/Article-Display/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/.

[82]*TWENTY-FIFTH AIR FORCE: BRIEF HISTORY*, 3, accessed June 12, 2017, http://www.25af.af.mil/Portals/100/Documents/AFD-150520-021.pdf?ver=2016-02-11-123439-690; John Casciano, *Los Angeles - October 18, 1996*, Air Force Association National Symposia, October 18, 1998, accessed June 2, 2017, http://secure.afa.org/aef/pub/la9.asp; United States Air Force, *Lieutenant General Kenneth A. Minihan, Biography*, Official United States Air Force Website, October 1, 1998, accessed July 5, 2017, http://www.af.mil/About-Us/Biographies/Display/Article/106229/lieutenant-general-kenneth-a-minihan/; Wiener, "Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation," 125

[83]Quoted in ibid., 122

[84]Kaplan, *Dark Territory: The Secret History of Cyberwar*, 59

[85]The AIA was a service cryptologic element and were affiliated with the Air Force and the NSA. Air Force ISR Agency, *Air Force Instruction 14-128* (Secretary of the Air Force, 2011), 2-3; For an explanation of the legal tension see: Robert Chesney, "Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of*

tasked with operationalizing the AIA plans, Walter Rhoads, proposed to Minihan that a specialized unit should be formed to carry out these attacks. Minihan agreed and successfully lobbied for the creation of the 609th Information Warfare Squadron (IWS) in 1995.[86] Therefore, the work of the AIA advocates refining infrastructural attacks led to the creation of the first formal combat unit.

Walter Rhoads became the first commanding officer of the IWS and reflected on its significance by stating: "I liken this to the very first aero squadron when they started with biplanes. We're at the threshold of a new era... We are not exactly sure how combat in this new dimension of cyberspace will unfold."[87] Rhoad's statement is significant for two reasons: first, he tacitly compares the air and cyberspace —signaling their equivalence *as* spaces of warfare; and second, his invocation of Air Force history draws on the struggle to institutionalize a new domain vision. While Rhoad's statement reflects a desire to advocate for cyberspace institutionalization, the actual impact of the IWS was limited for several reasons—first, its creation was opposed by some in the Air Force leadership which hampered unit build-out.[88] Second, the IWS was assigned the information warfare mission outlined in CMOP 30, and was therefore responsible for planning and using non-cyberspace capabilities such psychological warfare or military deception.[89] The responsibilities of the IWS meant that the AIA would continue to have a primary role in developing techniques for warfare in cyberspace while the IWS integrated them into the broader conception of information warfare.[90]

The creation of the IWS coincided with the service departments beginning to discuss information warfare doctrine and concepts based on the CMOP 30 Counter-C2 warfare concept. First,

National Security Law and Policy 5, no. 2 (2012): 539–629; Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities, and Covert Action," *Harvard National Security Journal* 3, no. 1 (2011): 85–142

[86]Kaplan, *Dark Territory: The Secret History of Cyberwar*, 107-108; United States Air Force, *Lieutenant General Kenneth A. Minihan, Biography*.

[87]Quoted in *609 IWS: A Brief History Oct 1995-Jun 1999* (Colorado Springs, CO: System Technology Associates, 1999), 1

[88]ibid., 2, 6-7.

[89]ibid., 7

[90]Casciano, *Los Angeles - October 18, 1996*; The IWS and AIA had a close relationship with many IWS officers being drawn from the AIA. *609 IWS: A Brief History Oct 1995-Jun 1999*, 38

the Air Force published a white paper entitled *Cornerstones of Information Warfare*, which articulated the role of attacks on and through information and information systems as a capability to achieve extant Air Force missions. Crucially, the document outlines a new capability called "information attack," stating:

> The Information Age has provided new and practical means to deny, exploit, corrupt, or destroy information, as well as the vulnerabilities to make those attacks possible. Air Force doctrine does not yet acknowledge or define these assaults on information, which we call Information Attack.
>
> **Information Attack:** directly corrupting information without visibly changing the physical entity within which it resides.

