Traveling Domain Theory:

A Comparative Approach for Cyberspace Theory Development

A Thesis
Presented to the Faculty
Of
The Fletcher School of Law and Diplomacy

By

Thomas David McCarthy

In partial fulfillment of the requirements for the
Degree of Doctor of Philosophy

May 2012

Dissertation Committee
Dr Robert L. Pfaltzgraff, Jr., Chair
Dr. William C. Martel
Dr. Stephen E. Wright

Copyright 2012

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

THOMAS D. McCARTHY

Born San Juan Puerto Rico, 1968

Education

- The Fletcher School of Law and Diplomacy, Tufts University, Medford, MA
  - 2008-2012: Ph.D.
- Air University, Maxwell AFB, AL
  - 2003-2004: Master of Airpower Art and Science, School of Advanced Air and Space Studies
  - 2002-2004: Master of Military Operational Art and Science, Air Command and Staff College, Distinguished Graduate
- The George Washington University, Washington, DC
  - 1996-1998: Master of Arts in Organizational Management, The Columbian School of Arts and Sciences
- United States Air Force Academy, Colorado Springs, CO
  - 1986-1990: Bachelor of Science in Management

Seminars and Short Courses

- Institute for Qualitative and Multi-Method Research, 2011 – Syracuse, NY, The Maxwell School of Syracuse University
- Political Leadership and U.S. National Interests, Public Policy Seminar, 2011 – Washington, D.C., Alan L. Freed Associates

Professional Experience

- ***Air University, Montgomery, AL: Professor of International Security Studies,*** Director for Air War College Language & Cultural Studies: 2011-2012
- ***White House, Washington, D.C.:*** Military Aide to the President, 2005–2008
- ***Pentagon, Washington, D. C.:*** USAF XOXS, Deputy Chief of Strategy Branch, 2004–2005
- ***Hurlburt Field, FL:*** Group Tactics Officer, 2001-2002, Deployed Mission Commander, 2001, Flight Commander/Instructor Pilot, 1999-2000, Mobility Officer, 1998
- ***Pentagon, Washington, D. C.:*** Air Force intern Office of the Deputy Secretary of Defense, 1996–1998
- ***RAF Mildenhall, England:*** 21st Special Operations Squadron Planner and Aircraft Commander, 1995-1996
- ***Albuquerque, NM:*** Student Pilot, MH-53, 1994-1995
- ***Kadena Airbase Okinawa Japan:*** Aircraft Commander and Squadron Budget Officer, 1992-1994
- ***Fort Rucker, Al:*** Student Pilot, 1990-1991

Instructional Experience

- Global Security course, Air War College, Air University, Maxwell AFB Montgomery AL, Spring 2012
- National Security Decision Makers – The Department of Defense, guest lecturer: Poli 3160, U.S. National Security Policy (Auburn University) – Professor Jim Seroka. September 2011.
- Instructor Pilot, MH-53 J/M

Conferences and Presentations

- "Domain Transference: The Maritime and Air Models for Cyber Theory Development" – presentation and panel discussion, Doctoral Conference, The Fletcher School, September 2011
- Moderator: Gen Hap Arnold Lecture Series, February 2012

Service, Volunteer, and Affiliations

- American Political Science Association (member)
- International Studies Association (member)
- Student Representative – Methodology Faculty Hiring Committee (Spring 2011)
- Student Chair 4th annual Fletcher PhD Conference (2010)
- Fletcher Ph.D. Colloquium (2008-2011)

Skills

- Spanish: Writing–tested intermediate, Oral–functional business (2008)
- Helicopter Pilot with over 2000 hours of operational and combat experience

Abstract

In response to the growing importance of the cyber domain, government institutions are setting policy, proposing legislation, and creating unique organizations wholly dedicated to its development and security. Simultaneously, academic, military, and commercial interest groups are working to define and describe the field, producing volumes of literature and warning of ever-increasing threats. There is, however, no comprehensive cyber theory to anchor efforts across the government, among scholars, and between concerned interest groups.

This is not the first time nations have developed a new domain without clear overarching guidance. Over the last 150 years, the maritime, air, and space domains have seen similar unsettled periods. These initial unsettled periods are what Rosenau terms the pre-theory stage, a time during which competing ideas and terminology jockey for acceptance by researchers, scholars, and practitioners in the field. As ideas in sub-fields of study gain widespread acceptance, the challenge to further theory maturation becomes one of tying them together into a general framework for further analysis. This research project seeks to provide the outlines for this framework regarding cyberspace.

Drawing from the seminal maritime and air theorists who wrote during the technologically driven expansion of their subject domain, this study identifies eighteen common elements of domain power theory. Applying these elements to the cyber domain reveals critical aspects of the domain and highlights areas a mature cyber theory must address. This process suggests a way forward for development of cyber theory and areas for future research. A key finding is that a nation's cyberpower potential depends on

three factors: 1) the ability of its national government to coordinate and enforce long-term cyber strategy, 2) the nation's cyber geography, and 3) the character of its population.

Acknowledgments

I thank my wife, Beverly, for picking up the pieces and carrying more than her fare share of the burden these last four years. She has always been there to take over when my attention needed to be elsewhere; she is a fantastic wife and mother. Thank you to my beautiful daughters for understanding when I needed to study, and for being there always to remind me of what is important in life.

I also thank my committee members, not simply for their efforts on this dissertation, but also for their guidance and advice through the last four years. Dr. Pfaltzgraff, thank you for your understanding and guidance through the entire PhD process as both my academic advisor and then as committee chair. From the first day we met in Washington, DC, I have enjoyed the chance to work with you. I value the experience of narrowing down the dissertation topic and your encouragement to take this subject on. Dr. Martel, as my first Fletcher instructor, you set the tone for my experience there. I appreciate the cyber discussions in your office and the opportunity to work with you on the Cyber Studies Group. Your research recommendations and insights gave me direction to keep looking during the long hours of this work. Dr. Wright, as the Dean at AWC, you selected me for the Air Force PhD program, for which I am eternally grateful. Our discussions about the research process and PhD programs in general helped shape my experience and my research focus. I appreciate your willingness to provide feedback along the way; it was a great help in keeping me on track.

Table of Contents

List of Tables

List of Figures

> So long as the United States – the Nation that created the Internet and launched an information revolution – continues to be a pioneer in both technological innovation and cybersecurity, we will maintain our strength, resilience, and leadership in the 21st century. – President Barack Obama

Chapter 1: Domain Theory and the Geopolitics of Cyberspace

President Barack Obama proclaimed October 2010 National Cyber Security Awareness Month. His announcement proclamation identifies America's digital infrastructure as a critical foundations for our nation's continued "economic prosperity, government efficiency, and national security."[1] Calling upon all the people of the United States to enhance security and resilience, he identifies the protection of our digital infrastructure as a national security priority. Unfortunately, for strategic planners and the government officials responding to his call for action, no theory of cyber strategy exists to guide development of cyberspace policy.[2] To begin filling this gap, the following research project establishes a theoretical foundation for building a theory of cyberpower.

Efforts to bring order to the process of developing cyber domain policy are already under way.[3] Importantly, the growing significance of cyberspace is included in

---

[1] Proclamation U.S. President, "National Cybersecurity Awareness Month," (Washington, DC: Office of the Press Secretary, 2010).

[2] The term *cyberspace* is was coined by the science fiction writer William Gibson, first appearing in print as part of his 1982 short story "Burning Chrome," published in *Omni* magazine. William Gibson, "Burning Chrome," *Omni*, 1 July 1982. The term reappears and becomes more widespread with his publication of *Neuromancer* in 1984. In this work he uses the term more than twenty times.———, *Neuromancer*, Ace Science Fiction (New York: Ace Books, 1984). A short etymological history of the term by Dr. Rick Sturdevant was published in *High Frontier* in 2009: Rick W. Sturdevant, Dr., "Cyberspace: An Etymological and Historical Odyssey," *High Frontier* 5, no. 3 (2009).

[3] The online Merriam-Webster dictionary provides ten definitions for *domain*. Most applicable to our discussion of the cyber domain are #2, "a territory over which dominion is exercised," and #4, "A sphere of knowledge, influence, or activity." Merriam-Webster Dictionary, "Domain, n," Merriam-Webster, Incorporated, http://www.merriam-webster.com/dictionary/domain.

the capstone US planning document, the 2010 US National Security Strategy (NSS), which identifies cyberspace and cyber security as critical to the future economic and military security of the United States.[4] Such high-level recognition has spawned numerous government and commercial sector efforts to design and implement policies for ensuring access to cyberspace for government, commercial, and private purposes.[5]

Because cyberspace operations have become a critical part of every element of national power – diplomacy, information, military, and economic (DIME) – the challenge for policy makers is to coordinate efforts across different agencies and different levels of federal, state, and local governments. Coordinating domain development policy across all agencies and all interest groups for each element of national power is an overwhelming task.

Without well-established and widely accepted theory to provide guidance, individual agencies develop, coordinate, and implement policy based on their own organizational needs, not on overall national security requirements.[6] Because virtually

---

[4] "National Security Strategy of the United States 2010," ed. White House (2010), 27.

[5] For example, on the economic front, the Federal Communications Commission (FCC) has begun to regulate Internet traffic and service to preserve competition among domestic providers. This effort is economically oriented and designed to limit the role market forces and technology play in driving domestic Internet development from an economic standpoint, subject to lobbying by the affected commercial interests. There is no clear and coherent national cyber strategy for meshing FCC concerns for domestic competition with international strategic competition and military uses of the domain. For an example of the concern regarding the FCC's actions, see Meredith Attwell Baker, "Hands Off Tomorrow's Internet," *The Washington Post* on-line (2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/12/20/AR2010122003901.html?wpisrc=nl_opinions.

[6] Efforts to coordinate government efforts are in their infancy with the recognition of the need to designate a cybersecurity coordinator. As of 2009, "no single individual or organization is aware of all of the cyber-related R&D activities being funded by the Government. This initiative is developing strategies and structures for coordinating all cyber R&D sponsored or conducted by the US government, both classified and unclassified, and to redirect that R&D where needed." U.S. National Security Council, "The Comprehensive National Cybersecurity Initiative," (Washington, DC 2009), 3. See also White House, "Cyberspace Policy Review: Assuring a

every department within government uses cyberspace for some critical aspect of its mission, bureaucratic and organizational interests hamper the development of coordinated policy across the US government. It is difficult to coordinate across distinctly different government institutions, each with responsibility for overseeing a unique yet interconnecting piece of cyberspace. For example, the Department of Homeland Security is responsible for securing cyberspace within the United States, the Department of Defense (DOD) for securing its own systems and developing war-fighting capabilities, and still others, such as the FCC, for development of commercial standards.[7] Without a common framework to reference, each of these organizations approaches cyberspace through its own institutional lens, bringing with it unique organizational goals and objectives, complicating the cross-government coordination process.

In addition to the challenge posed by the distribution of responsibilities among Cabinet-level agencies, competing perspectives on the authority to conduct operations legally in cyberspace for ensuring US security interests exist. For example, the DOD and Central Intelligence Agency (CIA) both lay claim to offensive cyber requirements. The CIA takes the position that covert cyber operations outside of a battle zone are legally its responsibility. The DOD, however, is interested in conducting peacetime off-battlefield operations to gather intelligence for conducting first-strike operations affecting an adversary's ability to defend itself. Simultaneously, the State Department is concerned about diplomatic backlash from operations conducted by either party.[8] Obviously, each

---

Trusted and Resilient Information and Communications Infrastructure," (Washington, DC 2009), 7.

[7] For an example of the emerging role played by the FCC, see Baker, "Hands Off Tomorrow's Internet."

[8] Ellen Nakashima, "Pentagon is debating cyber-attacks," *The Washington Post*, 6 November 2010.

department brings its own perspective to the policy development process. Sorting these perspectives and prioritizing agency requirements requires a holistic understanding of cyber domain power that only a fully formed cyber theory can provide.

In searching for a theoretical basis for cyberpower theory, this research project takes advantage of a rapidly growing body of cyber literature. The combined efforts of government agencies, academics, and cyber operators have produced literature touching upon development of cyberspace, the pace of technological change, our increasing reliance on cyber-provided information, and the threat posed by state and non-state actors to economic and military security.

These are just a few of the widely varied subjects falling under the cyber umbrella. For those seeking to plan and operate in the cyber realm, however, the lack of connective themes through the growing array of cyber literature is frustrating and demonstrates the relative infancy of this domain. Much of the available literature is dedicated to defining cyberspace in general and identifying potential problems, not providing guidance for policy makers. Without guidance, they have no coherent and consistent approach to ensure the United States positions itself to use cyberspace to its advantage.

Understandably, many writers focus on the threat posed by cyber actors to the security of the United States and not the development of cyber strategy. This is certainly true within the DOD and its associated institutions. As the largest of the numerous government agencies grappling with the problems of cyberspace, the DOD and associated research organizations have taken a leading role in developing government cyberspace policy and analyzing its effects. To date, “the DOD is the department largely responsible

for the federal government's cybersecurity efforts alongside the Department of Homeland Security [DHS]."[9]

Military leadership in the development of new domain theory is not without precedence. Over the previous 150 years, new technology has opened the sea, air, and space domains to competition between nations. The military has often taken a lead role in stimulating both the academic and policy process as it relates to these domains because as a general rule, it is well organized, has relatively large research budgets, and is under political and social pressure to safeguard national interests as they emerge. In each instance, the seminal military strategists of these domains used existing theory as a template to begin their work. It is reasonable to assume that efforts to create a theory of cyberpower should also look to existing theory for guidance. To date, no detailed analysis of existing theory to create a framework for cyber theory has taken place.[10]

[9] Elizabeth Montalbano, "DOD Website Sells Public On Cybersecurity Strategy," *Informationweek - Online*, no. 19383371 (2011), http://www.informationweek.com/news/government/security/231002588#.

[10] Two recent US publications do include work by Greg Rattray in which he explores the environmental nature of the cyber domain, comparing it to the land, sea, air, and space domains for physical characteristics and identifying some of the major theorists in those domains. Those publications are: Abraham M. Denmark and James Mulvenon, eds., *Contested Commons: The Future of American Power in a Multipolar World* (Center for a New American Security,2010), and Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security*, 1st ed. (Washington, DC: Potomac Books, 2009). His efforts, however, do not contrast the elements of the predominant domain theories to determine their suitability as guides for development of cyber theory, nor does he try to develop principles to guide development of cyber theory.

Cyberspace: Not Designed with Security in Mind

> "Attacks can be masked and routed across several networks, obscuring whether they are the work of independently operation 'patriotic hackers,' criminal groups, an official security agency, bored teenagers, or some combination of all four."[11]

At the heart of security concerns harbored by cyber professionals is that the design of the domain optimizes connections between systems, intentionally making it easy to add new components to the network. During the 1950s and 1960s, researchers working in laboratories undertook the challenge of networking computers to facilitate the exchange of information. During these early years, the connections between computers were known, users were trusted, and computer viruses yet to be invented. These researchers had no reason to emphasize security. They designed the system "to be collaborative, rapidly expandable, and easily adaptable to technological innovation. Information flow took precedence over content integrity; identifying authentication was less important than connectivity."[12]

Instead of security, the protocols used during these early years of cyber development emphasized speed and adaptability within local area networks. As more individual computer networks emerged, researchers developed standardized protocols to allow the exchange of data between formerly disconnected systems. These standardized protocols also emphasized speed and adaptability over security. Once standardized protocols were set in place, the path to creation of even larger networks lay open –

[11] Adam Segal, "Cyberspace Governance: The Next Step, Policy Innovation Memorandum No. 2," (Council on Foreign Relations, 2011), 2.
[12] Office of the Secretary of Defense U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," (Washington, DC 2011), 2.

today's networks retain these legacy protocols and unfortunately their security vulnerabilities.[13]

In reality, the Internet is not just one network; it is a vast network of interconnected networks all communicating through standardized, and open, architecture. The domain's intentional lack of security is a useful characteristic when viewed from the perspective of its effect on modern society. The ability to access cyberspace freely allows the proliferation of interconnected devices, revolutionizing the movement of data and changing modern life. The unfortunate side effect of this open characteristic is that no agency or group brings order the domain's development. No "one agency, either nationally or multilateral, exerts authority over all parts of the web."[14]

The State of Cyber Affairs

A Dynamic New Domain

The domain's lack of oversight is a cause for concern. Misuse of the domain increasingly threatens the safety and security of other users; crime, espionage, and interstate conflict have all migrated from the traditional domains and taken root in cyberspace. Concerns about the unregulated development of cyberspace are not new to those working in the field, however. Joseph Nye points out that "techies have been aware

[13] Numerous accounts describing the Internet's development are available for readers interested in the domain's history. I suggest the "Brief History of the Internet," found online and written by some of the original Internet pioneers: Barry M. Leiner et al., "A Brief History of the Internet," http://www.isoc.org/internet/history/brief.shtml. A key point is that the Internet is still growing and evolving. The Internet Society (ISOC) website is a good source of information regarding ongoing efforts to aid this evolution. Find their home page at: http://www.isoc.org/isoc/.
[14] Segal, "Cyberspace Governance: The Next Step, Policy Innovation Memorandum No. 2," 1-2.

of cyber problems for some time; political leaders and strategists are just beginning to come to terms with cyberpower."[15]

What they are coming to terms with is the widespread recognition that the effects of cyber attacks will not be limited to the destruction of military capabilities; in cyberspace, everything is on the table. In addition to military targets, cyber attacks are likely to target critical civilian economic and social infrastructure. As noted in a National Research Council report:

> The range of possibilities for cyberintrusion is quite broad. A cyberattack might result in the destruction of relatively unimportant data or the loss of availability of a secondary computer system for a short period of time – or it might alter top-secret military plans or degrade the operation of a system critical to the nation, such as an air traffic control system, a power grid, or a military command and control system. Cyber exploitations might target the personal information of individual consumers or critical trade secrets of a business, military war plans, or design specifications for new weapons. Although all such intrusions are worrisome, some of these are of greater significance to the national well-being than others.[16]

[15] Joseph S. Nye, "Facing up to cyber security challenges," *Policy and Power* (2011), http://belfercenter.ksg.harvard.edu/power/2011/06/13/facing-up-to-cyber-security-challenges/.
[16] Committee on Detering Cyberattacks, "Letter Report from the Committee on Deterring Cyberattacks: Informing Strategies and Develping Options for U.S. Policy," ed. National Research Council (Washington, DC: National Academy of Sciences, 2010), 3. The quote here itself references a larger work, also published by the National Research Council, that provides an in-depth overview of cyber attacks and the complicated issues surrounding them: William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press,2009).

Of growing concern is the ease with which nations and non-state actors take advantage of the relatively insecure cyber environment to threaten other international actors. Mike McConnell, the former Director of National Intelligence, likens the proliferation of cyber capabilities to the proliferation of nuclear weapons – only the former is easier.[18] Fears of terrorist groups or rising economic and military competitors such as China using cyber weapons to threaten US interests have begun focusing the executive branch, lawmakers, and defense officials on Internet security and defense of existing infrastructure and capabilities. The majority of the threat posed by terrorist groups, non-state actors, and economic competitors comes from probes of existing systems to conduct cyber crime,

> On April 8, 2010 for a period of 16 minutes, Chinese routers sent erroneous information to the network of routers that control the flow of Internet traffic, falsely indicating that they were the fastest routing for Internet traffic. This false reporting took advantage of a basic security flaw in Internet routing that currently relies on a system of mutual trust to determine traffic flow. During this period, an estimated 15% of all traffic was routed through Chinese servers, leaving that traffic open to capture and analysis. There is no way to clearly determine if any of the traffic was altered or even to determine if the incident took place as part of a deliberate action. Such an action might have been instigated to test response times and countermeasures of other nations to purposeful changes in Internet traffic flow. The importance of this incident is less the threat posed by China's demonstrated capability to re-route Internet traffic; instead, "the real significance of the incident is that it has captured the attention of US lawmakers, who are increasingly interested in drafting legislation to bolster Internet security and increasingly suspicious of China."[17]

[17] This incident, detailed in the US-China Economic Security Review Commission 2010 report to Congress: U.S. China Economic and Security Review Commission, "2010 Report to Congress of the U.S.-China Econiomic and Security Review Commission," ed. U.S. Congress (Washington DC: U.S. Government Printing Office, 2010), 243-44. The incident's significance is analyzed by STRATFOR: STRATFOR, "A Report on China's Internet Traffic 'Hijacking'," *STRATFOR Global Intelligence* (2010).