This is the first identifiable description of something like contemporary cyberspace operations in doctrine, but it is articulated as one of several capabilities that act on information.[91] In 1996, the Army published its own doctrine—FM 100-6 *Information Operations*–which likewise emphasized information warfare as operating upon and through information for maintaining an information advantage but omits "information attack."[92] Finally, the Navy did not publish a white paper or doctrinal statement at this time but the Chief of Naval Operations issued guidance that conformed to overall the view shared by the Army and Air Force, but like the Army omitting "information attack."[93] Unfortunately, there is no dispositive evidence to evaluate why the Air Force included "information attack," the closest analog to contemporary cyberspace operations, as a capability for information warfare, unlike the other services. Despite these doctrinal statements, there is no evidence that the senior leadership of any service sought to promote or develop capabilities like

[91] Formatting in original. Air Force Office of the Chief of Staff, *Cornerstones of Information Warfare*, 1995, accessed May 25, 2017, `http://www.c4i.org/cornerstones.html`. A follow-on white-paper was largely the same. Department of the Air Force, *Information Warfare* (Washington, DC: HQ-AF, 1996)

[92] HQ TRADOC, *FM 100-6*, FAS, 1996, accessed June 12, 2017, `https://fas.org/irp/doddir/army/fm100-6/`

[93] CNO, *Subject: IMPLEMENTING INSTRUCTIONS FOR INFORMATION WARFARE/COMMAND AND CONTROL WARFARE*, Information Warfare Document Archive, January 18, 1995, accessed August 20, 2018, `http://www.iwar.org.uk/iwar/resources/opnav/3430_26.pdf`

"information attack." Even the sincerity of service leader interest in information warfare was questionable as Fred Kaplan in *Dark Territory* notes: "the top generals had signed doctrinal documents on 'information warfare' but they didn't appear to take the idea very seriously."[94]

While the services focused on information as a medium and target, the available evidence indicates that advocates at the AIA played a core role in developing the cyberspace domain vision that drove the creation of USCYBERCOM. Retired General Michael Hayden, who succeeded Kenneth Minihan as head of the AIA in 1996, recalled that "the first article of faith at AIA was simply that cyber was a 'domain,"' and that he was "proselytized" by Minihan's "disciples."[95] A crucial feature of the AIA domain vision was viewing "computer network operations" as encompassing three activities: computer network exploitation (CNE), computer network attack (CNA), and computer network defense (CND). Hayden recalls: "our categorization had an eerie resemblance to the way that American air power is organized and explained, reconnaissance (CNE), bombers (CNA), and fighters (CND)." [96] This conceptual architecture is crucial to the development of USCYBERCOM because it created a conceptual unity between all three functions. Conceivably, CNA—"information attack" in the parlance of *Cornerstones*—could have remained an IW capability, CND could have been handled by law enforcement or a civilian agency like FEMA, and CNE treated as a signals intelligence capability.[97] Therefore, the AIA advocates' domain vision united military operations in cyberspace such that it demanded institutionalization via a single organization.

The conceptual unity of the CNE/CNA/CND framework was the core of Minihan and Hayden's domain advocacy—they worked to consolidate all three functions during their successive

[94]Kaplan, *Dark Territory: The Secret History of Cyberwar*, 118

[95]Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, 122, 136; See also: Kaplan, *Dark Territory: The Secret History of Cyberwar*, 122

[96]Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, 140

[97]During the late 1990s there was uncertainty over whether attacks on government networks necessitated a law enforcement or military (CND) response. Stephen A. Hildreth, *CRS Report for Congress: Cyberwarfare*, Federation of American Scientists, 2001, 6, 8, accessed June 12, 2017, `https://fas.org/sgp/crs/intel/RL30735.pdf`. CNA is first used in joint doctrine in 1998, where it is listed as a capability for information warfare. Joint Chiefs of Staff, *JP 3-13 Information Operations* (Chairman of the Joint Chiefs of Staff, 1998), I-9.

tenures as Directors of the NSA from 1996-2005. Having these three functions separated, Hayden recalls, "made about as much sense as America having three air forces... when it really was all about control of the air."[98] For CNA, Minihan initiated the creation of the Information Operations Technology Center (IOTC) in 1997 which supplanted the role of the AIA in the development of cyberspace doctrine.[99] Hayden described it as "the cyber-gathering place where cyber concepts could be defined, discussed, challenged, debated, and tested" the "center kept the doctrinal fire (and controversy) of cyber operations alive."[100] The IOTC complemented existing CNE efforts at the NSA, which Minihan had revamped over the objections of career NSA staff after he became director.[101]

CND was handled by the services through the Joint Task Force–Computer Network Defense (JTF-CND) which was created in 1998. The task force was created after two events: first, an exercise created by Minihan to convince DOD leadership to take cyber-security seriously called ELIGIBLE RECEIVER; and second, SOLAR SUNRISE, an intrusion into Air Force systems which was initially believed to have originated in Iraq but was actually perpetrated by two teenagers in California having fun. Together, these two events led DOD leadership to begin investing in cyber-defense, part of which was creating the JTF-CND.[102] The task force was placed under the control of the Assistant Secretary of Defense for C3I instead of a service or command because

[98] Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, 142

[99] Minihan had wanted the IOTC to operate with Title 10 authority, allowing it to conduct operations that were considered a use of force, but the service departments blocked this. Kaplan, *Dark Territory: The Secret History of Cyberwar*, 124; Nolte, "Anticipating Cyberspace Security: NSA's Experience 1992-1997," 35.

[100] Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, 139. It also possible that AIA members were moved to the IOTC after its creation, their role as service intelligence officers meant that they were also under the command of the NSA Central Security Service. The NSA was granted executive agent status in 1997, consolidating the development of offensive CNA at the IOTC. Perry, William A., *Memorandum for the Director, National Security Agency, Subject: Delegation of Authority and Creation of Executive Agent*, GWU National Security Archive, March 3, 1997, `http://nsarchive.gwu.edu/dc.html?doc=2778590-Document-02-William-A-Cohen-Memorandum-for-the`. The Air Force 609 IWS was disbanded in 1998 and its CNA functions were transferred to the AIA. *609 IWS: A Brief History Oct 1995-Jun 1999*, 27

[101] Kaplan, *Dark Territory: The Secret History of Cyberwar*, 59; Nolte, "Anticipating Cyberspace Security: NSA's Experience 1992-1997," 33

[102] Kaplan, *Dark Territory: The Secret History of Cyberwar*, 77; U.S. Strategic Command, *JTF-CND / JTF-CNO / JTF-GNO – A Legacy of Excellence*, GWU National Security Archive, 2010, 5, `http://nsarchive.gwu.edu/dc.html?doc=2849764-Document-05`

while the Air Force wanted control the Army and Navy did not want the Air Force defending their networks.[103] In 2000, the Assistant Secretary for C3I, Art Money, pushed to create the Joint Task Force-Computer Network Operations (JTF-CNO) by giving JTF-CNO the ability to conduct CNA as force—operations that NSA's IOTC could not legally conduct.[104] JTF-CNO was ultimately placed under U.S. Space Command because none of the other combatant commands were interested.[105]

During this time period evidence of the domain vision developed at the AIA and advocated for by Minihan and Hayden is visible at NSA. The indices of declassified issues of *Cryptolog*, an internal NSA journal, show that until 1997 there were few published articles on information warfare or cyberspace.[106] However, in 1997 *Cryptolog* published "Thinking Out Loud about Cyberspace" by Bill Black, who had been tapped by Minihan to expand NSA work on CNO, which argued for the AIA domain vision of cyberspace as an infrastructural medium. Black argued for a turn to "cyberology" consisting of "'exploitation', 'protection', and 'attack.'"[107] These activities are only possible, Black argued, because the Information Age has brought into being a "totally new sphere of operations, a new environment called cyberspace." Black defines cyberspace as being:

> both real and virtual: while the real portion consists of physical assets (computers, network terminals, satellites, fiber optic cables, etc.) located on earth and in space, it is the

[103] Bob Gourley, *JTF-CND to JTF-CNO to JTF-GNO to Cybercom*, CTOvision.com, September 8, 2010, accessed June 20, 2017, `https://ctovision.com/jtf-cnd-to-jtf-cno-to-jtf-gno-to-cybercom/`; See also: Healey, *A Fierce Domain: Conflict in Cyberspace 1986-2012*, 44-45; Kaplan, *Dark Territory: The Secret History of Cyberwar*, 121

[104] NSA/IOTC was deeply involved with the JTF-CNO, United States Space Command, *USCINCSPACE Implementation Plan for Computer Network Operations*, GWU National Security Archive, March 13, 2001, 2-1, 2-4, `http://nsarchive.gwu.edu/dc.html?doc=2805487-Document-03-The-White-House-Defending-America-s`; National Security Agency/Central Security Service and U.S. Strategic Command, Joint Functional Component Command - Network (JFCC-NW), *National Initiative Protection Program - Sentry Eagle*, GWU National Security Archive, 2004, 8, `http://nsarchive.gwu.edu/dc.html?doc=2838110-Document-03`.