[18] Nathan Gardels, "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly," *New Perspectives Quarterly* 27, no. 2 (2010): 16.

cyber espionage, or theft of industrial secrets. As a result, many of the authoritative calls for action today focus on securing the domain for commercial use, not for creating military-grade offensive and defensive capabilities.

The focus on general cyber security makes sense from an operational perspective but not from a long-term national security policy perspective. Current threats should not be the only source we use to guide the development of cyber theory, policy, and doctrine. As pointed out by Professor Jeffrey Caton of the US Army War College, "prudence dictates that we 'lead the target' as we develop theory for cyberspace."[19] In this context, leading the target is looking forward into the rapidly developing cyber domain and asking what it will look like in the future, questioning what opportunities and vulnerabilities will exist, and planning to meet them head on. At this point in the domain's development, however, we do not have the theoretical tools to make these assessments.

Recognizing the Need for Action

The federal government has recognized the need for a comprehensive approach to cyber policy development. In an effort to provide leadership for the creation of cyber policy, the Obama administration is working to construct a coherent strategy to guide defense of the US from attacks on computer and information systems that will damage power grids, corrupt financial transactions, or disable Internet providers.[20] This effort comes upon the heels of many similar efforts initiated through Congress and the previous administration, most of them unsuccessful.

---

[19] Jeffrey Caton, "The Future of National Security in Cyberspace: Are We Leading the Target?," in *Dime Blog*, U.S. Army War College (U.S. Army War College, 2010). Jeffrey Caton is Professor of Cyberspace Operations at the US Army War College.
[20] Nakashima, "Pentagon is debating cyber-attacks," A1.

Congress introduced approximately fifty cyber security–related bills within the last three years, the White House released a cyber security legislative proposal, and both the FCC and Commerce department proposed new cyber regulations.[21] Despite the flurry of activity, Richard Clark points out that "Congress hasn't passed a single piece of significant cybersecurity legislation."[22]

The bureaucratic system hampers Congress and other institutions in their efforts to provide cyber policy guidance; they are unable to keep pace with rapid developments in the domain.[23] From outside of government, calls for greater clarity in establishing US interests are numerous and seek to spur the government toward action. Illustrative of these efforts is a Council on Foreign Relations 2011 memorandum suggesting that two cyber declaratory statements are necessary: one clarifying what threshold of attack constitutes an act of war and another declaring "digital safe havens."[24] This level of clarification would be much easier to provide if we had strong domain theory to guide our actions.

Calls for guidance and movement toward securing the United States' cyber future are not limited to simply providing security for computer systems and the information they contain. From a national security perspective, equally important to the future security of cyber domain infrastructure is the need to create a population with the prerequisite skills and aptitude for cyberpower.

---

[21] Jerry Brito and Tate Watkins, "The Cybersecurity-Industrial Complex: The Feds Erect a Bureaucracy to Combat a Questionable Threat," *Reason* 43, no. 4 (2011).
[22] Richard Clark, "China's Cyberassault on America," *The Wall Street Journal* (2011), http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html?mod=wsj_share_facebook.
[23] Caton, "The Future of National Security in Cyberspace: Are We Leading the Target?." Safe havens are areas consisting of civilian targets the US "will consider off-limits when it conducts offensive operations."
[24] Segal, "Cyberspace Governance: The Next Step, Policy Innovation Memorandum No. 2," 1.

In order to ensure continuing cyber advantage, the US must develop a technologically skilled and cyber-savvy workforce through focused science, technology, engineering, and mathematics (STEM) education and training.[25] In 2007 General James Cartwright, then Vice Chairman of the Joint Chiefs of Staff, recognized a lack of cyber-focused STEM as an emerging national security shortfall. Speaking on the requirement to build national cyberpower, he stated, "We as a nation don't have a national lab structure associated with this, so we aren't growing the intellectual capital we need to, at least at the rate that we need to be doing."[26] Echoing his concerns, the 2009 *Comprehensive National Cybersecurity Initiative* (CNCI) identified the requirement for a national strategy to upgrade cyber education in the United States to ensure we have people with the right knowledge, skills, and abilities for cyber operations.[27]

Emerging Cyber Guidance

Despite the lack of either cyber theory or integrated policy guidance, efforts are under way to bring order to the cyber development process. Beginning with Presidential Decision Directive 63 (PDD-63) in May 1998, the Executive Branch has sought to coordinate government actions to secure the cyber domain. The 2003 release of the *National Strategy to Secure Cyberspace* updated PDD-63 and recognized the importance

---

[25] U.S. National Security Council, "The Comprehensive National Cybersecurity Initiative," 4. Adapted from Initiative #8 which is titled: Expand cyber education.

[26] James E. General Cartwright, USMC, "AFA's 2007 Air Warfare Symposium Transcripts," AFA, http://www.afa.org/events/AWS/2007/post_Orlando/scripts/cartwright.asp. Accessed at: http://www.afa.org/events/AWS/2007/post_Orlando/scripts/cartwright.asp.

[27] U.S. National Security Council, "The Comprehensive National Cybersecurity Initiative," 4. Initiative #8, titled Expand Cyber Education, discusses the fact that there are not enough cybersecurity experts within the Federal Government or Private sector to implement government cybersecurity plans and coordinate efforts across the federal government and private industry.

of the cyber domain to national security.[28] Additionally in 2003, the White House released Homeland Security Presidential Directive 7 (HSPD-7) designated the Secretary of DHS as the principal federal official to lead, integrate, and coordinate efforts among federal departments and agencies. This same directive also tasked the Secretary to liaison with state and local governments as well as the private sector to protect national critical infrastructure and key resources to include technology, telecommunications, chemical, transportation, and postal facilities as well as key dams, government, and commercial facilities.[29]

As the importance of cyber interaction continued to grow, so too did recognition of the requirement for strong government leadership. In 2007 the Bush Administration's CNCI further updated the Executive Branch's efforts to organize national efforts across the cyber domain. The CNCI picks up where HSPD-7 left off, seeking to coordinate efforts by the DHS and commercial industry to secure domestic infrastructure. It also seeks to strengthen and bring together the efforts of federal law enforcement, intelligence, and defense to improve cyber security through coordination of efforts across numerous government agencies.[30]

The Obama administration has continued efforts to focus and coordinate cyber security across the federal government. Cyberspace now figures prominently in the National Security Strategy, featured as a means of advancing national interests

---

[28] U.S. President, *The National Strategy to Secure Cyberspace* (Washington, DC: Dept. of Homeland Security, 2003). An overview of the executive department's actions regarding major cyber guidance can be found in the 2009 Cyberspace Policy Review: White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," 4.

[29] Bush Administration, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," ed. Executive Office of the President (Washington, DC 2003).

[30] U.S. President, "National Cybersecurity Awareness Month."

worldwide.[31] Additionally, in 2009, the Obama administration issued a *National Cyberspace Policy Review* and in May 2011 followed up with the *International Strategy for Cyberspace,* which makes cyber security efforts one of America's foreign policy priorities. This international strategy also identifies cyberspace as an international concern, suggesting that properly addressing it requires international cooperation.[32]

Parallel to White House efforts, within the Department of Defense (DOD), the 2006 Quadrennial Defense Review process found that the DOD "lacks a coherent framework to assess cyberpower policy issues."[33] Shortly after this, the DOD released a *National Military Strategy for Cyberspace* to act as a starting point to build a strategic framework for cyber development in support of the *National Security Strategy* and *National Military Strategy* guidance.[34] More recently, in addition to integrating cyber operations into various planning guidance, on 14 July 2011 the DOD released the *Department of Defense Strategy for Operating in Cyberspace*, its first formal strategy for operating in cyberspace.[35]

Included in this strategy are five strategic initiatives to guide cyberspace development and integrate DOD efforts with both domestic and international partners. The five pillars of this strategy are:

1. Treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of cyberspace's potential.

---

[31] U.S. President, "National Security Strategy," (Washington, DC 2010), 27. The term *cyber* appears on 11 of the 2010 NSS's 52 pages.
[32] White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." See also U.S. President, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," (Washington, DC 2011).
[33] Kramer, Starr, and Wentz, *Cyberpower and National Security*, XV.
[34] Joint Chiefs of Staff U.S. Department of Defense, "The National Military Strategy for Cyberspace Operations," ed. Chairman Joint Chiefs of Staff (Washington, DC 2006).
[35] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace."

2. Employ new defense operating concepts to protect DOD networks and systems.
3. Partner with other US government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.
4. Build robust relationships with US allies and international partners to strengthen collective cyber security.
5. Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.

In addition to issuing operational guidance, the DOD has created Cyber Command, a sub-unified command under US Strategic Command to coordinate, integrate, and synchronize DOD operations in the domain.[36] Cyber Command became operational on 21 May 2010. Drawing operational forces from cyber operating units set up by each of the various military services and defense agencies, Cyber Command is the DOD's lead for planning, coordinating, and conducting operations for the day-to-day defense of the DOD information networks.[37] In keeping with the third of the five strategic initiatives from the *Strategy for Cyberspace Operations*, Cyber Command will assist upon request the DHS to protect critical private sector infrastructure.[38] Despite all these efforts, there is still no well-coordinated, comprehensive framework to guide policy development.

Cyberpower Development Requires Guidance

What is missing from efforts to create comprehensive cyber policy is a framework for use as a point of reference across institutions and interest groups when discussing the domain and evaluating policy options. Creating a framework is becoming increasingly

[36] U.S. Cyber Command Public Affairs, "U.S. Cyber Command Fact Sheet," http://www.stratcom.mil/factsheets/cyber_command/.
[37] US Cyber Command draws forces from each of the military services: USA – Army Cyber Command (ARCYBER); USAF – 24th USAF; USN – Fleet Cyber Command (FLTCYBERCOM); USMC – Marine Forces Cyber Command (MARFORCYBER). U.S. Department of Defense, "U.S. Cyber Command Fact Sheet," ed. U.S. Strategic Command (U.S. Department of Defense Office of Public Affairs, 2010).
[38] Nakashima, "Pentagon is debating cyber-attacks," A1.

urgent as the US and other nations take steps to create the tools necessary for ensuring they maintain the capability to perform military and commercial network-centric operations during times of peace and war. Like the US, many nations are already undertaking steps to create cyber agencies and even cyber military forces to protect their cyberspace interests.[39]

At this point in the domain's development, barriers to entry are low and the volume of traffic within the domain is relatively unconstrained by transmission capacity. Much like the development of other domains, the rush to utilize the domain for both commercial and governmental purposes is creating rapid technological, organizational, and legal challenges that once again require a proper comprehensive framework to address.

The rapidly evolving nature of the domain means that our early attempts to develop cyber strategy must focus on the creation of structures, processes, and people capable of adapting to the inevitable changes in the domain.[40] To guide and provide coherence to policies supporting these efforts, policy makers and scholars need a shared understanding of the domain and where it fits into the context of our national security

---

[39] The US for instance has created Cyber Command with the mission of defending the .mil domain and attacking adversaries: ———, "An army of tech-savvy warriors has been fighting its battles in cyberspace," *The Washington Post*, 24 September 2010. Numerous articles also refer to the development of cyber doctrine and government (military) units as well as partnerships between information technology experts and government intelligence and military organizations around the globe. Nations often cited as developing these capabilities are China, Russia, India, Iran, Pakistan, and North Korea. For an example of unclassified research into the development of overseas cyber capabilities, see Charles Billo and Welton Chang, "Cyber Warfare and Analysis of the Means and Motivations of Selected Nation States," ed. Technology Institute for Security, and Society (Hanover, NH: Dartmouth College, 2004).

[40] Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 5.

landscape. The creation of a theory of cyberpower is a necessary step toward creating this understanding.

Guiding the Research: Questions and Hypothesis

This project addresses the lack of cyberspace theory and provides a basis for further development of the field of study. It does not create a wholly independent theory with a defined relationship between dependent and independent variables in the more traditional social science model. The domain has not yet matured to the point where cyber scholars and operators share enough widely held beliefs to support a fully developed cyberspace theory. With this research, I suggest a point of departure to advance the theory development process by identifying aspects of existing domain theory that inform cyber theory development. The research questions used to guide this exercise ask what theoretical basis is useful as a point of departure for the comparative investigation of the cyberspace domain and which existing theories provide guidance for the creation of cyber theory itself. To be specific, the following two research questions drive this research project and generate the two associated research hypotheses:

Q1: What is the theoretical basis from which to develop cyber policies and strategies?

Q2: Can existing military domain theory inform the development of a starting point for a domain control theory of cyberspace?

The following two research hypotheses serve as a starting point for answering the research questions and bring organization and clarity to the research effort.

H1: Existing military domain theory can inform cyber theory development and provide a starting point for theory expansion.

H2: Cyberspace is a physical domain, with a defined geography and geostrategic attributes similar to established domains.

Underlying this project is the assumption that nations pursuing national security objectives in the cyber domain will seek to control the domain, as they do the other designated military domains. In a geopolitical sense, control of the domain is the ability to ensure freedom of movement through the domain while denying the same to adversaries. This concept is readily apparent in land, maritime, and air theories, and it is reasonable to assume it will also apply to the transmission of information over lines of communication in the cyber domain. While this assumption does not act as a formal hypothesis, I assess its validity during the process of answering the research questions.

By answering the two research questions above, this research provides evidentiary support for the role of existing theory in the development of the new cyber domain. Validation of the two research hypotheses similarly provides the basis for future research expanding on this work.[41] In evaluating the ability of existing domain theory to serve as a basis of cyber theory development, the focus here is on identifying the similarities and differences between existing domain theory as shaped by the unique environment each seeks to control and then projecting these attributes into the cyber environment to identify areas of congruence and differentiation. These areas of congruence and differentiation provide guideposts for the theory development process.

[41] Hypothesis 2, concerning the physical nature of cyberspace, is not an entirely new and unaddressed hypothesis. Recent DOD publications make reference to the cyber domain's physical nature. The fact that this nature is not widely recognized outside of the narrowly defined cyber community of interest provides enough uncertainty that for purposes of this investigation I must avoid making the physical nature of the domain an assumption and address the issue head on before using physical domain theories to evaluate cyberspace. I review the argument for cyber's physical nature below in Chapter 3.

Chapter 2: Theory and Methodology

Until now, the United States has developed cyber capabilities, policy, and military doctrine without the backstop of cyber theory. This chapter begins the process of creating a baseline for cyber theory development through the extension of existing domain theories. It begins by briefly reviewing the nature and purpose of theory in general and highlighting the purpose of military theory in the national security development process. Having demonstrated the role cyber theory will play in the national security process, the chapter concludes with a description of the methodology used in this research's analysis of extant theory and the subsequent evaluation of these theories' ability to serve as the foundation upon which to build cyber theory.

In the early 1990s, the explosion of personal, commercial, and governmental computing that created global networks of machines and systems, also created networks of people, institutions, businesses, and governments. These networks are rapidly altering and reducing the importance of geographic and temporal barriers to trade, diplomacy, and social interaction. This radical flattening of the world poses new national policy and security questions for the United States as discussed in the previous chapter.

In this interconnected post-Cold War environment, the United States finds itself contemplating questions similar to those it faced during the early twentieth century's rapid expansion of the maritime environment, an expansion driven by the advent of steam propulsion. Theorists and policy makers then as now sought to determine the effect of the domain's expansion on commerce, important and vital national interests, and foreign

policy.[1] Determining these effects is a critical step in identifying the role government should play in developing commercial and military interests within the domain.

> "'I've been working in computer security for 23 years,' says BP's Chief Information Security Officer John Meakin,' and it's really only in the last two or three years that policy-makers have begun to wake up.'"[2]

What is missing in the search for what we need to know about cyberspace is a means of tying together the disconnected pieces of what we do know about the new domain – in short, a theory. A theory attempts to make sense of what would otherwise be inscrutable, to set forth "rules of the game" by which actions become intelligible.[3] As the Prussian military strategist and theorist Carl von Clausewitz put it, theory "gives the mind insight into the great mass of phenomena and of their relationships, then leaves it free to rise into the higher realms of action."[4] Rising to higher realms of action for the purposes of discussing cyberpower development means the integration of national efforts across governments at the federal, state, and local levels as well as the integration and regulation of commercial interests and non-governmental organizations. Using guiding principles and theory to tie all of these efforts together is the

---

[1] Beyond the scope of this research but of interest are potential questions policy makers seek to find answers for while grappling with a new domain. These questions include:

- How involved should the nation be in developing commerce in the domain?
- What are the national security implications of the growth of cyber commerce and cyber communication to important or vital American interests?
- What role should the United States government play in developing commercial capabilities and the military forces necessary to defend American interests?
- What changes to American foreign policy does the emergence of the new cyber-induced geopolitical landscape require?

The proceeding questions are adapted from Jon Sumida, "Old Thoughts, New Problems: Mahan and the Consideration of Spacepower," in *Toward a Theory of Spacepower: Selected Essays*, ed. Charles D. Lutes, et al. (Washington: National Defense University Press, 2011), 4.

[2] Brigid Grauman, "Cyber-Security: The Vexed Question of Global Rules," (Brussels, BE: Security & Defense Agenda, 2012), 22. Here BP stands for British Petroleum.

[3] Abraham Kaplan, *The Conduct of Inquiry; Methodology for Behavioral Science*, Chandler publications in anthropology and sociology (San Francisco, CA: Chandler Pub. Co., 1964), 302.

[4] Carl von Clausewitz, *On War*, ed. Peter Paret and Michael Howard, trans. Peter Paret and Michael Howard (Princeton, NJ: Princeton University Press, 1976), 578.

critical task strategists, planners, and policy makers undertake during the process of developing and executing national security policy.

Theory, then, is a critical component of the national security process, providing insights into strategic relationships and interconnections that are vital to national interests, the lack of which hampers a nation's ability to create policy and plan strategically. The dearth of coherent cyberpower theory, and its effect on the development of the cyber domain, has not gone unnoticed. John Sheldon, a noted space and cyber domain theorist, has pointed out that until now the majority of cyberspace and cyberpower research and writing efforts have focused on either the technical aspects of the domain or the tactical and operational levels of employment.[5] While these efforts are useful in identifying critical aspects of the developing cyber domain, they fall short of providing a framework within which cyberpower can, and should, be developed and used to influence the strategic environment in order to create and benefit from national advantages during both peacetime and war.

If a lack of theory retards development of critical national resources and capabilities, the importance of developing a theoretical basis for cyberpower development should be obvious to anyone concerned with the long-term cyber security interests of the United States and its allies. The noted military historian Harold Winton has written on the importance of developing theory in support of critical national security interests, specifically military theory, and the role it plays in organizing phenomena within the military domains. At the macro levels of grand strategy where national security strategies are determined, theory is useful because it provides insight into the interrelation

[5] John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly* 5, no. 2 (2011): 95.

of various domains and the importance of their interactions within a greater geostrategic perspective. Although Winton has yet to directly apply his talents to analysis of the cyber domain, an adaptation of his 2011 discussion of efforts to develop military spacepower theory applies equally well to the development of cyberpower theory. The simple replacement of the word *spacepower* with *cyberpower* in his writing results in the following defense of efforts to create and refine cyber theory:

> The quest for a theory of [cyberpower] is a useful enterprise. It is based on the proposition that before one can intelligently develop and employ [cyberpower], one should understand its essence. It is also based on the historical belief that, over the long haul, military practice has generally benefited from military theory. While such a conviction is generally true, this happy state has not always been realized. Faulty theory has led to faulty practice perhaps as often as enlightened theory has led to enlightened practice. This does not necessarily call into question the utility of theory per se, but it does reinforce the need to get it about right. Taking the broader view, it is a trait of human nature to yearn for understanding of the world in which we live; and when a relatively new phenomenon such as [cyberpower] appears on the scene, it is entirely natural to seek to comprehend it through the use of a conceptual construct. Thus, one can at least hope that the common defense will be better provided for by having a theory of [cyberpower] than by not having one.[6]

With that setup and to frame this overall effort to provide a basis from which to begin building cyberpower theory, the next section discusses the nature and purpose of theory in general.

[6] Here the quote is as written by Winton with the word *cyberpower* swapped into the text to replace *spacepower:* Harold R. Winton, "On the Nature of Military Theory," in *Toward a Theory of Spacepower: Selected Essays*, ed. Charles D. Lutes, et al. (Washington, DC: National Defense University Press, 2011), 19. Although the quoted text and the chapter from which it is taken appear in a book assessing the development of spacepower, it is primarily a discussion of military theory, its development, and its purpose and is therefore relevant to this effort.

Theory

The 2007 Oxford English Dictionary offers five definitions of *theory,* two of which have particular relevance to this effort:[7]

1. A mental scheme of something to be done, or of a way of doing something: a systematic statement of rules or principles to be followed.
2. The knowledge or exposition of the general principles or methods of an art or science, esp. as distinguished from the practice of it.

Both of these alternative definitions convey to the reader that theory is neither an unchallenged final description of a subject nor a prescriptive process. Instead, theory provides insight into the relationships between elements of a given subject. Theories are not infallible; they are the formal expression of presumptions about the interrelation of the elements making up any given phenomena based on the best understanding of the subject available to researchers at any given time. Far from being infallible, theory acts as a guide in the ongoing search for information, explanation, and solutions; it serves various purposes depending on the nature and scope of the subject matter it addresses.

Theory serves various purposes depending on the field of study with which it is associated.[8] Theories of the hard sciences, such as physics, mathematics, and astronomy, integrate and organized empirical laws into deductive systems; they are tools for use in objectively observing and gathering quantifiable empirical data. The hard sciences take an instrumentalist perspective on the use of theory; in these fields, theory defines a

[7] "Theory," in *Shorter Oxford English Dictionary* (Oxford, UK: Oxford University Press, 2007), 3233. The Oxford dictionary lists five distinct definitions, breaking #3 down into two distinct parts, "a" and "b." The definitions presented here are #1 and #3a.

[8] Kaplan, *The Conduct of Inquiry; Methodology for Behavioral Science*, 302-03, and 06. While the basis for much of this paragraph is general knowledge, at its heart I have adapted Kaplan's description of two completing perspectives on the use of theory: the realist and instrumentalist perspectives. I have attempted here to project them into the national security field, which is in many ways a soft science but generates extensive hard data for decision making.

starting point and means for further research.[9] In the soft and social sciences, such as psychology and economics, theories serve less as a starting point than as an aid to forming empirical laws and defining expected relationships and interconnections. This is a realist conception of theory.

Within the national security field, theory serves as both the realist and instrumentalist roles. When tasked with providing the macro view of the world necessary for determining the relative importance of geopolitical elements, theory provides a picture or map of the world, showing the interconnections between the various units within the international system (the realist conception of theory). On the other hand, when theory serves as a tool for guiding decisions and providing direction during problematic situations, such as an emerging military crisis or the distribution of scarce national resources, it is functioning in its instrumentalist role. At its most fundamental level, the importance of theory is that the insights it provides offer national security professionals a means of organizing and developing an integrated yet flexible approach to national security issues; theory is a tool for guiding actions, not a creed by which to live.[10]

---

[9] Scientific study is commonly broken down into two branches, hard and soft. The basis for this differentiation is the perception that some fields require the use of more rigorous scientific methods than others do. Hard sciences generally focus on the creation and analysis of quantifiable data through the strict application of scientific methods to prove and disprove specific research hypotheses. The heart and soul of hard scientific research is the conduct of reproducible experiments under strictly controlled conditions. Soft sciences, on the other hand, while still using hypothesis, commonly rely more on qualitative analysis and interpretation to arrive at guiding principles. Soft sciences may or may not have an experimental basis, and the interpretation of results is open to debate, especially when basing conclusions on information gathered under unique, uncontrolled, and non-replicable conditions.

[10] J. J. Thompson, *Tendencies of Recent Investigations in the Field of Physics* (London, UK: British Broadcasting Corp, 1930), 23. Although he is discussing the field of physics, Thompson writes that theory is "a tool and not a creed." The concept of theory guiding, not dictating, research and policy development is consistent with my use of it here.

Carl von Clausewitz alludes to the requirement for flexibility in his famous work *On War*, where in Chapter 2 he takes issue with the efforts of some theorists to reduce warfare and theory to a calculated science.[11] For Clausewitz, it is neither useful nor possible to construct a theoretical model based on rules and mathematical calculations to serve as a guide for national security decision making. In his opinion, theories based on physical and quantifiable values are useless because they fail to take into account variable quantities and the effect of psychological forces.[12] As a result, the use of theory in a purely instrumentalist manner breaks down when faced with the problems of implementation in the infinite complexity of the real world. Instead of creating a list of quantifiable factors for comparison, theory in the national security context serves as a guide for action, a means for becoming familiar with the subject matter through the development of deeper understanding.[13] It educates the minds of the analyst, policy maker, and strategist, creating a framework upon which to hang information instead of

[11] Clausewitz, *On War*, 134 - 47. Book Two of *On War*, titled "On the Theory of War," as is Chapter Two within it. In the first few pages of this chapter, he reviews the role that increasing complexity of conflict played in the need to create theory of warfare to bring order to reflections and musings based on historical experience.

[12] Ibid., 136, 40. In his development of theory, Clausewitz argues for a descriptive approach to theory development as opposed to the descriptive approach favored by many of the other writers of his time. In addressing this subject in his own work, Harold Winton describes Clausewitz's motivation as being "fed up with theories that excluded moral factors and genius from war." He goes on to contrast the descriptive and proscriptive approaches to military theory by contrasting the works of Clausewitz and Jomini. Winton ultimately determines that the two approaches are polar opposites in suggesting how theory should influence practice: The Clausewitzian view suggests "indirectly by educating the judgment of the practitioner; in the Jominian view, it does so directly by providing the practitioner concrete guides to action." Winton, "On the Nature of Military Theory," 22-27.

[13] Clausewitz creates a list of what he calls positive conclusions some theorists of his day attempted to create as the basis for a scientific approach to war. He takes issue with discussions limited solely to material factors, such as numerical superiority, supply, logistics, and interior lines of communications. Clausewitz, *On War*, 134-36.

guiding actions and reactions.[14] Admiral J. C. Wylie, United States Navy, arrives at a similar conclusion, writing, "Theory serves a useful purpose to the extent that it can collect and organize the experiences and ideas of other men, sort out which of them may have a valid transfer value to a new and different situation, and help the practitioner to enlarge his vision in an orderly, manageable and useful fashion – and then apply it to the reality with which he is faced."[15]

Theory then, in a national security context, is the art of relating desired ends to the means at hand, regardless of the domain of interest.[16] The value of theory is that it provides the national security establishment a means of discovering a way forward. It provides a common understanding and touchstone to guide policy makers, academics, and practitioners alike toward the discovery of hidden interactions, interrelationships, and facts. Once recognized, theory provides a means of organizing and connecting these newly discovered interactions, interrelations, and facts to established ones and serves as a means for evaluating their interlocking relationships. It is the theoretical backdrop to research that makes the effort of analysis and discovery worthwhile.[17]

Pre-theory and Military Theory in the Cyber Domain

Having reviewed the role of theory in general, we now move to a discussion of cyberpower theory development and continue to expand upon the role military domain

---

[14] Ibid., 141. Here I continue to use Clausewitz to point out that theory used in the fields of national security and military operations takes the form of guiding, not prescribing, action. It provides a tool for decision makers to frame information by keeping the desired end state in mind. As Clausewitz puts it, "Theory exists so that one need[s] not start afresh each time sorting out the material and plowing through it, but will find it ready to hand and in good order."
[15] J. C. Wylie, *Military Strategy: A General Theory of Power Control* (New Brunswick, N.J.,: Rutgers University Press, 1967), 35.
[16] Clausewitz, *On War*, 142.
[17] Kaplan, *The Conduct of Inquiry; Methodology for Behavioral Science*, 309.

theories play in development of national security strategy. As a starting point, the reader should recognize that cyberspace domain development and scholarship is in what James Rosenau described as a pre-theory stage. According to Rosenau, during the development of a field of study, in this case the cyber domain, creating frameworks helps explain various ends, means, capabilities, and sources of policy and advancement that occur.[18] Often isolated and addressing unique facets of a domain or explaining the interaction and relationship between specific actors, these concepts are islands of scholarship that are evolving and growing, or withering and dying, on their own merits and occasionally fed by the attention they capture in the greater community of scholars.

During the pre-theory phase of domain development, a scheme to link these isolated frameworks together is missing. Maturation of the domain is literally the process of building connections between related ideas, observations, and insights. Creation of bridges between these islands of understanding is the process of creating a theoretical framework. This linking also allows ideas, observations, and insights to interact and be assessed as parts of a larger community bringing greater clarity to the field. Over time, the accumulation of linkages facilitates the development of a comprehensive theory, gradually elevating scholarship within the domain out of the pre-theory stage.

According to Rosenau, during the theory development process, it is necessary to endure this messy, often disjointed process of developing pre-theory frameworks before a general domain theory takes shape.[19] The process of building this framework serves to categorize data into recognizable bins and organize observations and insights. In a

---

[18] James N. Rosenau, *The Scientific Study of Foreign Policy*, Rev. and enl. ed. (London: New York: F. Pinter; Nichols., 1980), 119. Adapted from an explanation of theory development in Chapter Six, "Pre-Theories and Theories of Foreign Policy," 115-169.
[19] Steve Smith, "Review: Rosenau's Contribution," *Review of International Studies* 9, no. 2 (1983): 139.

mutually reinforcing manner, as the categorization of data becomes more widely accepted, the emerging pre-theory constructs serve as rallying points for further research, gaining even wider acceptance. This process leads to the creation of shared intellectual constructs and the standardization of terms and explanations within the field.[20] Eventually this incremental accumulation of knowledge allows the debate of competing constructs (or pre-theories), sharpening and improving them through the crucible of peer review. Over time, in a matured domain environment, as competing pre-theories merge or fall out of favor, a general theory of the domain emerges.

With regard to the cyber domain, the process of emergence and acceptance over how to organize and understand the national security implications of technology development has been ongoing for more than a decade.[21] In addition to discussions of intergovernmental roles and responsibilities, arguments over the nature of the domain have focused on such fundamental aspects as the inclusion of physical and nonphysical features and whether the domain consists of all electromagnetic transmissions or simply those occurring within the global information grid. At the most basic level, there are some researchers and observers who question whether cyberspace is itself a separate

[20] The Government Accountability Office (GAO) recognizes the requirement for standardizing terms in the emerging cyber domain within its recommendations to the Armed Services Committee. Committee on Armed Services U.S. Congress (House of Representatives), Subcommittee on Emerging Threats and Capabiliites, "Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates," ed. Government Accountability Office (Washington, DC: United States Government Accountability Office, 2011), 6.

[21] Although perhaps not the first cyber strategy document, in 1998, PDD-63 discussed critical infrastructure protection, lumping cyber-based systems in with other physical critical infrastructure. It arguably marks the formal beginning of the cyber domain debate at the national security level by assigning roles and responsibilities to government agencies. U.S. President, "Presidential Decision Directive 63: Protecting America's Critical Infrastructures," (Washington, DC: White House, 1998). The lack of comprehensive understanding about the difficulty of dominating the cyber domain is apparent in the national goal, Section 3, which explicitly set a target date for acquiring the ability to protect the nation's critical cyber infrastructure by 22 May 2003, a goal we have yet to achieve today.

domain, existing as a subset of the larger information environment, or simply one aspect of manipulating the electromagnetic spectrum.[22] This debate, while instructive, is in the process of being overcome by events. As pointed out in Chapter 1, the DOD and other major national security agencies have designated cyber as a domain.

From a national security perspective, there are significant advantages to designating cyberspace a separate military operating domain.[23] These advantages all flow from the fact that national security infrastructure is based on the division and distribution of responsibilities, manpower, and budgets to organizations with domain-based identities. For example, the current DOD organization into secretariats for the land, sea, and air (Department of the Army, Department of the Navy, and Department of the Air Force) is an example of this domain-based nature. Each of these departments receives budgets and manpower primarily based on its roles and responsibilities relating to one focal domain. While it is true that each of the military services associated with these secretariats contains elements transcending or cumulating in other domains, the Department of the Navy's Marine Corps being the most obvious example, it is the primary domain responsibility designation that drives planning and discussion as well as organizational identity.

The bureaucratic process of identifying how and why government entities are involved in a domain, or why sub-elements of these organizations participate in crossing domain borders, provides a common framework for discussing the assignment of functional responsibilities and the merits of expending limited national resources in pursuit of vital interests. These domain designations similarly form the basis for the

[22] A review of this debate appears in Chapter Three, where identification of the cyber domain's physical properties takes place.
[23] A discussion of the term *domain* for purposes of this research project occurs in Chapter Three.

organization of non-military governmental departments, such as the Federal Aviation Administration, the Federal Communications Administration, the Department of Homeland Security, and the Department of Health and Human Services, to name a few. From a geopolitical standpoint, standardized domain designations form the basis for negotiating international treaties and identifying international custom and norms. Government agencies with similar, adjacent, or overlapping domain responsibilities are able to coordinate actions and assess each other's capabilities based upon a shared set of perceptions. In short, the designation of domains facilitates the organization of efforts to bring order to both the physical world and the governments overseeing modern society.

More than a decade into the cyber debate, the growing recognition that cyberspace is its own operating domain, subject to competition by nation-states, has gained enough traction that governments and militaries are opening dialogues both domestically and internationally. At the heart of this discussion are concerns over control and ensured access to cyberspace and the effect the loss of access would have on a nation's future. As previously mentioned, the United States is developing strategies for military and whole-of-government organization regarding cyberspace, as is true for many if not most nations. States, however, are not the only global players making these efforts; world bodies such as NATO and the United Nations, who are also working to define their cyber interests, roles, and responsibilities, join them.[24]

NATO, for instance, has published and updated policies that seek to coordinate and standardize approaches to cyber defense across its organizational members.[25] Beyond publications, in order to develop and operationalize these efforts through research and

[24] NATO is the common acronym for the North Atlantic Treaty Organization.
[25] "Defending the Networks: The NATO Policy on Cyber Defence," ed. NATO Public Diplomacy Division (Brussels, BE: North AtlanticTreaty Organization, 2011).

education, NATO has created a Cooperative Cyber Defense Center of Excellence, located in Tallinn, Estonia.[26] At the global level, the United Nations International Telecommunications Union has added cyber coordination to the role it plays in creating standards and improving access to globally networked communications and commerce.[27] These sorts of actions are part of the domain's maturation process, and they are beginning to include importing familiar terminology and strategic concepts from extant domains, terminology such as physical geography, chokepoints, and the advantages of offensive and defensive postures within the cyber domain.

> "A central feature of the cyber revolution is that no one agrees on the terminology. There's the language of the military and the language of the geeks, and a wide variety of interpretations in between. The place to start any global discussion on cyber-security is therefore to agree common definitions, but so far this hasn't happened."[28]

From a domain development perspective, this growing involvement of international organizations and governments in the debate and the associated increasing attention directed toward cyberspace acts as a forcing function for the standardization of terminology and concepts of operation. In these actions, we find examples of the efforts necessary to build legal and international norms. Building these norms is a vital step toward creation of the pre-theory frameworks discussed above because they make further development of the field possible.

The continual refinement and abandonment of organizational constructs in the domain development process is a commonly recognized methodology for improvement. The understanding that scientific advancement occurs through successive replacement of

[26] The NATO Cooperative Cyber Defense Center of Excellence website is regularly updated with publications and cyber-related events. See http://www.ccdcoe.org/.
[27] Find the International Telecommunications Union website at http://www.itu.int.
[28] Grauman, "Cyber-Security: The Vexed Question of Global Rules," 6.

old theories and ideas by newer and better ones is common to all sciences. The direction these advances take and the standards they set for further development depend greatly on the way new theories take into account the achievements of preceding theory and build upon it.[29]

In his work, seminal modern methodologist Imre Lakatos describes the advancement of science as the replacement of old ideas, proven inadequate or unable to explain the phenomena in question, with new ones.[30] The theory development process follows this model. As theorists propose relationships between factors of interest and provide supporting evidence for their proposals, peers evaluate these relationships, refining or rejecting them.

One example of how this process is playing out in the cyber theory development process is the debate over analogies and metaphors used to describe cyberspace interactions. As new analogies and metaphors are used, practical experiments and analysis of real-world events test their validity; theorists in the field confront inaccuracies and grapple with inconsistencies, abandoning those ideas and comparisons they find less than satisfactory. While some cyber professionals favor military analogies such as Pearl Harbor or a crippling sudden nuclear attack, others advocate perspectives based on legal and social frameworks, such as the Wild West. Some theorists even place emphasis on the cyber domain's similarity to natural environments that leads them toward the use of

---

[29] Kaplan, *The Conduct of Inquiry; Methodology for Behavioral Science*, 304.

[30] Imre Lakatos, "Falsification and the Methodology of Scientific Research Programmess," in *Criticism and the Growth of Knowledge*, ed. Imre Lakatos and Alan Musgrave (Cambridge Eng.: Cambridge University Press, 1970). As problems with extant theory are identified, researchers suggesting possible means of overcoming these difficulties will undoubtedly take a variety of possible paths, each subject to assessment by peers who then refine and validate each new theoretical advancement in the field.

security approaches based on controlling the spread of disease and other contagions.[31] This progression of adaptation and refinement is the basis of the theory building process.

Building cyber theory

Starting the process of building a cyber theory requires establishing an initial framework to serve as a point of departure. Potentially leveraging extant theory as a source of this framework may not only provide guidance out of the pre-theory stage, it may also help integrate cyberpower theory with extant domain theories as a basis for guiding national security planning.

In order to begin this task, theorists must create an outline of what a cyber theory should look like. One way of identifying and selecting elements to include in the construction of this framework is to assess existing domain theories and pull from them structural elements that can serve as a basis upon which to build. This effort is the focus of my research project: to analyze the relationships between elements of analysis derived from existing domain theory in order to determine how well they serve as predictors of phenomena in the cyber domain.

Perhaps the best assessment of the theory building process and its intended outcome comes from political scientist David J. Singer. Singer states that the intent of theory building is to create "a highly accurate *description* of the phenomena under consideration – a capacity to *explain* the relationships among the phenomena under

[31] For an interesting and short discussion of analogies commonly applied to the cyber domain, see Kandice McKee, "A Review of Frequently Used Cyber Analogies," (Smithfield, VA: National Security Cyberspace Institute, 2011). In this discussion, she touches on the air, sea, and space analogies for the physical domains and addresses analogies to the lawlessness and wide-open nature of the Wild West, the application of deterrence in a Cold War manner, and the use of public health analogies.

investigation … [and] offer the promise of reliable *prediction*."[32] Singer's observation neatly ties the process of theory building in with the purpose of theory introduced above by Wilie, Clausewitz, and Lakatos, amongst others.

Assuming that Lakatos and others are correct that the theory building process is one of continuous growth and refinement, then in reality this process is never complete. It is an ongoing process that seeks to define a unique position within the overall national security strategy discussion and provide guidance for the formulation of policy. The challenge is to define what purpose a cyberpower theory will serve in placing the cyber domain within the context of greater national security efforts.

The military historian Harold Winton posits that a military theory must accomplish five tasks.[33] According to Winton, a military theory must:

1. Define the field of study.
2. Categorize the field of study into its constituent parts.
3. Provide an explanation for the elements in these categories.
4. Connect the field of study to other relevant fields.
5. Anticipate key trends and changes to facilitate policy development.

Taking a brief look at how these five tasks relate to the cyber domain provides an outline of what a fully developed valid cyber theory will both look like and do.[34]

---

[32] J. David Singer, "The Level-of-Analysis Problem in International Relations," *World Politics* 14, no. 1 (1961): 78-79. Italics in original.

[33] Harold R. Winton, "An Imperfect Jewel: Military Theory and the Military Profession," in *Society for Military History Annual Meeting* (Bethesda, MD 2004). Although not specifically presented as a laundry list, the tasks appear on pages 3-5. These same tasks are laid out by Winton again in ———, "On the Nature of Military Theory," 20-21.

[34] John Sheldon takes up the task of discussing how Winton's five tasks should be addressed regarding the cyber domain in his article: Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 108-9. Here I use Sheldon's effort as a basis for my review of the way in which these five tasks may be applied to cyber. Sheldon also identifies an incomplete attempt by Stuart Starr to address Winton's five tasks in his work: Stuart H. Starr, "Toward a Prelimary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009).