[105] Kaplan, *Dark Territory: The Secret History of Cyberwar*, 122; U.S. Strategic Command, *JTF-CND / JTF-CNO / JTF-GNO – A Legacy of Excellence*, 6

[106] Neither of two articles published prior to 1997 resembled the domain vision. [Author Redacted], "Information Warfare: A New Line of Business for NSA," *Cryptolog* XX, no. 2 (1994): 3–4; [Author Redacted], "Global Network Intelligence and Information Warfare: SIGINT and INFOSEC in Cyberspace," *Cryptolog* XXI, no. 1 (1995): 29–37

[107] William B. Black Jr., "Thinking Out Loud About Cyberspace," *Cryptolog* XXIII, no. 1 (Spring 1997): 2

> virtual aspect—all interconnected, all networked, all compatible and interoperable—that is the most important.[108]

Eschewing the conception of information warfare presented in service doctrine, which treated information as a medium, Black's conceptualization of information warfare is premised on "digital coercion" through the degradation of information infrastructure. Whereas service conception of information warfare relied on a suite of capabilities such as psychological warfare or deception, Black argues that true information warfare depends on "viruses, worms, logic bombs, trojan horses, spoofing, masquerading, and 'back' or 'trap' doors."[109] Standing in stark contrast with the service vision of information warfare as operating on information through a variety of different capabilities, Black articulates a domain vision through the CNE/CNA/CND framework that identifies cyberspace as an infrastructural medium with a native suite of unique capabilities.[110]

The next major drive by cyberspace domain advocates came in 2004 when U.S. Space Command was shuttered and authority over the JTF-CNO was passed to Strategic Command (STRATCOM.) Michael Hayden saw this as an opportunity to finally construct the organizational structure uniting all three CNO roles that he and Minihan had long desired. He suggested to the STRATCOM commander, James Cartwright, that he "devolve his authority and responsibility for cyber attack to Fort Meade and dual-hat me as his action arm."[111] The JTF-CNO would be renamed the Joint Functional Component Command-Network Warfare and the IOTC would perform its core functions through the devolution of authority from STRATCOM. Hayden described it in this way: "the combined team at Fort Meade would access and conduct reconnaissance of a target based on my authorities as DIRNSA [Director NSA] and then, on order, could manipulate or destroy the

[108] Black Jr., "Thinking Out Loud About Cyberspace," 2-3

[109] ibid., 4. Black's article was part of a special issue of *Cryptolog* on Information warfare. Other articles in the issue share the foundational claims of Black: [Author Redacted], "IO, IO, It's Off to Work We Go," *Cryptolog* XXIII, no. 1 (Spring 1997): 5–9; [Author Redacted], "The Role of Information Warfare in Strategic War," *Cryptolog* XXIII, no. 1 (Spring 1997): 20–27; [Author Redacted], "The Infowar Revolution(s)," *Cryptolog* XXIII, no. 1 (Spring 1997): 11–19

[110] Parsing authorship and origination are fraught given the secrecy of the NSA and military cyberspace, however, the preponderance of the evidence suggests that this was the conceptual chain. The NSA shared authority over the AIA with the Air Force and it is entirely likely that Bill Black had contact prior to Minihan's directorship.

[111] Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, 142-143

target based on Cartwright's exercising his combat authority through me." Cartwright approved this proposal and along with Hayden successfully lobbied the service departments, Joint Chiefs, and relevant congressional committees for approval.[112] Reflecting on the significance of this arrangement, Hayden reflects "we now had a structure to go along with our vision," and this structure would form the foundation for the creation of CYBERCOM.[113]

By 2006 this domain vision—cyberspace as an infrastructural medium—had come to inform high-level policy. The Joint Chiefs issued the *National Strategy for Cyberspace Operations*, which defined cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." The strategy document is self-conscious that "treating cyberspace as a domain establishes a foundation to understand and define its place in military operations," the DOD had previously denoted cyberspace as an environment.[114] While much of the document is still redacted, it does identify "strategic cyberspace superiority" as a core goal and argues that other traditional missions apply to cyberspace.[115] This document represents the first high-level embrace of cyberspace as a domain with unique capabilities instead of a mere subsidiary of information operations.