Define the field of study: A cyber theory must define cyberspace as a military domain, including 1) what constitutes the domain from a physical and conceptual standpoint and 2) what cyberpower means – clearly differentiating the development of cyber domain capabilities from those of other military domains.[35]

Categorize the field of study into its constituent parts: To accomplish this, a theory of the cyber domain must break the field down into its constituent parts, making them accessible for analysis as pieces of a larger whole. The advantage of this is that these individual pieces can then be taken apart, examined, and then put back together in a manner that allows others to understand their relationship to each other and place them into the context of the overall domain.[36] In order to do this, a cyber theory must identify the parts that constitute cyberspace and also the use of cyberpower to generate strategic effects. Differentiations such as planning vs. operations, offensive vs. defensive use of cyberpower, strategic vs. tactical uses of the domain, etc., are examples of ways with which the constituent parts of overall cyber theory must be addressed and categorized.

Provide an explanation for the elements in the categories: Cyber domain theory must explain how cyberpower achieves the desired effects (such as destruction,

---

[35] Winton characterizes this task as drawing a circle around the defined domain and declaring that "everything inside the circle is encompassed by the theory, while everything outside it is not." As an example, he uses Clausewitz's theory of war, within which Clausewitz "offers two definitions. The first states baldly, 'War is thus an act of force to compel our enemy to do our will.' After introducing the limiting factor of rationality into the consideration of what war is, Clausewitz expands this definition as follows: 'War is not a mere act of policy but a true political instrument, a continuation of political activity with other means.' A synthesis of these two definitions would be that war is the use of force to achieve the ends of policy. Although the utility of this definition has been argued at some length, it leaves no doubt as to what Clausewitz's theory is about." Winton, "On the Nature of Military Theory," 20.

[36] In this case, Winton recommends a citrus fruit divided into sections and put back together. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 109. In addition to the citrus metaphor, Winton suggests the use of any spherical object divisible along may internal lines (vertically, laterally, horizontally). Winton, "On the Nature of Military Theory," 20.

disruption, denial, and deception) within the strategic environment and identify the circumstances within which it can be effectively used.[37]

Connect the field of study to other relevant fields: A fully formed theory must also connect the cyber domain to the wider military and national strategy. In order to do this, cyberpower theory must identify the ways and means through which it interacts with other domains and other avenues for exerting national power. The key contribution here is that it places the domain within the greater strategic context, identifying critical if not vital areas of interaction.[38]

Anticipate key trends and changes to facilitate policy development: Cyber domain theory should also "identify those aspects of cyberpower that are likely to be timeless long after society and technology change."[39] Winton's use of the word *anticipate*

---

[37] Winton has used as an example Alfred Mahan's description of seapower. Winton writes, "Alfred Thayer Mahan's statement that the sea is 'a wide common, over which men may pass in all directions, but on which some well-worn paths show that controlling reasons have led them to choose certain lines of travel rather than others' explains the underlying logic of what are today called sea lines of communication. Reading further in Mahan, one finds an extended explanation of the factors influencing the seapower of a state. Explanation may be the product of repetitive observation and imaginative analysis, as Copernicus' was, or of 'intuition, supported by being sympathetically in touch with experience,' as Einstein's was. In either case, theory without explanatory value is like salt without savor – it is worthy only of the dung heap." ———, "On the Nature of Military Theory," 21.

[38] In describing the task of connection, Winton returns to the use of Clausewitz's definition of war: "War is not a mere act of policy but a true political instrument, a continuation of political activity with other means" to provide an example. Winton says, "Although war had been used as a violent tool of political institutions dating to before the Peloponnesian War, Clausewitz's elegant formulation, which definitively connected violence with political intercourse, was perhaps his most important and enduring contribution to the theory of war." ibid.

[39] See Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 109. To expand upon this point, borrowing again from Winton, the choice of the verb *anticipation* is deliberate. "In the physical realm, theory predicts. Isaac Newton's theory of gravitation and Kepler's laws of planetary motion, combined with detailed observations of perturbations in the orbit of Uranus and systematic hypothesis testing, allowed Urbain Jean Joseph Le Verrier and John Couch Adams independently to predict the location of Neptune in 1845. However, action and reaction in the human arena, and therefore in the study of war, are much less certain, and we must be content to live with a lesser standard. Nevertheless, anticipation can be almost as important as prediction. In the mid-1930s, Mikhail Tukhachevskii and a coterie of like-minded Soviet officers discovered that they had the technological capacity 'not only to exercise pressure directly on the enemy's

is important here. Within the context of domain development, rapid changes in the technologies used within the cyber domain and the infinite numbers of ways to apply technologies make any efforts of prediction practically impossible.[40] Instead of prediction, it is more appropriate to speak of anticipating major changes in the importance of strategic principles, such as the central control of operations, the importance of security versus utility, and the use of deterrent means from outside domains. Unlike in a hard science such as astronomy, where efforts to confirm the existence of celestial bodies is based on predictions from observing gravitational anomalies, no well-defined rules of cyber analysis exist to guide advancement in the field. The national security field deals with nothing as concrete as gravitational constants or Newton's laws of motion.

Clearly, defining the field of cyberspace studies and connecting it to other domains and to national security strategy in general is a challenge for academics and practitioners alike. The rate at which technology-driven changes in cyber capability have altered almost every aspect of national security and are altering the geopolitical distribution of power has provided little chance for full assessment of what the field of study entails. As a result, there is little guidance available for policy development. We are

---

front line, but to penetrate his dispositions and to attack him simultaneously over the whole depth of his tactical layout.' They lacked both the means and the knowledge that would allow them to extend this 'deep battle' capability to the level of 'deep operations,' where the problems of coordination on a large scale would become infinitely more complex. But the underlying conceptual construct – that is, what was practically feasible on a small level was theoretically achievable on a much larger scale – was a powerful notion that has only recently been fully realized in the performance of the US Armed Forces in the Gulf Wars of 1991 and 2003" Winton, "On the Nature of Military Theory," 21.

[40] A prediction is an anticipated outcome from reasoned inference based on collected information. Kaplan, *The Conduct of Inquiry; Methodology for Behavioral Science*, 350. This is as opposed to anticipation, which grounds itself in the understanding and explanation of phenomena that utilizes insight into the relationships within a system to foresee the direction in which events will unfold. Unlike predictions, confirmable through further testing, confirmation of successful anticipation takes place by actual occurrence of events.

at the initial stages of explaining and defining the field, a necessary task before creating a cyber theory that can fully explain the domain and anticipate future developments. Even in a mature form, cyberpower theory will have limitations.

In the domain power context, no theory can account for all aspects of the environment and actors that make up the strategic landscape. Theory is by necessity designed to apply to a simplified version of the real world and cannot account for the rapid nature of change within the environment; it has no hope of providing prescriptive solutions to strategists and policy makers seeking to create cyberpower and develop a cyber-faring nation.[41] Theory can only provide an understanding of how the domain is expected to develop and react in a given situations.

Methodology

The analysis performed in the following chapters uses a combination of approaches in an effort to evaluate the suitability of existing domain theory to serve as the basis for development of cyber theory; it applies a two-step process. First, the research uses deductive reasoning to develop elements of analysis from existing theory, identifying the guiding characteristics of each theory of interest and then determining how the nature of the domain in question influences the theory development process. Second, using the common characteristics developed in step one and applying them to the cyber environment, the use of inductive reasoning creates guidance for further cyber theory development. Once complete, this dual-natured deductive-inductive process provides a solid basis for understanding how the nature of the cyber domain influences

[41] Winton, "On the Nature of Military Theory," 22. In his discussion of this subject, Winton himself borrows from Michael Howard when he opines that it is a theorist's task to make theory as "little wrong as possible."

theory development and gives insight into the guiding principles around which further cyber theory development will take place.

Extant Theory Analysis

Although he recognizes that "there is no generally accepted recipe for making theories," the researcher and methodologist Stephen Van Evera recognizes nine aids to theory development.[42] Of the nine he discusses, two are particularly suited to this study. First, he identifies the use of the comparative method, derived from John Stuart Mill's "methods of difference" and "methods of agreement" as an aid to inductive theory making.[43] This method, directly comparing existing theories, comes into play during the first phase of the analysis process.

The process itself is not difficult, comparing two different subjects of analysis to determine how they match up. In this case, the subjects of comparison are five extant domain power theories. The purpose of comparing these theories to one another is to identify both their differences and similarities, not to rank or

> "A study of the past shows what has worked and what has failed, but no two events are ever quite the same. Historical analogies do not create axioms but, more valuably, suggest the questions that need to be considered and the range of considerations that pertain."[44]

[42] Stephen Van Evera, *Guide to Methods for Students of Political Science* (Ithaca: Cornell University Press, 1997), 21.
[43] Ibid., 23. Mill discusses the process of comparing cases as a method of inquiry in order to determine areas of agreement and infer causation extensively beginning on page 450 of John Stuart Mill, "A System of Logic, Ratiocinative and Inductive: Being a Connected View of the Principles of Evidence, and Methods of Scientific Investigation." (London, UK: John W. Parker, 1843), http://books.google.com/books?vid=HARVARD:AH6PQC&printsec=titlepage#v=onepage&q&f=false.
[44] John B. Hattendorf, "The Uses of Maritime History in and for the Navy," *Naval War College Review* Spring, no. 56 (2003): 26.

criticize them in comparison to each other. The goal is to understand which aspects of these theories are important to making them the seminal theories of their domains. Areas of congruence between the theories revealed by this comparison process serve as guides, pointing us toward a promising area for further cyber research and development. The assumption here is that aspects of domain theory that appear consistently across other domains are likely to be useful in building a framework for creation of cyberspace theory.

Areas of polar differentiation between the theories are also of great interest because they may indicate outlying considerations that may or may not also apply to the emerging cyber environment. If the analysis below identifies that one theorist uses a fundamentally different concept in theory development, the follow-up analysis will have to identify what aspects of the physical domain or domain development process drove that theorist's thinking. Of particular interest will be the identification of areas of congruence in theories dealing with one particular domain that are absent or distinctly different from theories addressing another domain. If identified, exploration of such a domain-based differentiation will examine what drives the resultant theory.

The second of Van Evera's aids to theory development used in this project is the application of theory to a new domain. In Van Evera's words: "We can fashion theories by importing existing theories from one domain and adapting them to explain phenomena in another."[45] Leveraging the understanding of individual theories developed in step one, the analysis below also seeks to determine how well the areas of agreement and differentiation travel into the cyber domain. This inductive process validates or invalidates the identified areas of interests from extant theory as conceptual guides providing direction and insight into areas where we should focus inquiry in the new

[45] Van Evera, *Guide to Methods for Students of Political Science*, 27.

domain.[46] The use of induction in this case creates points of comparison for further discovery, not for the comparison of specific hypotheses regarding the nature of the cyber domain.[47] These points of comparison, once validated, can act as a starting point for the development of principles for cyberpower theory. They are also a means of satisfying Winton's fourth task for military theory because they identify interconnections with the other domains and aspects of national power.

The use of these two comparative processes to establish a theoretical basis for development of emerging military theory is not in itself new. In his work on spacepower development, Winton discusses the value of beginning with extant theory and the analysis of historical experience. He proclaims them rich sources of information when designing a theoretical framework for new and emerging military domains.[48] Much of the value gained by using extant theory and historical events comes from leveraging preexisting understandings and points of reference as a method to begin the intellectual process.

To provide examples, the naval theorist Julian Corbett discusses his theoretical principles for naval power through occasional references to Clausewitz and Jomini, among others from the land domain, to help make his points.[49] Keeping with the maritime theme, A.T. Mahan begins his work with an assertion that the study of history is useful

---

[46] Barney G. Glaser, *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory* (Mill Valley, Calif.: Sociology Press, 1978), 37.
[47] Ibid., 38.
[48] Winton, "On the Nature of Military Theory," 22.
[49] Sir Julian Stafford Corbett, *Some Principles of Maritime Strategy*, Classics of Sea Power (Annapolis, MD: Naval Institute Press, 1988). Although references to terms and concepts from landpower theory are used in numerous places through the book, an example for making my point is Chapter Four, beginning on page 52, entitled "Limited War and Maritime Empires: Clausewitz's and Jomini's Theory of a Limited Territorial Object, and Its Application to Modern Imperial Conditions."

because it helps illustrate universally applicable principles of war.[50] In the works of both these maritime power authors, they are leveraging established history and a preexisting theoretical understanding from well-understood extant domains in order to more clearly illustrate concepts they introduce in their own work. This technique is important because it provides a frame of reference for seeking to understand an aspect of the new domain by overcoming that domain's lack of self-illuminating history and theory.

What Winton is suggesting and what Mahan, Corbett, and others have done is in harmony with Van Evera's theory development process: the use of direct comparison and the importation of theory into new domains. In the works of both Mahan and Corbett, it is clear that development of a deep understanding of extant domain theory aided their efforts. Animating this understanding with historical data allowed them to make comparisons between existing and emerging theoretical constructs. When the comparative process between domains is underwritten by an understanding of how the developing domain and its emergent theory relate to a general conceptual framework of war, it provides a solid foundation for the development of new theory beyond that which arbitrary choice, pure, chance, or blind intuition on the part of any individual theorist would allow.[51]

---

[50] Alfred Thayer Mahan, *The Influence of Sea Power Upon History, 1660-1783* (New York, NY: Dover Publications, 1987). See his introduction, pages 1-24, entitled "Influence of Sea power Upon History."

[51] Modified from John J. Klein, "Corbett in Orbit: A Maritime Model for Strategic Space Theory," *Naval War College Review* 57, no. 1 (2004): 2. Here Klein is in turn referencing Hattendorf, "The Uses of Maritime History in and for the Navy," 27.

Analytical Steps

Step one: analysis of extant domain theory

The first challenge in leveraging extant domain theory as a source for cyber theory development is selection of the domains and theorists for analysis. The following chapter, Chapter 3, discusses the reasoning used to narrow this projects focus down to the maritime and air domains, and the selection of particular theorists in general. Having discussed the reasoning for using maritime and air theorists as the source of extant theory, beginning in Chapter 4 with the maritime theories, continuing in Chapter 5 with a review of aviation theory, and concluding in Chapter 6 with the comparison of derived elements, a total of five extant domain theories are examined using the inductive process introduced above. The domain theories subjected to this analysis are those written by A. T. Mahan, Julian Corbett, Giulio Douhet, Billy Mitchell, and Alexander de Seversky.[52]

The process of evaluating each theory begins with a brief review of the theory and the historical context surrounding its creation. Following the review of each theory, this study identifies areas of emphasis and important considerations from within the theory for use as elements of analysis and points of comparison across the five theories. Repeated for all five authors, across both domains, this process creates a database of relevant concepts for comparison in Chapter 6. To facilitate comparison of derived elements between theories, each appears in a table similar to the one below.

[52] The specific works in question are Mahan, *The Influence of Sea Power Upon History, 1660-1783*, Corbett, *Some Principles of Maritime Strategy*, Giulio Douhet, *The Command of the Air*, World Affairs: national and international viewpoints (North Stratford NH: Ayer Company Publishers, Inc, 1942; reprint, 1999), William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military* (New York, NY: Dover, 1988), Alexander P. De Seversky, *Victory Through Air Power* (New York, NY: Simon and Schuster, 1942).

Table 1: Sample Elements of Analysis Depiction

Elements of Analysis	Douhet	Mitchell	Seversky
Element #1			
Element #2			
Element #3			
Element #4			
Element #X			

In Chapter 6, identification of similar elements across all five theorists and within each of the two domains takes place. Simultaneously, identification and analysis of factors unique to each domain or to an individual theory takes place.

As introduced previously, this comparative process uses a variation of John Stuart Mill's "method of difference" and "method of agreement."[54] Areas of agreement between theories are combined to create common elements of analysis. Outlying elements and areas of disagreement receive additional analysis for inclusion in the list of elements for comparison to the cyber domain.

> "But while it is wise to observe things that are alike, it is also wise to look for things that differ; for when the imagination is carried away by the detection of points of resemblance – one of the most pleasing of mental pursuits – it is apt to be impatient of any divergence in its new-found parallels, and so may overlook or refuse to recognize such."[53]

The outcome of this first step in the research process is the development of unique elements of analysis that are valid outside of their particular domain and potentially useful in assessment of the cyber domain. These elements, developed through cross-domain and cross-theory analysis, become *Elements of Domain Power* for use in creating domain theory.

[53] Mahan, *The Influence of Sea Power Upon History, 1660-1783*, 2-3.
[54] Mill, "A System of Logic, Ratiocinative and Inductive: Being a Connected View of the Principles of Evidence, and Methods of Scientific Investigation."

Step two: cyber domain analysis

Once developed in Chapter 6, the elements of analysis become the basis for deductive analysis of the cyber domain in Chapter 7. The purpose of this step is to identify not only what cyber has in common with the other physical domains, but also to identify the differences that present challenges to theory development. During this second stage, evaluation of how well each element identified in Chapter 6 matches with the cyber domain's unique characteristics takes place.[55] This process evaluates each element's suitability for travelling into the cyber domain and provides insight into the domain's future development.

> "Theory should cast a steady light on all phenomena so that we can more easily recognize and eliminate the weeds that always spring from ignorance, it should show how one thing is related to another, and keep the important and unimportant separate. If concepts combine of their own accord to form that nucleus of truth we call a principle, if they spontaneously compose a pattern that becomes a rule, it is the task of the theorist to make this clear."[56]

After identifying how the elements apply to the cyber domain, the final step of analysis is a discussion of how extant theories apply as guides for the development of cyber theory. The identification of relevant elements from extant domain theory is particularly useful to the creation of cyberspace strategy; they provide theorists a point of departure from which to begin.

Having laid out the roll of theory and the evaluation process, the following chapter discusses the selection of the maritime and air domains for comparison to the

[55] Glaser, *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*, 46.
[56] Clausewitz, *On War*, 578.

cyber domain. It also provides the operational definition of the cyber domain used in the follow-on analysis.

Chapter 3: Research Parameters

The previous chapters have identified the growing importance of the cyber domain as an element of national security and discussed the role domain theory development will play in organizing and developing cyberpower. This chapter sets the stage for evaluating extant theory using the analytical methodology laid out in the previous chapter. It begins by briefly outlining the process of defining the cyber domain as a physical environment, a process that clearly followed the pre-theory growth stage of domain development. The chapter then presents the rational for narrowing the scope of this research project to the maritime and air domains.

Cyber Is a Physical Domain

The Merriam-Webster online dictionary provides ten different definitions for the term *domain*.[1] All ten of these definitions have as their common purpose the delineation of a defined area of influence or interest. Three of these ten definitions have particular relevance to the discussion here:

1. A region distinctively marked by some distinctive feature.
2. A sphere of knowledge, influence, or activity.
3. A territory over which dominion is exercised.

[1] The online Merriam-Webster dictionary provides ten definitions for domain. The three displayed here are #2, 3, and 4. For illustrative purposes, I have changed the order of their presentation above to be 4, 2, and 3. The other seven definitions focus on legal ownership; the study of mathematics, biology, and physics; and the subdivision of the Internet into common Internet address groupings such as .com, .gov, .edu: Dictionary, "Domain, n." The DOD dictionary of terms does not define the term *domain*: Joint Chiefs of Staff U.S. Department of Defense, "Department of Defense Dictionary of Military Associated Terms Joint Publication 1-02," Joint Publication (Wahington DC: Government Printing Office, 2010, as amended throught 15 October 2011).

Taken together, these three definitions provide a basis for understand how the designation of cyberspace as a domain advances the national security process.

First, the process of designating cyberspace as a domain clearly identifies its boundaries, providing a defined area of responsibility. This helps to organize and define relationships between national security agencies involved in cyber development, defense, and regulation, a subject touched upon briefly in the previous chapter. Second, this designation identifies a field of study or debate for further planning and refinement by experts in the field. In this case, the field of interest is national security strategy and narrows down to the sub-field of cyber domain systems' organization, personnel development, and overall integration into national security strategy.[2] Finally, designation of a domain delineates the borders – both physical and conceptual – from within which the exercise of cyberpower occurs and from which the effects of cyberpower originate.

Interestingly, the concept of what makes up a domain is not clearly defined in military literature, yet it forms the basis for our commonly understood core functions of the four DOD services.[3] A nation's division of military responsibility by physical properties is useful because it allows planners and strategists to organize operations in both time and space. Like the other military domains, cyberspace has physical

---

[2] James N. Miller, Dr., "Statement of Dr. James N. Miller Principal Deputy Under Secretary of Defense for Policy," in *Hearing on the Department of Defense in Cyberspace and U.S. Cyber Command,*, ed. U.S. Congress (House of Representatives) Committee on Armed Services Subcommittee on Emerging Threats and Capabiliites, U.S. Congress, (House of Representatives) (Washington, DC 2011), 3-4. In a prepared statement to the House Armed Services Committee, Dr. Miller states that the DOD treats cyberspace as a domain for organizing, training, equipping, and, when directed, operating in the same manner as the air, land, and space domains.

[3] The Army, Navy, Air Force, and Marines. These four services are overseen by three Service Secretaries: Secretary of the Army, Secretary of the Air Force, and the Secretary of the Navy, who oversees both the Navy and Marine Corps. This division by domain is a universal phenomenon among the developed nations. Even in forces without a specified air or naval force, these forces are separate elements of the larger force.

characteristics, and military planning and strategy benefits from this realization. Widespread recognition of the utility gained through the use of physical properties to define the cyber domain properly has emerged gradually as practitioners, policy makers, and academics have sought to bring order to the field; as we discuss next, a formal definition including these physical properties has been a long time in coming.

Defining cyberspace

William Gibson coined the term *cyberspace* in his 1982 science fiction short story "Burning Chrome" and popularized it in his 1984 novel *Neuromancer*. In these early works, the term described a sort of consensual hallucination, a depiction that appealed to many during the early days of computer networking because it invoked a realm in which existence is conceptual and fleeting.[4] Romantic as it is, Gibson's original concept bears little resemblance to the use of the word today.

In our modern lexicon, the term *cyberspace* describes not only the transient nature of information as it moves within the network but also the computer networks and storage locations themselves. It has become a generally accepted fact among scholars and practitioners that cyberspace includes the physical aspects of both individual computer systems and the global information grid. Despite this recognition and the term's widespread usage, there has been surprisingly little agreement on the definition of cyberspace.

Beginning in the 1990s, theorists, government agencies, and civilian organizations offered numerous formal definitions for cyberspace, none of which gained lasting or widespread acceptance. A look at each step along the term's evolutionary path offers

[4] Gibson, "Burning Chrome." And, ———, *Neuromancer*.

insights into the development of the domain from both an academic and policy standpoint. National Defense University professor and cyber scholar Daniel Kuehl provides a comprehensive review of these definitions in his contribution to *Cyberpower and National Security*, an overview of which is reproduced here as Figure 1 (below).[5] This brief summary of Kuehl's detailed review nicely illustrates that despite various levels of sophistication and inclusiveness, as the definition of cyberspace evolved, common themes within these definitions included electronics, telecommunications, infrastructure, and information systems, all of which are integral parts of a larger organized communications structure.[6]

[5] The list of previous definitions in Figure 1 is taken from the draft of Kuehl's contribution, which appears as Chapter 2 in the book: Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 26-27.
[6] Ibid., 25.

Figure 1: Definitions of Cyberspace

- Greece: *kybernetes*, "the steersman", ie. cybernetics, the study of control processes, which was the basis for Dr Tom Rona's concept (1976) of "information warfare"
- William Gibson, *Neuromancer* (1984): "a consensual hallucination";
- Edward Waltz, *Information Warfare: Principles and Operations* (1998), pgs 27, 150: The "Cyberspace dimension" refers to the middle layer—the information infrastructure—of the three realms of the information warfare battlespace. These three realms are the physical (facilities, nodes), the information infrastructure, and the perceptual.
- Google: "The electronic medium of computer networks, in which online communication takes place…. a metaphor for the non-physical terrain created by computer systems…. the impression of space and community formed by computers, computer networks, and their users…. the place where a telephone conversation appears to occur…the place between the phones."
- Winn Schwartau**,** *Information Warfare: Chaos on the Electronic Superhighway* (1994), pgs 49 & 327: "Cyberspace is that intangible place between computers where information momentarily exists on its route from one end of the global network to the other…. the ethereal reality, an infinity of electrons speeding down copper or glass fibers at the speed of light…. Cyberspace is borderless…. [but also] think of cyberspace as being divided into groups of local or regional cyberspace—hundreds and millions of smaller cyberspaces all over the world."
- Schwartau**,** *Information Warfare*, (2nd Edition, 1996), pgs 71 and 641-2: [national] "cyberspace are distinct entities, with clearly defined electronic borders…. Small-C cyberspaces consist of personal, corporate or organizational spaces…. Big-C cyberspace is the National Information Infrastructure….add [both] and then tie it all up with threads of connectivity and you have all of cyberspace."
- *Oxford English Dictionary (1997):* "The notional environment within which electronic communication occurs"
- Walter Gary Sharp, *CyberSpace and the Use of Force* (1999), pg 15: "Cyberspace….[it is the] environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the Internet and the World Wide Web."
- Dorothy Denning, *Information Warfare and Security* (1999), pg 22 "Cyberspace is the information space consisting of the sum total of all computer networks."
- Greg Rattray, *Strategic Warfare in Cyberspace* (2001), pgs 17 & 65: "a physical domain resulting from the creation of information systems and networks that enable electronic interactions to take place…. Cyberspace is a man-made environment for the creation, transmittal, and use of information in a variety of formats…. Cyberspace consists of electronically powered hardware, networks, operating systems and transmission standards."
- *Merriam-Webster Third New International Dictionary (2002):* "the on-line world of computer networks."
- *National Military Strategy for Cyberspace Operations* (2006): "Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked systems and physical infrastructures."
- *NSPD 54 (2008):* Cyberspace' means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."
- DepSecDef Gordon England *(*2008): "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

Although the first truly military definition on Kuehl's list does not appear until the *National Military Strategy for Cyberspace Operations* (2006), interest in the definition of cyberspace as a military term can trace its roots to early efforts at defining the information environment and network warfare beginning after the 1991 Gulf War. During the Gulf War the US's ability to gather, process, and use intelligence more quickly than the Iraqi army was seen as the primary cause of its stunning success against the world's third largest army.

Use of the term *information environment* began with efforts by the DOD's Command and Control Research Program to analyze the development of networked warfare and the effect of technology on the modern battlefield.[7] This program identified three distinct features of the information environment that act in concert with each other to collect, process, disseminate, and act on information: 1) individuals, 2) organizations, and 3) systems.[8] In the early formative stages of domain development, the composite environmental approach helped frame the thinking of national security strategists and gave both voice and visibility to the increasing role information plays at all levels of warfare.

These early efforts began the process of cataloging cyberspace as an environment made up of distinct yet integrated parts. Implicit in these efforts was the requirement for organizations using the environment to create personnel to serve as both users and

---

[7] The Command and Control Research Program is part of the DOD, located within the Office of the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer, and focuses on the National Security implications of the information age. Their website is: http://www.dodccrp.org.

[8] David S. Alberts et al., *Understanding Information Age Warfare*, CCRP publication series (Washington, DC: DOD, 2001), 10-14. In Chapter 2 of this publication, the authors identify three domains, physical, information, and cognitive, as well as human perception, which filters the way information is perceived and processed in the cognitive domain. These three realms are also reflected in Edward Waltz's 1998 definition found in Figure 1 above.

producers of information. The expectation was that these same organizations would undertake efforts to integrate their organically developed systems with operations in other military domains, across services, and across agencies with little formal guidance. These individual efforts took on increased urgency as the information environment construct gained widespread acceptance. Organizations tasked with the pursuit of national security objectives quickly recognized that their post-Gulf War effectiveness hinges on their ability to organize and utilize information as much as on their ability to produce physical effects.

At the end of the 1990s, increased acceptance of the environmental construct succeeded in spotlighting the need to manage information across the DOD. Reacting to this need, the 2001 Joint Publication (JP) 3-0's designated *Information* as a new war-fighting domain, placing it on equal footing with the four traditional domains.[10] This unprecedented domain designation could have created a common understanding of information's importance and helped develop an integrated approach to the development of future doctrine and strategy.

> "It is worth noting the difference between the terms *cyberspace* and *cyberpower*. Cyberspace is the domain in which cyber operations take place; cyberpower is the sum of strategic effects generated by cyber operations in and from cyberspace. These effects can be felt within cyberspace, as well as the other domains of land, sea, air, and space, and can also be cognitively effective with individual human beings."[9]

Unfortunately, far from serving as a rallying point for the advancement of the concept, this designation created more problems within the growing cyber community than it solved. The military services and other DOD organizations recognized that such a

[9] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 96.
[10] Joint Chiefs of Staff U.S. Department of Defense, "Doctrine for Joint Operations," Joint Publication (Washington, DC.: Government Printing Office, 2001). The term *Information Domain* appears four times in the text. Information is included in a list of domains including Air, Land, Sea, and Space numerous times within the text.

broadly defined domain threatened to upset their organic efforts to develop intelligence and information systems as well as their control over development of personnel and systems to support operations. Who would have the power to create standards and guide personnel and systems development in the new domain? Would one agency gain the power of setting standards and be able to dictate requirements to others, possibly influencing or restricting operating capabilities in other agencies?

Resistance to such a tectonic change led to an inability of the military services and DOD agencies to reach consensus on doctrinal and organizational issues, magnifying and not minimizing the debate over various approaches to information warfare.[11] In an effort to calm the debate, in 2006 JP 3-0 recategorized *Information* back to an environmental designation while simultaneously suggesting a definition for cyberspace, creating a separate domain within the information environment.[12]

Sixteen years after the gestation of the information domain began, and five years after its birth, the release of the 2006 JP 3-0 caused its demise. This same document,

---

[11] Olen L. Kelley, Colonel, "Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative" (Masters Thesis, U.S. Army War College, 2008), 1-2. Portions of this debate are still ongoing. In a 2011 presentation, Daniel Kuehl discussed the tension between categorizing cyber as part of integrated network electronic warfare operations or as a separate domain of its own. His purpose for raising this point is that in the US and much of the West, the cyber advocates have won the debate. In China and Russia, the debate has gone the other way, and as a result, they look at cyber less as a separate means of warfare and more as a tool to be used in creating the information environment within which conflict takes place across the DIME. For these global competitors, cyber strategy is more readily accepted as a subset of the information warfare strategy than in the West. Daniel T. Kuehl, "CYBERSPACE: Its Place in National Security," in *Cyber Power: The Quest for Common Ground* (Maxwell AFB, AL: Verbal presentation to conference panel 27 October, 2011).

[12] The information environment: "A global environment composed of all individuals, organizations, and systems that collect, process, disseminate, or act on information." Joint Chiefs of Staff U.S. Department of Defense, *Joint Operations*, 17 September 2006, Incorporating Change 2, 22 March 2010 ed., vol. 3-0, Joint Operations (Washington, DC: U.S. Government Printing Office, 2010), II-22. The most recent version of JP 3-0 maintains this environmental designation. ———, *Joint Operations*, vol. 3-0, Joint Operations (Washington, DC: U.S Government Printing Office, 2011), IV-2.

however, gave birth to the cyberspace domain. As defined in the 2006 JP 3-0, the new domain "consists of the interdependent network of information technology infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" – in other words, the physical infrastructure used for manipulating and storing electronic information. [13]

In 2006, the DOD also released another document containing a definition of cyberspace, the *National Military Strategy for Cyberspace Operations.* This document suggested a slightly different and more complete definition for the cyberspace domain: "Cyberspace is a domain characterized by the use of electronic and electromagnetic spectrum to store, modify, and exchange information via networked information systems and physical infrastructures."[14] The important difference between these two definitions is that the latter retains the emphasis on physical infrastructure and systems from JP 3-0 and adds the electromagnetic spectrum as the defining property of the domain.[15]

The designation of physical infrastructure as the border of the domain received an executive branch boost in 2008 when two additional official definitions emerged. First, National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," defined cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical

---

[13] _____, "The National Military Strategy for Cyberspace Operations," II-22.
[14] Ibid., 3.
[15] Each domain has a defined operational property. Operations in the maritime domain are primarily subject to the properties of hydrodynamics, the air domain by aerodynamic forces, and space by gravitational forces. These properties define, enable, and limit what can be done within the domain.

industries."[16] By defining the domain in this manner, the executive branch specifically aims to create a basis for categorizing and securing government/military information networks through a focus on the physical systems that compose them.

The second 2008 definition appears in a DOD memo from Deputy Secretary of Defense Gordon England. In May of that year, he defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[18] As with the previous efforts, this definition continues the trend of narrowing the domain down to the physical network infrastructure used for transmitting and storing information. As of this writing, the 2008 definition provided by Deputy Secretary England remains the official DOD definition of the domain.[19]

> DOD Cyber Strategy is based on five pillars: "to treat cyberspace as an operational domain; to employ new defense operating concepts; to partner with the public and private sector; to build international partnerships; and to leverage talent and innovation."[17]

The evolution of the cyber domain from the broad environmental construct of the 1990s to the emphasis on physical infrastructure today is illustrative of the pre-theory shaping process at work. The gradual process through which the national security community refined the definition of cyberspace resulted in a domain description that clearly identifies the physical nature of the domain – focusing on platforms and

---

[16] The 8 January 2008 NSPD 54 remains classified. The definition of cyberspace used within it is not, however. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 26.
[17] Montalbano, "DOD Website Sells Public On Cybersecurity Strategy."
[18] Gordon England, "The Definition of Cyberspace," (Washington, DC: Department of Defense, 2008), as cited in Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 27, and Richard Mesic et al., "Air Force Cyber Command (Provisional) Decision Support," ed. Rand Corporation. (Santa Monica, CA: RAND Corporation, 2010), 3.
[19] It appears as the formal definition in the official DOD dictionary: U.S. Department of Defense, "Department of Defense Dictionary of Military Associated Terms Joint Publication 1-02," 86.

infrastructure – while simultaneously retaining the domain's nature as a global common by not defining geographic boundaries or recognizing sovereignty over portions of the domain by any nation.

By no means is this evolution a completed process. Published one year after these more formal domain definitions, the 2009 National Defense University (NDU) work *Cyberpower and National Security* criticizes previous definitions for failing to identify what makes cyberspace a unique domain alongside land, sea, air, and space. It sought to refine the definition further by blending the 2008 definition from Deputy Secretary England with the definition in the 2006 *National Military Strategy for Cyberspace Operations*. The NDU work suggests defining the domain as:

> A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communication technologies.[20]

This definition, the NDU argues, demonstrates the simultaneous physical and virtual nature of the domain and identifies the unique physical characteristic that differentiates it from the other domains – the electromagnetic spectrum. While no national security agency has yet adopted this definition, this author agrees with the reasoning used by the NDU authors and their re-incorporation of the electromagnetic spectrum into the definition. This study adopts the NDU definition as the working definition for cyberspace for this research project. Having established the physical nature of cyber and its designation as a domain, the challenge now turns to determining how the

[20] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.

physical and electromagnetic characteristics of the cyber domain make it similar to and different from the other domains.[21]

Suitability of the Existing Domains as Sources of Cyber Theory

A political theory's usefulness is dependent on how well it describes and/or predicts the actions of the units exercising power in the world.[22] As presented in Chapter 2, the refinement of social science theory occurs through comparison of actual events to theoretical predictions. This process either reinforces theory or causes it to be reevaluated. As previously identified, both history and experience play a role in the theory development process. Cyberspace, however, has very little history upon which to draw. Relevant cyber operations, attacks, and events are usually classified or go unreported making it difficult to identify historical lessons to draw from. The lack of domain-specific history to draw from for guidance makes it necessary to survey existing International Relations theory to determine how the growth of cyberpower will affect the international system, the distribution and exercise of power within this system, and the relationships between political actors.[23]

---

[21] Not all scholars would agree that cyberspace has a definitive definition. For example, MIT professor David D. Clark provides a similar definition: "It is the collection of computing devices connected by networks in which electronic information is stored and utilized, and communication takes place." However, he goes on to say that to get a better understanding of what cyberspace is, one must to identify its important characteristics and catalog those rather than refining specific definitions. See David D. Clark, "Characterizing Cyberspace: Past, Present and Future," (Cambridge, MA: MIT CSAIL, 2010), 1.

[22] Robert L. Jr. Pfaltzgraff, "International Relations Theory and Spacepower," in *Toward a Theory of Spacepower: Selected Essays*, ed. Charles D. Lutes, et al. (Washington, DC: National Defense University Press, 2011), 37. Much of the context within the next several paragraphs is inspired by Dr. Pfaltzgraff's discussion of applying international relations domain theory to space as presented in his article and in personal discussions with the author regarding the application of existing theory to the cyber domain.

[23] Ibid., 39.

Over the last few centuries, the global domains of air, sea, and space have increasingly become the connective tissues that bind together the international system.[24] Current international relations theory addressing these domains emphasizes the power relations between international actors and provides a means of assessing their respective abilities to pursue national security interests through, and from, the subject domain. In each of these connective domains, the basic interests of states and other actors is to ensure safe passage for both themselves and their allies while maintaining the ability to deny the same freedoms to their enemies. It is reasonable to assume that state interests in the cyber domain will remain the same as in the more mature domains. Specifically, these interests are to ensure access to the lines of communication during peace and war while simultaneously retaining the ability to deny adversaries the ability to use these same lines of communication. Having established the reasoning behind defining cyber a physical domain and adopting the NDU definition for cyberspace, the remaining task is to establish cyberspace as a global common.

[24] S. Brimley, "Promoting Security in Common Domains," *Washington Quarterly* 33, no. 3 (2010): 119. Brimley's use of connective tissues as imagery is appealing because the global commons bind together the system of states in a manner that requires continuous effort to forgo the benefits of trade, commerce, and communication. Additionally, some areas within each of the common take on greater importance than others; the commons are not simply spaces within which the systems of states exist. More specifically, certain lines of communication within these commons act like tendons and ligaments to pull the system together, a concept that will be explored later in this dissertation.

A global common

The physical characteristics of cyberspace pass through and exist within the other domains; it is unique in this respect. The reliance of cyber lines of communication on the other physical domains for continued existence means that in some cases use of the domain is subject to many of the same legal, physical, and international norms that define the more traditional domains. Examining how closely the cyber environment mirrors the land, sea, air, and space domains is an important step toward determining their suitability to serve as models for further analysis and to narrow the scope of the investigation.

> Cyberspace is obviously a man-made domain, but it retains many of the basic characteristics of the natural domains of the sea, air, and space – ubiquitous, central to lives and livelihoods, and so vast that establishing total awareness or control is practically impossible. While component parts of information networks and infrastructure are owned by states, businesses, and other actors, the nature of this architecture and the way information moves within it demands a global view. In this important respect, it is useful to conceive of cyberspace as a global domain – like the sea, air, and space domains.[25]

Of the big four extant domains, three are commonly identified as global common: air, sea, and space. Each of these three is global by nature and serves as a common medium used and for the most part shared by all international actors for communication and commerce.[26] In almost all modern scholarly analysis, the cyber domain is also included in the list as a global common; however, what is a global common?

[25] Ibid., 125.
[26] Ibid., 120.

The Oxford Dictionary defines a global common as "any of the earth's ubiquitous and unowned natural resources, such as the oceans, the atmosphere, and space."[27] International agencies and institutions use a similar approach. Both the UN and the Organization for Economic Cooperation and Development define a global common as "natural assets outside national jurisdiction such as the oceans, outer space, and the Antarctic."[28] Clearly, this definition remains constant from source to source, focusing on unowned natural resources.

From a national security perspective, the key element in these definitions is not the national resource characteristic. Instead, the key feature is that these areas are unowned and that no one nation is capable of exercising sovereignty over them in a manner that denies global access to the domain.[29] Instead, formal and tacit international agreements consider these areas shared space. Although not yet formally reflected in treaties, the approach to the cyber domain has evolved in a similar manner. No nation has yet claimed sovereignty over the right to transit its physical borders.[30] As unowned territory, commons are not subject to any individual nation-state's law, and enforcement

---

[27] "Global common." *The Oxford Pocket Dictionary of Current English*. 2009. *Encyclopedia.com.* 14 March 2012 <http://www.encyclopedia.com>.

[28] United Nations Statistics Division, "Global Commons Definition," (2011), http://unstats.un.org/unsd/environmentgl/gesform.asp?getitem=573. and , Organization for Economic Co-operation and Development, "Global Commons Definition," (2011), http://unstats.un.org/unsd/environmentgl/gesform.asp?getitem=573. Last visited 8 November 2011.

[29] Barry Posen describes the commons in the following manner: "The 'commons,' in the case of the sea and space, are areas that belong to no one state and that provide access to much of the globe." See Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28, no. 1 (2003): 8. Like the sea and air, cyberspace provides access to much of the globe. It is important to note here that individual elements of cyber infrastructure are owned, are physical hardware, and for the most part exist within sovereign territory. The domain in its entirety is not owned, and no one nation or individual can restrict access to the global domain.