The political opening to create USCYBERCOM was created by a 2008 attack on the DOD's classified networks called BUCKSHOT YANKEE. While the rest of the DOD reeled over the attack, the NSA/JFCC-NW led by Keith Alexander took the lead in response and mitigation. The Director of National Intelligence Mike McConnell, a cyber-advocate who was deeply involved in the early development of cyber-attacks during the Gulf War, seized on this opportunity to push for the creation of USCYBERCOM. The performance of the NSA/JFCC-NW impressed both Presi-

[112]Hayden, *Playing to the Edge: American Intelligence in the Age of Terror*, 143-144
[113]ibid., 144
[114]Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, GWU National Security Archive, December 1, 2006, 3, accessed March 17, 2017, `http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf`
[115]ibid., 14

dent Bush and Secretary of Defense Gates who approved McConnell's plan.[116] The JFCC-NW was the nucleus for USCYBERCOM and inherited command relationships: subsidiary to STRATCOM and led through a "dual-hat" arrangement with the NSA.[117] Deputy Secretary of Defense William Lynn III hailed the creation of USCYBERCOM as a step toward institutionalizing cyberspace as a domain by providing the basis for a distinct force structure and body of doctrine.[118]

Over the next few years, the Joint Chiefs and service departments began to publish separate doctrinal statements for cyberspace operations that centered the infrastructural vision of cyberspace. For example, the 2011 edition of the Air Force Doctrine Document 3-12, is careful to note that "cyberspace operations are not synonymous with information operations" but rather are operations "where the primary purpose to achieve military objectives or effects in or through cyberspace."[119] Beyond doctrine, recent years have seen USCYBERCOM expand and gain greater organizational independence—while USCYBERCOM retains the dual-hat relationship with the NSA it was elevated to a full functional combatant command in 2018, gaining direct authority to use force. As of 2019, the rapid growth of USCYBERCOM suggests that cyberspace is likely to become a strategic domain in the short to medium-term, the Trump administration has delegated an increasing amount of autonomy to USCYBERCOM to conduct offensive operations that fall below the threshold of force.[120] Furthermore, USCYBERCOM's Cyber Mission Force achieved

[116]Harris, *@War: The Rise of the Military-Internet Complex*, 150; Kaplan, *Dark Territory: The Secret History of Cyberwar*, 184

[117]Robert M. Gates, *Memorandum: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*, GWU National Security Archive, June 23, 2009, accessed June 13, 2017, http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-029.pdf; Ellen Nakashima, "Dual-leadership Role at NSA and Cyber Command Stirs Debate," *Washington Post*, October 6, 2013, accessed March 11, 2017, https://www.washingtonpost.com/world/national-security/dual-leadership-role-at-nsa-and-cyber-command-stirs-debate/2013/10/06/ffb2ac40-2c59-11e3-97a3-ff2758228523_story.html

[118]Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy"

[119]United States Air Force, *AFDD 3-12 Cyberspace Operations*, Secretary of the Air Force, 2011. Cf. Joint Chiefs of Staff, *JP 3-12 Cyberspace Operations* (Chairman of the Joint Chiefs of Staff, 2013); Joint Chiefs of Staff, *JP 3-12 Cyberspace Operations*

[120]Ellen Nakashima, "White House authorizes 'offensive cyber operations' to deter foreign adversaries," September 20, 2018, accessed September 20, 2018, https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html

operational capacity in 2018 with approximately 6,200 servicemembers spread across four functions.[121] The organizational growth of USCYBERCOM and the generation of an independent body of cyberspace doctrine indicates that cyberspace is being institutionalized as a strategic domain.