[30] Some nations, notably China and Saudi Arabia, have firewalls that restrict access to domain users within their borders, but they do not restrict the flow of transient information through the lines of communication in any meaningful way.

of international law is subject to the discretion and capability of members of the international community.[31] A fundamental and universal principle of each of the global commons is the assumption that all members of the international community have an equal and unquestioned right to use and transit these shared spaces. This same rite of passage has become the international norm for the global network composing the cyber domain. This is an important point because despite the recognized right of individual nations to control access to information within their territory, widespread intentional disruption or denial of the right to freedom of transit in the cyber domain is not accepted international practice.[32] This is true even though the domain's physical assets travel through the sovereign territory of other nations on privately owned physical infrastructure.

As Shawn Brimley points out, the term *global common* does not imply any specific legal meaning. Regardless of their location, while transiting the global commons, ownership and responsibility for the actions of the aircraft, satellites, ships, and now information networks operating within these commons remain the property and responsibility of their owners and operators. Legal scholars are working to determine if the same rights of ownership and responsibility apply in the cyber domain, a position the

[31] There are some exceptions to this statement; airspace over a nation is subject to its sovereign laws, which in some cases differs from international aviation standards. Additionally, well-established maritime law provides well-defined zones off a nation's coast within which it can enforce sovereign law.

[32] For instance, China and Saudi Arabia restrict access to cyber-delivered information within their borders.

United States supports, with its emphasis on both freedom of navigation within the commons and freedom of information.[33]

Because of overwhelming scholarly and government designation as a global common, for research purposes, this study defines cyberspace as a global common.[34] Despite public ownership of individual elements of the physical cyber domain, the network as a whole is free from claims of sovereignty, which is in line with both the dictionary and international definitions of a global common. Furthermore, this conclusion is in keeping with the majority of scholarly writing and discussion, the worldwide nature of the domain, and the freedom of navigation that exists within the domain.[35]

To briefly review, up to this point in the chapter, we have concentrated on identifying cyberspace's relevant characteristics: It is physical in nature, it is a domain, and it is a global common. We have also identified that a lack of historical experience and narrative from which to draw in creating a cyber domain theory requires us to look outside the domain for guidance. Using cyber's relevant characteristics as a guide, we now transition to the next step, identifying the domains and theories it most closely resembles.

---

[33] Brimley, "Promoting Security in Common Domains," 122. When he wrote this article, Brimley was a strategist in the Office of the Secretary of Defense. He has since moved on to become Director for Strategic Planning at the National Security Council.

[34] The DOD's Joint Operations Access Concept lists cyberspace as a global common along with air, sea, and space. See Joint Chiefs of Staff U.S. Department of Defense, "Joint Operational Access Concept," (Washington, DC: Government Printing Office, 2012), 1.

[35] Despite the almost universal treatment of cyberspace as a global common, an argument can be made that cyberspace has not met the requirements for this designation. See Patrick W. Franzese, Lt Col, USAF, "Sovereignty in Cyberspace: Can it Exist?," *Air Force Law Review* 64 (2009).

Selection of domains for comparison

Cyberspace's designation as a global common narrows the field of suitable extant theory to that of the other global commons – air, sea, and space. What this drops from consideration are the landpower theories from such seminal strategists as Clausewitz and Jomini. This is not a claim that such august terrestrial theory has nothing to teach us, but simply that by the nature of its subject domain, landpower theory is less well suited for use as a basis from which to create a foundation for cyberpower theory. Fortunately, the universality of these seminal landpower theories means that incorporation of their key aspects into domain power theory of the commons has already taken place.[36]

Of critical importance in differentiating land theory from theories of the commons is that fundamentally, land theory addresses an environment that is not reliant on technology to enter and exploit. This condition is the polar opposite of the technologically based cyber domain that not only requires technology to navigate and manipulate, but in the absence of technology ceases to exist.

Finally, the geographic elements that define the land domain are the dominant factor in determining the nature of relationships between states and their ability to compete with each other for control and influence beyond their geographic borders. These extreme differences in the nature of the land domain as compared to the cyber domain make it the least suitable of the extant domains for service as a model for cyber theory development.

[36] In fact, theorists of the global commons often patterned their theories upon elements of land theory.

At the other end of the spectrum is the space domain. While it would be unfair to claim that there have been no attempts to create space domain theory, unlike the land, sea, and air domains, spacepower has no universally recognized theory.[37] The development of spacepower has not occurred according to a master plan or with guidance from spacepower theory. Spacepower nations gained prominence in an ad hoc manner by mating technical capabilities and requirements to meet existing mission needs.[38] In general, the space domain suffers from a lack of focus and advocacy.

Defense and political leaders tend to view space domain assets as individual tools to solve a collection of often unrelated problems, rather than as a new holistic capability for advancing national security interests. For all practical purposes, it was not until Desert Storm and the integration of spacepower into combat operations that the US began to think in terms of spacepower.[39] Like cyber, space too is in a pre-theory stage, meaning there are no suitable theories from which to choose in order to perform a comparative analysis. More than half a century after the Russian launch of Sputnik on 4 October 1957, we are still in search of a formal theory; space domain theorists are still working to develop a common understanding of spacepower and its national security implications.

---

[37] The only fully developed attempt to create a geopolitical theory of space the author is aware of is Everett C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age*, Cass series--strategy and history (Portland, OR: Frank Cass, 2002).

[38] For a good discussion of the history of space development and the difficulties in developing space theory, see James Andrew Lewis, "Neither Mahan nor Mitchell: National Security Space and Spacepower, 1945-2000," in *Toward a Theory of Spacepower: Selected Essays*, ed. Charles D. Lutes, et al. (Washington, DC: National Defense University Press, 2011).

[39] With real-time satellite detection of missile launches and warning to theater commanders, GPS navigation feeds directly to individual combatants in the field, and communications requirements both within and between theaters of operations and controlling headquarters all came together to demonstrate the utility of spacepower on the modern battlefield, bringing increased attention to its development.

Many factors hinder the development of spacepower theory. One is the lack of force application from the domain, making it a lesser sibling among military domains. Another is the cost of programs to reach orbit that keeps numbers of assets low, reducing the perceived urgency for creation of spacepower theory. Additionally, the lack of manned combat systems and interservice/departmental rivalries both contribute to the inability to form consensus and move toward the next stages of theory development. For the most part, the spacepower theory that has emerged from military and academic sources does not focus on the environment as a war-fighting domain. Instead, it focuses on maintaining ensured access to the domain for development and transmission of information, not control of the lines of communication.

The air and maritime domains, on the other hand, are quite similar to the cyber domain and are good candidates to serve as the basis from which to begin cyber theory development. Most importantly, both domains have well-established theories for analysis and comparison to the cyber domain. More specifically, however, both domains are technologically dependent, meaning that technology is required to access and maintain a presence within them.

Additionally, like cyber, both the air and maritime commons are unclaimed areas within which allies, adversaries, and neutrals share lines of communication. Even more important, as we see occurring today with cyber, the development of the technology to enter and leverage these domains had a significant effect on every element in the DIME.

Finally, the development of the sea and maritime domains redefined the nature of interactions between nation-states during both peacetime and war, a state of flux that continues today as new technology increases man's ability to utilize these mediums.

Taken together, it is clear that the established domain power theory of both the sea and air commons provides the most appropriate point of comparison to begin our search for a model upon which to begin building cyberpower theory.

Maritime and Air Models

Cyber operations have more in common with operations in the maritime and air domains than most observers initially appreciate. Just as air and maritime operations rely on defined points of entry into the domain (ports and airports), linked by lines of communication for movement of goods and services (sea lanes and airways), cyber operations also depend on lines of communication to move goods through undersea cables and satellites to established destinations. Additionally, like the air and maritime lines of communication, the paths of international cyber communication are for the most part open to all nations and all users.

In international territory, air, maritime, and cyber lines of communication all transit the global commons free from claims of sovereignty and national appropriation. Even when the lines of communication in these domains transit through otherwise sovereign

> "In the late 19th century, American Admiral Alfred Mahan described the rise of sea power and its relationship to a nation's global strength. In the early 20th century Italian General Giulio Douhet was first to develop theories about the essentiality of air power to future military superiority. Today America's 'cyber warriors' have begun to talk about the need for their nation to be the 'dominant' cyber war power in order to be assured of continued global military superiority. Although no Mahan or Douhet has yet emerged, America's cyber generals have described cyberspace as a domain similar to sea, air, and outer space as a potential battleground."[40]

[40] Richard Clark, "Software Power: Cyber Warfare is the Risky New Frontline," Harvard Kennedy School, http://belfercenter.ksg.harvard.edu/power/2011/02/07/software-power-cyber-warfare-is-the-risky-new-frontline/.

territory and cross international borders, the air, sea, and cyber lines of communication continue to operate with a minimum of inspection or requirement for prior approval/coordination.

Moreover, all three are international commons, spanning the globe, used for the movement of goods, services, information, and the exercise of national power along shared lines of communication, by all nations, organizations, and individuals – allies, foes, and neutrals alike. Finally, just as freedom of movement and access to lines of communication in the air and on the seas is critical for national power, freedom of movement and access to the global cyber lines of communication is increasingly becoming a critical aspect of international power.

These macro similarities between the environments of sea, air, and cyber, however, do not allow us to simply create good cyber theory by picking an established air or maritime theorist and substituting in cyberspace strategy for that theorist's use of the word *air* or *naval*. As would be expected, air and maritime theorists deal with the development, organization, and use of military forces uniquely suited to the specific environment upon which they focus. In general, theories of the air and sea domains focus solely on the employment of forces within these domains to achieve national goals and increase national power and prestige.[41] Naval theorists focus on the use of fleet action to control lines of communication and destroy opposing forces on the high seas. Air theorists focus on destruction of enemy air capability and war-supporting infrastructure from the air to eliminate an enemy's military capabilities. A cyber domain theory must be broader to fully describe the interaction and interdependence of cyberspace operations

[41] Klein, "Corbett in Orbit: A Maritime Model for Strategic Space Theory," 62. Klein touches on this point regarding seapower theories as he works to adapt them for spacepower. I have modified his statements for application to cyberpower and expanded it to include air domain theory.

with other operating environments and to capture cyber's effect across the DIME during both peacetime and conflict.

Where to begin

Having selected our domains to serve as sources of theory for analysis, we move to the next chapter, where we begin the assessment process with the maritime domain theorists.[42] Following that is Chapter 5 assessing our air theorists. In keeping with the natural progression of domain development, presentation of these theories is in the order of their first publication. This allows the reader to experience the development and refinement of domain power theory as each writer leverages new historical experience.

[42] As identified in Chapter 2, the theorists of interest are Alfred Mahan and Julian Corbett,[42] from the maritime domain, and Giulio Douhet, William Billy Mitchell, and Alexander de Seversky, from the air. These are all writers from the initial decades of both the maritime domain (post-metal hull and steam) and air domain development. This is in keeping with Van Evera's guidance on case selection. Van Evera discusses case selection at the end of Chapter 2. Of his eleven suggested criteria for selection, #5: *Select cases that resemble current situations of policy concern* and #7: *Select cases that are well matched for controlled cross-case comparisons* apply in this instance. See Van Evera, *Guide to Methods for Students of Political Science*, 77-88.

Chapter 4: Maritime Theory

This chapter begins the process of assessing extant theory in order to identify elements of analysis for comparison to the cyber domain. As discussed above, this process begins with the maritime domain, focusing on two of the most prominent maritime theorists, Alfred T. Mahan and Julian S. Corbett. Both great theorists formulated and wrote their theories after the end of the Civil War and before the beginning of World War I. This was a time of great change in the role of the maritime domain in binding together the international system. Building upon the historical lessons gleaned from an analysis of events during the age of sail, both theorists identified aspects of maritime power and assessed their enduring aspects by applying them to a domain dominated by the new technologies of steam propulsion, steel hulls, and rifled cannon. The theories they espoused informed and guided the transition from the romantic days of sail into the modern naval forces of today.

For this dissertation's purposes, Mahan's theory will be considered as having been published in *The Influence of Sea Power Upon History, 1660–1873* in 1890.[1] Similarly, Corbett's *Some Principles of Maritime Strategy*, published in 1911, will serve as the basis for evaluation and comparison.[2] The author chose these books because each represents the complete publication of that theorist's thesis in its initial and most influential form. These books set the stage for

[1] Mahan, *The Influence of Sea Power Upon History, 1660-1783*, 183-88.
[2] Corbett, *Some Principles of Maritime Strategy*.

discussing each theorist's views in subsequent analysis of their writings by critics or the authors themselves.

This chapter begins with a short review of the domain itself, describing development of the domain and its key characteristics to the extent necessary for framing subsequent analysis of the relevant theories. It then assesses each author's theory individually, briefly discussing the environment within which the author wrote from a geopolitical and strategic standpoint and providing a background for the creation of his theory. Having introduced the environment within which the author wrote, this paper will then review his maritime power theory and pull elements of analysis from the theory for further assessment. This chapter then concludes with a summary of the maritime domain theories and their combined elements of analysis.

The Maritime Domain

It would be difficult to overstate the importance of the maritime domain in international relations and trade, both in the time our theorists were writing and today. According to a 2011 NATO report on access to the global commons, 80% of all raw commodities and merchandise transported internationally move upon the maritime domain, three-quarters of which transit international chokepoints, such as a canal or strait.[3] The volume of goods transported in this manner quadrupled between 1968 and 2008, including over half of the world's oil

[3] Summarized from: Major General Mark Barrett et al., "Assured Access to the Global Commons," ed. Supreme Allied Command Transformation (Norfolk, VA: North Atlantic Treaty Organization, 2011), 4-5.

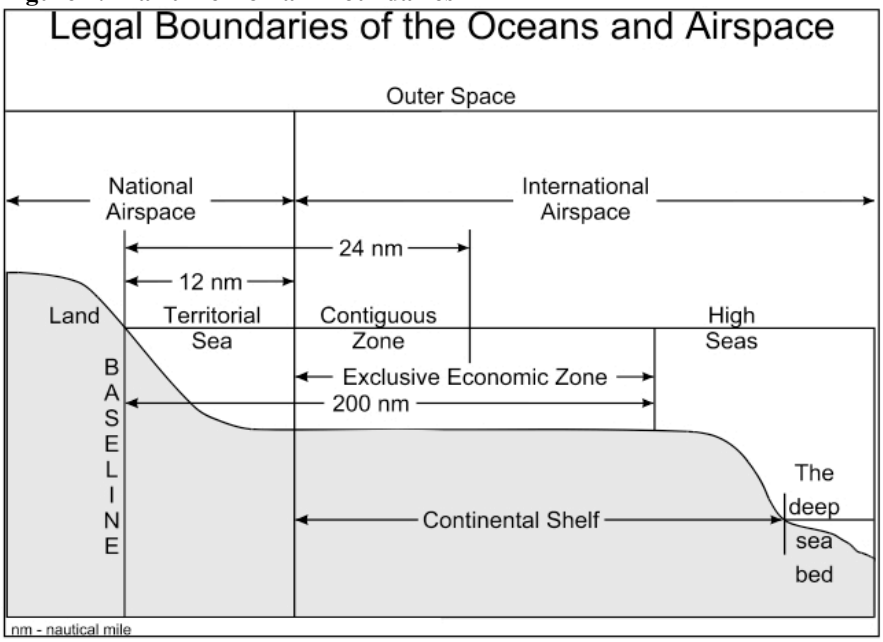
distribution. The sheer volume of commerce and communication taking place in the maritime domain makes it a critical factor to any nation's national security.

Of the four global commons introduced earlier in this dissertation, the seas were the first to be both explored and exploited using technology. The opening of the maritime domain for commerce between nations meant that the maritime power became a critical factor in determining national livelihood and the distribution of power within the international system. By virtue of its long history and the central role played by maritime commerce during development of both modern nation states and the international system, a well-defined and widely recognized set of international agreements and customs applying to the maritime global commons have developed. These agreements and customs rest upon centuries of practical experience in negotiation and conflict between nation-states. The modern capstone agreement capturing these historical lessons and providing guidance for maritime operations worldwide is the United Nations Convention on the Law of the Sea (UNCLOS).[4]

[4] United Nations, "United Nations Covention on the Law of the Sea," ed. Division for Ocean Affairs and the Law of the Sea (New York, NY 1982). According to the US Navy's *Handbook for Commanders*, NWP 1-14M, the United Nations Convention on the Law of the Sea (UNCLOS) is rooted in traditional recognition that the world's oceans separate into international waters, territorial seas, and high seas. The extension of national jurisdiction out to 12 miles (previously 3 miles, a distance once associated with the range of projectiles shot from a cannon) was the subject of intensive negotiation between 1973 and 1982. Originally, UNCLOS was designated to come into effect on November 16, 1994. Despite wide international participation, the US neither ratified nor signed the original UNCLOS because of concerns over deep seabed mining provisions within the treaty. Subsequent changes to these provisions resulted in the president's submission of the UNCLOS to the Senate for ratification in 1994. It was not until ten years later, in February of 2004 that the Senate Foreign Relations Committee recommended action on this document; as of the date of this writing, the US has yet to ratify the treaty. Despite not being a party to the UNCLOS, the US considers the navigation and oversight provisions it contains to be customary international law and compiles with the UNCLOS in all areas except the provisions on deep seabed mining. A

From a national security perspective, the term maritime domain is broadly defined as consisting of the "oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals."[5] Within this domain are a series of waterways from the coastline to the high seas that require transitioning during the exercise of maritime power as well as exclusive economic zones over which nations claim varying levels of sovereignty. The UNCLOS describes all of this (Figure 1).[6] Although the United Nations convention is a modern document, it

Figure 2: Maritime Domain Boundaries



short but more complete description of this history can be found in the US Navy Commander's Handbook: Department of the Navy U.S. Department of Defense, "The Commander's Handbook on the Law of Naval Operations," ed. US Naval War College President, International Law Department (Washington, DC: Government Printing Office, 2007).

[5] U.S. Department of Defense, "Department of Defense Dictionary of Military Associated Terms Joint Publication 1-02," 207, For a discusson of utility of maritime forces across this "broad" definition see William C. Martel, *Victory in War: Foundations of Modern Strategy*, Rev. and expanded ed. (New York, NY: Cambridge University Press, 2011), 350-58.

[6] Part II of the UNCLOS, Article 2 defines sovereignty to include the airspace over territorial waters. Articles 3 through 16 define the limits of territorial sea extending out to 12 miles from the coast.

is rooted in customs in effect during the late nineteenth and early twentieth centuries, the period within which Mahan and Corbett developed and espoused their theories.

Before launching into a discussion of Mahan's theory, a brief review of the maritime domain's characteristics is in order. Most importantly, the domain is a global commons, completely circling the planet, the majority of which consists of surface area unclaimed by sovereign nations. Defining the geography and boundaries of the domain are the landmasses upon which we live and from which nations project power. Throughout the maritime commons, outside of specifically defined territorial waters, there is an international expectation for freedom of navigation for peaceful purposes.[7] In the age of steam, it was very difficult to monitor and track ships with any degree of accuracy. Although these ships were transiting the domain in exercise of this assumed right to freedom of navigation, lack of tracking accuracy made locating and identifying friends, enemies, and neutrals difficult without maintaining a physical presence within the domain. Finally, and particularly important to understanding the unique nature of theories pertaining to this commons, are two points:

1) All nations simultaneously share military and commercial lines of communication, as well as the infrastructure to support these "highways of the sea."

[7] Freedom of navigation: the right recognized in international law, esp. by treaties or agreements for vessels of one or all states to navigate streams passing through two or more states. See Merriam-Webster Dictionary, "Freedom of navigation," Merriam-Webster, Incorporated, http://www.merriam-webster.com/dictionary/freedom%20of%20navigation.

2) Landmasses and ports from which access to the domain is possible create geographic chokepoints that funnel movement along the lines of communication within this vast global commons.

Mahan

Alfred Thayer Mahan (1840–1941) was born on September 27, 1840, the son of West Point professor and author Dennis Hart Mahan and his wife, Mary Okill Mahan.[8] Mahan gained both insight into the academic environment and ready access to education through his parents. He was a good student, eventually settling on a desire to attend the United States Naval Academy. Over his father's initial objections, Mahan entered the academy as a sophomore in 1856.[9] Graduating in 1859, he became an ensign assigned to blockade duty during the Civil War. Despite the overall monotony of the blockade posting, Mahan's understanding of naval power benefited from repeated exposure to action against forts and the conduct of amphibious warfare. These events shaped his conception of maritime power and the role it plays in pursuit of national security objectives.[10]

At the end of the Civil War, the US Navy, in keeping with the standard military operating policy of the time, began a rapid demobilization, sold, and

[8] W. D. Puleston, *Mahan; The Life and Work of Captain Alfred Thayer Mahan* (New Haven, CT: Yale University Press, 1939), 12.
[9] Ibid., 18.
[10] Ibid., 40. Chapter 2 of Puleston's biography of the great seaman details Mahan's Civil War blockade service, including various ship-and-shore postings. Mahan did not experience a single engagement considered fleet action – a deficiency that perhaps allowed him to view maritime power in a less romantic light than others with a taste of ship-on-ship combat.

decommissioned its wartime fleet of 700 ships mounting 5,000 guns.[11] The pace of this demobilization was stunning; by December 1870, the US Navy claimed only 52 fully commissioned ships out of the 200 hulls it retained. This reduced fleet mounted a mere 500 guns, and was by all meaningful measures obsolete in comparison to the European navies. Clearly, during the post-Civil War years the United States did not place a strong maritime force high on its list of national security priorities.

Instead of maintaining its naval forces, US national wealth focused on rebuilding the southern states and exploring/expanding the nation westward. This was a period of national introspection and internal development, a time that found the Navy relegated to missions of costal patrol and limited overseas operations to show the flag. With the nation's attention focused inward, there was little interest in reversing the erosion of naval capabilities or maintaining a large peacetime military.[12] As a serving naval officer, Mahan observed this period of decline while assigned to various commands both afloat and ashore, including a stint at the Naval Academy. What he observed did not fit well with his growing understanding of the role maritime power plays in the growth of nations. His overseas experiences and duties exposed him to the importance of maritime commerce for trade to foreign markets and highlighted for him the role geography plays in shaping international power. Having served during both war and peacetime operations, witnessing first-hand the role of military forces toward pursuit of national security objectives, Mahan was now intellectually equipped to

[11] E. B. Potter and Chester W. Nimitz, eds., *Sea Power; A Naval History* (Englewood Cliffs, NJ: Prentice-Hall,1960), 338-39.
[12] Ibid., 339.

begin formulating his theory of maritime power. All that was missing was the opportunity to develop his ideas fully, an opportunity that soon arose.

The post-Civil War impotence of the US Navy, while little appreciated by the public, was not lost on the nation's maritime professionals. In 1884, at the urging of the Navy's senior active duty officer, Rear Admiral Stephen B. Luce, the Secretary of the Navy, William E. Chandler, issued General Order 325, which established the Naval War College (NWC) to provide a facility for advanced professional study by naval officers.[13] The NWC curriculum focused on the growth of naval forces and their use of modern steam-driven, steel-hulled ships mounting rifled cannon. It also explored how this modern force should "influence national foreign policy aspirations and planning" for the United States.[14]

Seeking instructors capable of intertwining naval history and the study of technology, in 1844, Admiral Luce, already familiar with Mahan and his thinking invited him to join the NWC faculty. Tasked with preparing lectures on naval history, tactics, and the evolution of tactics, Mahan leapt at the chance and began to formulate and articulate his thoughts regarding seapower theory and command of the sea.[15] It was these lectures, developed and delivered over a period of years at NWC that served as the basis for publication of *The Influence of Sea Power Upon History 1660–1783*.

In the manner of pre-theory development introduced in Chapter 2, Mahan sought to create a common understanding among naval professionals about the

---

[13] Robert Seager, *Alfred Thayer Mahan: The Man and His Letters* (Annapolis, MD: Naval Institute Press, 1977), 142-3. See also, "History: NWC History," U.S. Naval War College, http://www.usnwc.edu/About/History.aspx.
[14] ———, *Alfred Thayer Mahan: The Man and His Letters*, 143.
[15] Ibid., 145-6.

importance and role of maritime power, an understanding that would enable them to make their case for a strong effective navy and turn the nation away from a militarily isolationist position. Like the land theorists who preceded him, when formulating and creating his theory, Mahan relied upon historical study of the age of sail, his own military experience serving at sea and ashore, and his understanding of the need for a powerful naval force to pursue lasting national security.[16] With this brief background and an understanding that Mahan developed his theory at a time of great change in the maritime domain, the transition from sail to steam and wood to steel and the introduction of long-range rifled weapons, we now transition to a discussion of his theory and its principles.

The Theory of Mahan

As noted, Mahan formulated, refined, and raised to prominence his theory of maritime power during the period between the Civil War and World War I, a period of great change within the US Navy and one of expanded use of the maritime domain in general for

> "The first and most obvious light in which the sea presents itself from the political and social point of view is that of a great highway: or better, perhaps of a wide common, over which men may pass in all directions, but on which some well-worn paths show that controlling reasons have led them to choose certain lines of travel rather than others. These lines of travel are called trade routes; and the reasons which have determined them are to be sought in the history of the world."[17]

[16] A. T. Mahan, *From Sail to Steam; Recollections of Naval Life* (New York, NY: Harper & brothers, 1907), 276-86. On these pages Mahan describes his use of Jomini and other authors as a means of focusing his thoughts and the decision to use history as the means for exploring how both military and commercial control of the sea influences the polices of nations. Historical scholars consider Jomini to be Mahan's touchstone for development of his theory.

[17] Mahan, *The Influence of Sea Power Upon History, 1660-1783*, 25.

transportation and communication. The technological transition from sail to steam multiplied the commercial importance of the domain. Expanded commercial use led to increased military importance. In the space of a few decades, steam technology reduced the importance of prevailing winds and weather. Transit time decreased, allowing information and goods to flow more freely and for power projection to occur more rapidly. The increased freedom to move across the seas increased contact between nations and cultures, bringing with it a competition for wealth and power. In formulating his theory to fit these new and expanding uses of the domain, Mahan's insight was that although the sea is a great commons, particular lines of communication within the commons develop and become important to national power. Through his studies, Mahan concluded seaborne commerce makes nations great and that security for this trade is essential; command of the sea ensures the ability to engage in commerce.[18] Until the publishing of his theory, control of the sea "was an historic factor which had never been systematically appreciated and expounded."[19]

Mahan's effort to fill this gap consists of both theory and historical analysis. The first chapter (89 pages) contains the heart of his argument, while the historical analysis illustrates and refines his points.[20] Fundamentally, Mahan's writings argue "that strong naval and commercial fleets are critical to a nation's

---

[18] William Edmund Livezey, *Mahan on Sea Power* (Norman, OK: University of Oklahoma Press, 1947), 48.
[19] Mahan, *From Sail to Steam; Recollections of Naval Life*, 276.
[20] Mahan added the first chapter at the recommendation of his publisher, who wanted to make the book more accessible and entertaining for the general public. Because his book uses historical examples from the age of sail, it was initially much more popular and well-read in Europe, especially England, the nation whose domination of the sea under sail is painted in a favorable light by Mahan's theory.

military power."[21] His inclusion of commercial fleets and the importance of trade in addition to the naval facet of maritime power are a significant contribution to the power of his theory, giving it instructive sway and making it a source for policy guidance about domain power development.

Mahan's experience and studies in the late 1800s during a time of colonialism, international trade, and expanded European influence led him to conclude that nations that rely solely on domestic trade cannot become major powers; international exchange and the access to capital and the raw materials it provides are critical for continued national growth.[22] According to Mahan, three elements are necessary for creating global economic power in a command mercantile system: 1) production, 2) shipping, and 3) colonies/markets as sources of commerce and resources.[23] The requirement to create, protect, and facilitate trade over the maritime lines of communication underpins this triad of trade and necessitates the construction and maintenance of strong maritime power capabilities. As nations seek international trade, growing dependence on maritime lines of communication leaves them vulnerable to attacks on shipping and leads to international complications as competing interstate interests come into conflict. On the international stage, the solutions to these inevitable conflicts require, at least in part, a strong maritime force.

---

[21] Martel, *Victory in War: Foundations of Modern Strategy*, 119.
[22] Livezey, *Mahan on Sea Power*, 42, See also: Mahan, *From Sail to Steam; Recollections of Naval Life*, 25-28.
[23] Mahan, *The Influence of Sea Power Upon History, 1660-1783*, 28, As sumarized in: James C. Bradford, *Admirals of the New Steel Navy: Makers of the American Naval Tradition, 1880-1930*, Makers of the American Naval Tradition (Annapolis, MD: Naval Institute Press, 1990), 39. Later in this discussion the author will present Mahan's elements for creating maritime power; those listed here are for national economic power.

For Mahan, the mission of naval forces during times of war is to control areas of sea communications in order to secure their use for allied cargo vessels and transports while denying the same freedom of movement to foes.[24] Central to Mahan's thesis is the idea that during times of conflict between a nation and another seapower, ensured access to these lines of communication is only possible through the neutralization or destruction of the enemy's fleet by a more powerful fleet of one's own.[25] Mahan's theory does not accept that commerce warfare by cruisers to interrupt trade is sufficient to achieve national security objectives; rather, during times of war, destruction of the enemy fleet is necessary. From Mahan's perspective, commerce warfare can deny the use of the sea to enemy merchant marine forces but cannot secure it for one's use. Commerce warfare is not a means to the desired end state; rather, it is an adjunct to the main objective of destroying the enemy fleet.[26]

Mahan's belief in the inherently offensive nature of naval forces leads him to focus on destruction of an enemy's fleet.[27] This offensive nature requires concentration of the fleet at decisive points when opportunities to strike a killing blow against an enemy's source of maritime power present themselves. This philosophy leads to operational strategies where the fleet must never be divided or dispersed, but rather capable at all times of providing overwhelming force to cleanse the commons of threats. The process of destroying enemy naval power is thus the process of gaining and maintaining command of the sea to keep one's

[24] Potter and Nimitz, eds., *Sea Power; A Naval History*, 342.
[25] Ibid.
[26] Ibid.
[27] Livezey, *Mahan on Sea Power*, 47.

own lines of communication open while simultaneously monitoring neutral trade without unnecessary efforts at privateering operations against enemy merchant traffic.

While naval power for destruction of enemy fleets is a critical factor of Mahan's theory, he also recognizes that maritime power is more than the simple act of building a fleet. His theory addresses the maritime potential of nations by specifically identifying the following six factors that determine a nation's sea power:[28]

1. Geographical position
2. Physical conformation (including natural conditions and climate)
3. Extent of territory
4. Number of population
5. Character of the people
6. Character of the government (and national institutions)

Geographic position:[29] The geographic position of a nation determines its ability, aptitude, and potential for developing seapower. According to Mahan, geographic positioning is the single most important factor in seapower potential. An island nation is able to focus its efforts on naval defense without the need to simultaneously support development and maintenance of a large army and prepare for defense against invasion.[30] Geography also plays a role in determining the disposition of a nation's fleet. Nations with one shoreline are able to concentrate their forces as opposed to dividing them between theaters of operations, which requires the development and maintenance of two operating fleets or a reduction

[28] According to Mahan, maritime power not only includes the strength of naval forces "afloat, that [rule] the sea or any part of it by force of arms, but also the peaceful commerce and shipping from which alone a military fleet naturally and healthfully springs, and on which it securely rests." See ibid., 41.
[29] Mahan, *The Influence of Sea Power Upon History, 1660-1783*, 29-35.
[30] He is writing before the development of airpower.

of fleet strength in individual theaters. Nations lucky enough to be in a central position that provides interior lines of communication and movement have an advantage during times of conflict. They can use their territory for defense and homeports for refuge. Similarly, nations close to or on a major trade route have the advantage of geographic control over that route, which allows them to use the line of communication for their own purposes while denying use of the same to others when desired.[31]

Physical conformation:[32] This attribute focuses on the nation's physical characteristics and how they affect both the ability to access the maritime domain and the nation's incentives for development of maritime power. Key features of the maritime domain for consideration include numerous well-placed ports for deep draft ships and navigable waterways extending into a nation's interior – ideally ending at those good ports – to encourage internal and external trade. Placement of these ports and waterways determines whether they act as a strength or weakness during conflict. During times of war, undefended ports and waterways become a liability by providing an enemy access to a nation's territorial heartland.

In addition to the strictly maritime aspects of a nation, the predominant physical condition of the land is important. Contrasting France and England best illustrate this point. Mahan identifies the requirement for England to trade in order to acquire goods and supplies, whereas France, as a continental power with good

[31] Mahan discusses potential importance of US positioning along any trade route opened due to the construction of a cross-isthmus canal in Central America, a vision that later came to fruition.
[32] Mahan, *The Influence of Sea Power Upon History, 1660-1783*, 35-42.

land and access to resources, was able to rely on domestic sources and overland trade with other nations for goods. Therefore, France historically had less incentive to develop maritime commerce.

Finally, Mahan notes that a nation's internal physical geography provides situations where the sea becomes a vital internal line of communication, such as in Italy. Italy is demonstrative of a nation consisting of states separated by internal mountains that restrict overland trade and islands separated by expanses of water. Both of these internal physical characteristics of the nation necessitate and incentivize the development of maritime capability.

Extent of territory:[33] The extent of a nation's territory determines its ability to gain and maintain exposure to the domain. Here the size of a nation's territory is not Mahan's focus; instead he focuses on the relationship between the physical characteristics discussed above – the length of a nation's coastline, number of harbors, location and extent of waterways, etc. – compared to the total population of the nation. A nation with a long coast and many good ports has excellent access to the sea. If the nation is populous and maritime-focused, this provides many points from which to access the maritime domain, making it difficult for an adversary to restrict access (blockade). On the other hand, if the nation is under-populated with relation to the access, the coast is difficult to defend and adversaries can use these points of access to gain a foothold without having to overcome strong defenses. Conversely, if ports are few in numbers and closely spaced, then concentration of force for defense is possible, as is concentration for blockade by an adversary. Ultimately, Mahan's point is that if a

[33] Ibid., 42-44.

nation is well prepared to use and defend the access points to the maritime domain, a long coast with many ports is an advantage. If the nation is not capable of defending and using these ports, then they are a disadvantage. For means of illustration, he uses the Confederate states during the US Civil War. Their numerous ports and access locations could have made blockade actions impossible for the Union, who would have been unable to cover the long coastline in sufficient strength to resist determined attempts run the blockade. Instead, the lack of a dense population in the South along its waterways, ill-defended ports, and a low concentration of Confederate naval vessels enabled the Union to string out forces thinly and still achieve its operational goals.

Number of population:[34] The larger the population pursuing domain-oriented occupations, the greater the nation's potential for domain power. Closely related to the ratio between extent of territory and overall population above, here Mahan refers to both the total population and the percentage of personnel engaged in maritime domain operations (occupations that follow the sea), such as shipbuilding or seafaring for their livelihood. He further expands this group to include those with a reserve of wealth to fund maritime expansion and that percentage of the population employed in tasks providing knowledge, skills, and abilities suitable for adaptation to maritime requirements. Mahan assumes that these personnel are available to backfill expanding domain-oriented requirements, acting as a reserve on call in times of need (i.e., general mechanical skills and construction). A nation lacking in population and without a reserve to call upon when needed lacks maritime potential.

[34] Ibid., 44-49.

Character of the people:[35] A nation's cultural and societal disposition toward the domain determines potential. Here Mahan is referring to the aptitude and orientation of people toward the sea. Because seapower is not solely built on naval capacity but also on the extensive pursuit of peaceful maritime commerce, a population focused on pursuing trade over the maritime domain is critical. An economy and national character based upon international trade push people to produce trade goods, encourage investment in means to transport these goods, and are favorable toward investment in the means to defend trade. A people predisposed to trade and exploration is suited for the development of maritime capacity and the cultivation of trade partners, which further strengthens maritime potential. In Mahan's assessment, trade is the key to national maritime power.

Character of the government:[36] Fundamentally, Mahan asserts that for a nation to develop maritime power, its government must understand the value of this particular domain and encourage both its commercial and military development. Understanding and valuing development of the entire field of maritime power enable a government to align its actions with the will and skills of the people by encouraging trade and seafaring pursuits. In order to become a maritime power, the government must continuously focus on development of all aspects of the domain with the conviction that the rewards outweigh the costs. In other words, it should be strategic policy to gain and maintain seapower.

---

[35] Ibid., 50-58. Although clearly the same topic (by numbering and subject matter), Mahan titles the expanded discussion of this attribute "National Character," which differs from "Character of the People" as introduced on page 29. The author has retained the original title here for clarity and because it is much more appropriate, in this author's opinion.

[36] Ibid., 58-89.

Governments encourage the development and growth of trade and seafaring careers as well as those in associated industry through innumerable means, such as trade policy, tariffs, production incentives, treaties, taxes, and more. Under Mahanian theory, national leaders should encourage the creation of large mechanical industries and court extensive trading agreements among allies through centrally coordinated public and international policy, continuously pursuing the strategic aim of creating and maintaining seapower.

While it is true that a mandate can create naval power (i.e., a monarch ordering construction of a navy), Mahan contends that a nation has little hope of gaining or maintaining maritime power without public policy that also encourages the development of commercial power to back it up. In many ways, by carefully constructing regulations and incentives, the government significantly influences how successful a nation is at tapping into the domain power factors previously discussed. Through its actions and policies, it has a say in the percentage of the population focused on maritime trade, and through these same incentives, it develops and shapes the character of its people.

Government influence is not simply restricted to commercial endeavors. During times of military tension, a government too concerned with preserving maritime forces breeds a conservative naval force, one unwilling to exercise command of the sea. Mahan's belief that maritime forces should be offensive in nature eschews this conservative approach, instead encouraging naval forces to engage and seek decisive combat when possible to gain and maintain control over the seas wherever and whenever possible. Over time, nations that favor and

encourage the development of seapower attract more trading partners and develop the ability to carry the goods of other nations by means of a domestic commercial fleet, turning them into maritime leaders, which in turn encourages further domestic maritime development.

Mahan's elements of analysis

From the preceding review of Mahanian theory, we pull several themes regarding the development and use of force in the maritime domain. Consisting of two distinct categories – the use of forces within the domain and the potential to become a domain power – these become our elements of analysis for comparison to other theories and the cyber domain. These elements of analysis are:

1. Domain power depends on the creation and maintenance of both strong military and commercial use of the domain.
2. International trade via a domain is critical to a nation's development of domain power.
3. Lines of communication develop between commercial partners and become sources of strength and vulnerability within the domain.
4. Defense of commercial lines of communication requires and encourages the development of strong military capabilities.
5. During conflict, exercising domain power guarantees one's access to lines of communication in the domain while denying access to one's foe.
6. Destruction of enemy capability to challenge one's access to the domain is critical and achieved through decisive action against enemy forces.
7. A nation must not divide its forces; concentration of force in the domain is necessary to destroy the enemy when the opportunity appears.
8. Geographical position affects a nation's domain power potential.
9. Physical conformation (including natural conditions and climate) determines a nation's ability to access a domain and its incentive to develop domain power.
10. Extent of territory determines a nation's ability to gain and maintain exposure to the domain.

11. The number of population engaged in domain pursuits determines potential and the size of reserves.
12. The character of the people as well as their cultural and societal predispositions affects domain development.
13. The character of the government (and national institutions) determines how effectively domain power is developed and used.

At this point in the analysis, it is apparent that some of the identified categories overlap or are dependent upon each other for domain power development. By casting the analytical net broadly, however, we increase the chance of identifying consistency between this and the following theoretical assessments while searching for critical aspects of domain power theory. This then is the beginning of the process for building cross-theory and cross-domain comparison as reflected in the following table.

Table 2: Maritime Elements of Domain Analysis - Mahan

Maritime Domain Elements of Analysis		
	Mahan	**Corbett**
1	Domain power depends on the creation and maintenance of both strong military and commercial use of the domain.	
2	International trade via a domain is critical to a nation's development of domain power.	
3	Lines of communication develop between commercial partners and become sources of strength and vulnerability within the domain.	
4	Defense of commercial lines of communication requires and encourages the development of strong military capabilities.	
5	During conflict, exercising domain power guarantees one's access to lines of communication in the domain while denying access to one's foe.	
6	Destruction of enemy capability to challenge one's access to the domain is critical and achieved through decisive action against enemy forces.	
7	A nation must not divide its forces; concentration of force in the domain is necessary to destroy the enemy when the opportunity appears.	
8	Geographical position affects a nation's domain power potential.	
9	Physical conformation (including natural conditions and climate) determines a nation's ability to access a domain and its incentive to develop domain power.	
10	Extent of territory determines a nation's ability to gain and maintain exposure to the domain.	
11	The number of population engaged in domain pursuits determines potential and the size of reserves.	
12	The character of the people as well as their cultural and societal predispositions affects domain development.	
13	The character of the government (and national institutions) determines how effectively domain power is developed and used.	