The creation of USCYBERCOM was the consequence of a sequence of organizational and conceptual shifts driven forward by two key domain advocates—Kenneth Minihan and Michael Hayden of the Air Force. As identified at the beginning of this section, there were multiple competing conceptions of the role that cyberspace and cyberspace capabilities would play in warfare. Primary among them was information warfare—war that operated within and upon information as a medium—which dominated the debates of the 1990s. There is little evidence that service leaders, even those within the Air Force, drove forward the infrastructural conception of cyberspace as a domain. Likewise, it is not clear that there was anything about the technology itself that drove the specific interpretation institutionalized through USCYBERCOM. The highly abstract nature of "cyberspace," a term to describe the existence and uses of networked information infrastructure, placed a premium on the conceptual articulation of what role cyberspace played in national security. The winning cyberspace domain vision, premised on three inter-related roles (CNA, CND, CNE), thereby necessitated that cyberspace be institutionalized as a domain as opposed to a set of capabilities or bundle of distinctive missions.

Conclusion

In this paper, I have sought to resolve a foundational question for understanding cyberspace and international security: why cyberspace is articulated as a military domain—similar to air, land, sea, and space—by the U.S. military. My theory of domain development identifies the key process for this outcome: military domain advocates who work to institutionalize a vision of spatially distinct warfare. Crucially, my argument illuminates why the U.S. adopted a conception of cyberspace and

[121] Mark Pomerlau, "Cyber Command reaches critical staffing milestone," May 17, 2018, accessed June 4, 2018, `https://www.fifthdomain.com/dod/cybercom/2018/05/17/cyber-commands-cyber-warriors-hit-key-milestone/`

cyberwarfare that is premised on military action within and through infrastructure instead of information warfare. My other case study, on the institutionalization of the air domain, demonstrated that there are substantial similarities between cyberspace and other technologically mediated domains. In both cases, the core work of advocating for and conceptually elaborating the role of the new domain was driven forward by low and mid-level officers seeking to institutionalize in doctrine and organization their domain vision. These cases also reveal that large-scale military change is a slow process and that the nature of that change is unlikely to be visible in the pronouncements of service leadership.

The contingent nature of domain institutionalization explains why there is substantial variance both within the U.S. and cross-nationally over the nature and status of cyberspace in conflict. Domains are social facts and states, militaries, and societies have not yet converged on a common understanding of what role cyberspace plays in conflict. Due to this variation, further research is necessary to contrast the U.S. conception of cyberspace alongside other major powers such as China and Russia. While existing scholarship has identified key differences at the level of strategy between these states, domain visions explain deeper patterns in organizational structures and doctrinal focuses. Similarly, scholarship must also address the processes by which new domains develop for other militaries. Finally, given major similarities between air forces across the world, the mechanisms by which states come to share conceptions of military domains must be identified.

On a substantive level, if cyberspace is a strategic domain then it is necessary to reckon with what might be the most revolutionary aspect of its development—the creation and naturalization of new forms of vulnerability. A military domain not only defines patterns in military organization and doctrine but also naturalizes ways of inflicting harm and enables new forms of vulnerability. In the case of the air domain, the shift from confronting enemy aircraft in the air to bombing the industrial centers of states justified expanding violence beyond the space of a battlefield and into the civilian interior of a country. Industrial-web theory thereby naturalized the large-scale killing of civilians and destruction of infrastructure for strategic purposes. Institutionalizing large-

scale strategic bombardment extended the vulnerability of a combatant to every individual within a state. The most radical aspect of cyberspace as an infrastructural domain is that it deepens and widens vulnerability in warfare. This is for two reasons: first, the medium of cyberspace operations are the computing devices and information networks largely held or operated by private parties. Second, powerful cyberspace capabilities are dependent on utilizing flaws or "exploits" that exist within these computing devices and information networks.[122] Exploits are not exclusive and only useful as long as they are kept private thereby generating strong incentives for states to hoard them. This extension and stabilization of infrastructural vulnerability is not theoretical—a series of malware attacks in 2017 utilized exploits from a stolen NSA cyber-toolkit.[123] Cyberspace as an infrastructural medium of war has created a dynamic whereby the devices deeply integrated into everyday life are kept vulnerable for exploitation. This creates a paradox: the development of cyber-capabilities is fundamentally dependent on stabilizing cyber-insecurity.

[122] Valeriano and Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, 20-45

[123] Nicole Perlroth and David Sanger, "Hacks Raise Fear Over N.S.A. s Hold on Cyberweapons," June 28, 2017, accessed July 23, 2017, https://www.nytimes.com/2017/06/28/technology/ransomware-nsa-hacking-tools.html