The Theory of Corbett

Julian S. Corbett's *Some Principles of Maritime Strategy* is in many ways a response to the work of A. T. Mahan, and while there are similarities between the two theorists, their works differ in two important ways. Where Jomini and his focus on the processes of war and preparation for war influenced Mahan, Corbett bases his theory on the work of Clausewitz with its integration of military power into overall national security. Corbett's theory, while differing in significant ways from Clausewitz's continental theory, focuses on maritime power against a background of diplomacy, coalitions, and alliances formed before and during times of conflict and executed through policy enacted with consideration to economic, financial, and military considerations.[37]

Born in London, England, the son of a moderately successfully architect and his wife, Corbett (1854–1922) was widely exposed to culture and learning throughout his childhood. Through his parents' efforts to provide him with the advantages of a well-rounded education, he developed a strong intellectual curiosity that prepared him for studies at Trinity College in Cambridge and later in life.[38] Upon graduation from Cambridge, Corbett briefly applied himself as a lawyer before travelling extensively through India and to the United States. These

[37] Michael I. Handel, *Masters of War: Classical Strategic Thought*, 3rd rev. and expanded ed. (London ; Portland, OR: F. Cass, 2001), 203.
[38] D. M. Schurman, *Julian S. Corbett, 1854-1922: Historian of British Maritime Policy from Drake to Jellicoe*, Royal Historical Society Studies in History Series (London, UK: Royal Historical Society, 1981), 3. While specific details are footnoted within this section, unless otherwise noted, generalized details of Corbett's childhood and career presented here are gleaned from Schurman's excellent biography of Corbett.

travel experiences and the exposure to international travel, commerce, and culture they provided was instrumental in providing depth to his writings.[39]

Returning from his travels, Corbett applied himself to writing historical works focused on maritime forces within the context of European history. Although he never served in the Royal Navy, nor ever employed in the maritime field, his historical research into maritime operations exposed him to copious amounts of original source material and first-hand observations regarding the British experience of gaining and maintaining global power without the requirement to develop a strong army. Not only did this academic exposure give him insight into the role maritime forces play in international relations, it also led to an insightful understanding of the mutually supporting nature of land and maritime forces working toward national security goals. Corbett's theory recognizes that during both times of peace and times of conflict, the aims of individual services and government agencies should not be confused with the national policies and best interests of the state.[40]

In the final decade of the nineteenth century, while Corbett was developing his nuanced understanding of maritime operations, the British Royal Navy was undergoing technological, doctrinal, and strategic challenges without clearly defined guidance for development of national policy – a gap Corbett would seek to fill. By 1900, the US Naval War College had been in existence for 16 years, and Mahan's *The Influence of Seapower Upon History* was used as a guide for development of maritime policy and a source of naval theory

[39] Ibid., 7.
[40] Ibid., 21-22. A Clausewitzian approach to identifying that all government actions should support government efforts to provide security for the nation.

worldwide. During the decade after Mahan's publication, technological advances in ship construction resulted in the beginnings of a naval arms race, eventually producing dreadnaughts. In a Mahanian manner, nations sought to build larger and more powerful ships in hopes of wresting control of the sea through decisive combat. Recognizing that great changes were occurring in the maritime domain, the Royal Navy sought to formalize the process of educating its officers by establishing the Naval War Course in 1900, under the direction of Captain W. J. May.[41]

In an historical echo of Mahan's experience, in 1902 Corbett's path to becoming a great naval theorist began when the Naval War College invited him to give a series of lectures. Relying on his historical study of maritime conflict and the development of national power, Corbett produced a series of lectures that focusing on both the development of strategic theory and its application to the Maritime domain.[42] These lectures, as they did with Mahan, helped refine Corbett's arguments and form the foundation of his maritime theory. Where Mahan focuses on the means of gaining maritime power, Corbett focuses on explaining and exploring the effect of naval operations on national security policy. Like Mahan, experiences from the age of sail form the basis for many of his explanations and examples.

Corbett's challenge was to provide strategic instruction to students at the war college while simultaneously teaching the historical context from which these strategic lessons were drawn. From his frustration at having to perform both tasks

[41] Ibid., 32.
[42] Ibid., 33-34.

simultaneously emerged what in many ways is a first draft of Corbett's theory: *Notes on Strategy.* This later became "The Green Pamphlet" and was published in 1906 and handed out to students. His pamphlet was Corbett's first organized attempt to present a historical and logical means of refuting some of the general rules of thumb about maritime strategy clung to by senior naval personnel attending the course.[43] It is this logical and historical analysis that formed the basis for publication of his theory in 1911, titled *Some Principles of Maritime Strategy*.

Most important for purposes of this dissertation, nothing in Corbett's writing indicates disagreement with Mahan's list of characteristics that govern a nation's seapower potential. Furthermore, their writings are both similar in their advocacy of maritime power as a requirement for development of national power.

Where the two men differ is in their approach to the maritime domain's role in grand strategy. Both discuss naval and maritime issues; however, Mahan, heavily influenced by Jomini, focuses more than Corbett on naval operations, the building and employment of naval forces, and the conduct of naval engagement toward achievement of command of the sea. Corbett, who relies heavily on Clausewitz for his inspiration, uses history as a tool to develop and illustrate his theory, like Mahan. However, instead of focusing on naval operations, Corbett

[43] Ibid., 50. "The Green Pamphlet" appears as an appendix in the reprinting of Corbett's 1911 work referenced by the author beginning on page 326; see Corbett, *Some Principles of Maritime Strategy*.

discusses the inter-relationship of naval operations and economic and political concerns; therefore, his theory is more maritime in nature and broader in scope.[44]

Corbett's work is not simply an assessment of how to gain control of the seas; instead, it focuses more broadly on how maritime power affects the balance and distribution of power in the international system. This does not mean he ignores achieving command of the sea. He devotes a significant portion of his writing to identifying the various levels of command a nation might possess – general, local, temporary, and permanent–as well as discussing the conditions under which these types of command are desired.[45]

For Corbett, however, the objective is not simply the defeat of enemy forces. His is a more nuanced treatment of the subject than Mahan's and includes discussion of commercial, economic, and diplomatic elements of maritime power and their use for furthering national security aims – which may or may not require defeat of enemy forces – when combined with efforts in other domains and used in conjunction with other elements of national power.[46]

---

[44] In his discussion of the difference between maritime and naval fields, the historian John Hattendorf points out that from a historical perspective, naval is a subset of maritime. Maritime is an overarching field of study and "deals with the full range of mankind's relationships to the seas and oceans of the world." Hattendorf adds that the maritime field cuts across academic boundaries and links disciplines to form a greater understanding of how history, science, tactics, politics, etc., combine to affect the field. The naval field is a subset of the maritime field. Other subsets and sub-specialties are: geography, cartography, employment of forces, leadership, tactics, etc. The naval model emphasizes naval engagements as a means of achieving national interests such as prestige and power. The maritime perspective is thus a broader view of the same subject. Along the continuum from naval up to maritime, Corbett is the broader of the two theorists. For Hattendorf's full discussion of the maritime vs. naval differentiation, see Hattendorf, "The Uses of Maritime History in and for the Navy," 15-21.

[45] For a summary of these definitions, refer to the appendix of Corbett's work: Corbett, *Some Principles of Maritime Strategy*, 338.

[46] Ibid., 16.

Like Mahan, Corbett places command of the seas at the center of his theory. His treatment of the subject, however, is more situational, defining various types of command, their duration, and their purpose. For Corbett, command of the sea is defined as "control of maritime communications, whether for commercial or military purposes."[47] The normal state of affairs is not one in which one side has command of the sea; instead, the normal state of affairs is an uncommanded sea.[48]

The objective of naval power is to prevent the adversary from gaining command and significantly interfering with one's operations. Corbett's theory focuses on lines of communication, contrasting with Mahan's more general *command of the sea*. Corbett differentiates controlling lines of communication on the maritime commons from controlling those on land because, unlike communication for land forces, lines of communication on the sea are more than military. They are, in his words, "the life of the nation" during both peace and war.[49]

Lines of communication in the maritime commons are more than paths for information; they include commerce, supply, cultural interaction, trade, financing, and the thousands of internal and external transactions that are vital to a nation's economy and well-being. A nation that controls or keeps command of the sea in doubt has the ability to use the domain for its own purpose and exert economic pressure to reduce or eliminate an adversary's power and will to resist.[50] For

[47] Ibid., 94.
[48] Ibid., 91.
[49] Ibid., 94, 100.
[50] Ibid., 102.

Corbett then, the fleet's mission in exercising maritime power is not destruction of the adversary's fleet, as it is with Mahan. Instead, it is to defend and occupy lines of communication. By occupying these lines, friendly forces can use them without interference while preventing adversaries' use of the same lines and allowing the controlling force to monitor the movement of neutral traffic.

Corbett's emphasis on lines of communication leads to a different strategic treatment of the offensive vs. defensive nature of maritime forces than that of Mahan. Where Mahan views maritime forces as inherently offensive in nature, Corbett advocates strategic offensive operations only when the goal is to take something from the enemy.[51] In other cases, he advocates defensive operations to secure something or prevent the enemy from gaining an advantage.

Falling back upon Clausewitz as a guide, Corbett acknowledges that the tactics of individual operations may necessitate offensive or defensive engagements. However, in his view, political objectives at the strategic level should determine the overall nature of forces. Like Mahan, Corbett acknowledges defensive operations as the stronger form of warfare, as they require less force and are therefore the preferred form of war for a weaker power.[52]

Achieving command of the sea, Corbett writes, allows the commanding power to execute limited warfare if it so chooses. Control of the maritime lines of communication enables isolation of either a homeland or theater of operations, limiting the ability of an adversary to escalate the conflict – a state of affairs that gives other elements of national power the time they need to become effective.

---

[51] Ibid., 31-33.
[52] Ibid., 309-11.

Alternatively, if a state is unable to achieve command of the seas, either because it is the weaker naval power or due to other circumstances, it is still capable of disputing command of the sea. Corbett's *fleet in being*, the retention of naval forces with the potential for military operations, is a means of keeping command of the sea in dispute through commerce and coastal raiding to prevent the enemy from gaining the strategic initiative.[53] By continuing to contest command of the seas, a nation keeps its options open and gives other levers of national power the opportunity to become effective, Corbett suggests.

Corbett, like Mahan, addresses the importance of geography by highlighting its relation to lines of communication relevant to conflict and trade. Obvious geographic chokepoints or other areas where lines of communication converge take on significance because they are the richest positions from which to deny an adversary use of the lines of communication and also the most vital to protect or, as a minimum, deny the adversary an opportunity for control.[54]

Like Mahan, he addresses the effect of the geographic disposition of a nation and its influence on that nation's maritime strategy and potential. A coast with widely distributed ports is difficult to control and forces the opposing side to monitor each point of access in order to be able to quickly exercise control of the sea when necessary.[55] If left unmonitored by a blockading force, these points of access to the maritime domain can sustain national life via trade and contest control of the sea through naval action.

---

[53] Ibid., 165-66.
[54] Ibid., 105-06. By way of example, he specifically mentions the maritime chokepoints of Finisterre, Gibraltar, Suez, the Cape of Good Hope, and Singapore.
[55] Ibid., 151-52.

Corbett discusses two types of blockade for use to control opposing forces' ability to use and contest the lines of communication: commercial and naval. The use of these blockades is dependent on the political objective, whether it is preventing an adversary from using the domain to maintain national life (commercial), or preventing him from exercising control of the sea (naval). These two forms of blockades are further broken down into two categories: closed and open.[56] In a closed blockade, the enemy fleet is bottled up in port, unable to challenge for command of the sea or gain access to the domain for other purposes. When facing a closed blockade, the enemy must either accept this state of affairs or fight to break the blockade.

In an open blockade, the occupation of lines of communication force the enemy to forgo use of the domain or risk its fleet by spreading its forces out to protect traffic transiting the domain from interdiction, which leaves these forces vulnerable to decisive engagement. Open blockades are a means for a superior force to draw an inferior force out for battle, by making it costly for that force to remain in port. Despite inferiority, the weaker force must sortie forth to protect maritime traffic sailing upon its lines of communication. Regardless of which form of blockade is instituted, for Corbett, a naval blockade is the means of gaining command of the seas, and a commercial blockade is the means of exercising it.[57]

Corbett's most important maritime domain objective is protection of friendly lines of communication, unlike Mahan, who advocates destruction of the

[56] Ibid., 183-88.
[57] Ibid., 183.

enemy's fleet. For this important task of protection, Corbett advocates the use of cruisers, naval units that are smaller, swifter, and more maneuverable than battleships yet sufficiently strong to perform interdiction operations and deter or counter adversary commercial raiding on their own.[58] The vastness of the maritime domain requires numerous cruisers to exercise command, while the heavy fleet and its more costly battleships are necessary only due to the numbers required to secure control of the domain. It is the fleet's job to prevent adversaries from interfering with cruisers by concentrating quickly when required to engage the enemy. Built in greater numbers than the battleships, cruisers are the means by which a force exercises its domain control.

With a basic understanding of Corbett's theory, this discussion now moves on to identifying the principal themes in Corbett's theory of maritime power. Each of these themes or propositions represents Corbett's approach to development and utilization of maritime forces. While they are less clearly defined in his text than Mahan's list of requirements to create maritime power, they are no less important because they speak more clearly about the role maritime domain power has in dictating the distribution of power in the international system and the use of the domain at the strategic level.[59]

Subset of integrated national power: Maritime operations and power are a subset of national power and must be developed and used efficiently without

---

[58] Ibid., 114. Corbett's focus on cruisers is in contrast to Mahan, who focused on creation of heavy ships (battleships) capable of defeating the enemy naval forces.

[59] Klein, "Corbett in Orbit: A Maritime Model for Strategic Space Theory," 66-69. The following list of elements of analysis is inspired by a list of aspects for spacepower theory Klein presents in the referenced article. This article served as much of the outline for not only these elements of analysis but also the review of Corbett above.

wasting effort unnecessarily to gain control of the domain for its own sake. Maritime domain theory is part of an overall strategy to gain and maintain advantage over adversaries during periods of peace and war, both commercially and militarily, using the entire DIME. Because the maritime domain is the medium through which much of the nation's DIME actions are pursued, maritime power is an important factor in determining the potential for wealth and national power that a state has and how overall power is distributed within the international system.

Command of the domain: Command of the maritime domain rests with control of communications within the domain. The maritime domain is valuable to a nation because of the communications that occur through this commons – it has no value of its own (unlike land territory). Maritime domain operations are valued for their effect on efforts to gain command of the domain directly or prevent an adversary from gaining command of the domain either temporarily or permanently.

Domain communications: Lines of communications within the maritime domain are vital to national life. In addition to the movement of information, these avenues are important to trade, finance, diplomacy, movement of raw materials, and movement of personnel. A successful effort to restrict the ability of another nation to use lines of communication influences all aspects of their DIME, hampering their ability to pursue national security objectives. The primary purpose of maritime warfare is to secure an adversary's lines of communications. If an enemy force is capable of denying one's use of these lines of

communications, one must render it incapable of interfering with these operations – but not necessarily destroy it.

Offensive operations: A nation uses offensive operations when the political objective is to take something away from an adversary. Offensive operations, as the weaker form of warfare, are usually the course of action for the stronger maritime force. The enemy's ability to retreat to areas of safety complicates offensive operations by denying decisive battle and keeping control of the domain in doubt. Attempts to root out these enemy forces for destruction may prove more costly in effort and materials than simply maintaining control of the domain.

Defensive operations: A nation uses defensive operations when the political objective is to prevent an enemy from gaining an advantage or achieving one of its political objectives – in other words, denying the enemy its desired goal. Defensive operations are inherently the stronger form of warfare, much as they are on land. It is difficult for a stronger power to force decisive conflict in the maritime domains as long as the weaker force has the option of remaining in safety.

Isolation and limited war: A nation with enough maritime power and favorable geographic positioning can isolate itself from counterattack and is even capable of isolating a distant region of conflict. Isolation limits an adversary's ability to successfully escalate a conflict or reinforce in-theater operations. As Corbett says, command of the domain allows a nation to dictate escalation of the war, taking as little or as much of it as necessary. If a nation is unable to isolate

itself and its interests from adversaries, it is less likely to be able to limit escalation of the conflict.

Contesting command of the domain: Weaker forces can continue to achieve political objectives by retaining the capability to contest command of the sea. Taking advantage of the difficulty in maintaining continuous command over a vast commons, the weaker force can seize temporary and/or localized control to achieve political objectives such as disruption of trade or alliances. Simply retaining this power, Corbett's *fleet in being*, maintains the ability to threaten communications in the domain, tying up the resources of the stronger power disproportionally to the actual threat it poses.

Positioning and geography: Strategic positioning along lines of communication provides nations the ability to control the use of the domain for all DIME purposes. Internal lines of communication aid a nation by helping it isolate itself for defense, ideally allowing limited warfare. Regardless of home-front geo-location, control of strategic positions allows the exercise of command of the sea in a way that either forces an adversary to contest command or accept the limitations it places upon its ability to exercise power through it – limiting its "national life" in the domain.

Access to the domain: Corbett's closed and open blockades are two approaches to a strategic problem. Closed blockades prevent the enemy from accessing the domain and using lines of communication for purposes of the DIME. Preventing an adversary's ability to access the domain at the port of origin creates a closed blockade. Closed blockades provide an enemy with the option of

either accepting loss of the domain as a tool for national security purposes or choosing to expose its forces in order to challenge command of the sea. A closed blockade requires the blockading nation to commit sufficient strength to the endeavor to be constantly ready to engage enemy forces; it is reserve-intensive.

An open blockade, which emphasizes interference with an adversary's ability to use the domain, operates by occupying and interdicting distant lines of communication to draw the adversary into action by forcing it to divide its fleet in support of units transiting the domain. Because the blockading fleet can choose when and where to engage, division of the adversary's maritime power provides an opportunity for selective decisive engagement, potentially strengthening the blockading nation's command of the sea.

Nature of forces: The types of forces necessary to gain and then exercise command of the maritime domain differ from each other. Corbett's cruisers are a class of combatant specializing in exercising command of the sea through control of the lines of communication. They are strong enough to operate independently, deterring commerce raiders, while fast and flexible enough to engage in interdiction when necessary. Battleships, the heavy artillery of the fleet, are required to deter and defeat enemy battleships and cruisers, thus providing the command of the sea within which cruisers operate. Battleships are not suited to the fast work of exercising command of the sea and are too resource-intensive to build and maintained in large enough numbers to cover the expanse of the maritime commons. Cruisers are therefore the more important, numerous, and economical of the two types of force and should form the bulk of the fleet.

Dispersal of forces: Exercise of control over the maritime commons requires forces capable of dispersing to cover far-flung lines of communication. These widely dispersed forces should contain enough power to protect national interests by defending lines of communication from raiding and denying use of those lines of communication to adversaries. These dispersed forces exercise control through independent action, but must also retain the ability to concentrate quickly should the opportunity for decisive combat appear or be forced upon them by the enemy fleet.

Corbett's elements of analysis

As guidance for gaining and exercising control of a commons, the propositions from Corbett presented here form the basis for elements of comparative and cumulative analysis between theories. Each provides insight into the problems of gaining and exercising control of a large and dispersed international commons. The elements of analysis we take from Corbett are:

1. Domain power is a subset of integrated national power; political considerations to strengthen all elements of the DIME during times of both peace and war guide its use.
2. Command of a commons lies in control of the lines of communication within it, either temporarily or permanently.
3. Lines of communications are the vital pathways by which nations sustain their life and pursue national power (whole of DIME) in a global commons.
4. Offensive operations wrest control from an adversary; they are the purview of the stronger force but are complicated by an adversary's option to deny engagement, thus keeping command in doubt.
5. Defensive operations deny an adversary its intended purpose and are inherently the stronger form of action, often the option of the weaker force.
6. Isolation allows a nation controlling the commons to dictate a conflict's degree of escalation to match its political goals.

7. Being uncommanded is the natural state of global commons – weaker forces retain the ability to disrupt and challenge stronger forces locally and for short durations.
8. Control of geopolitically strategic points where lines of communication converge, such as geographic chokepoints, are critical to gaining and exercising command of the domain.
9. Denying an adversary the use of a domain can occur through either prevention of entry or harassment while transiting lines of communication.
10. To control a commons, a nation must be capable of both gaining and exercising command of the domain – exercising command is the more critical of the two.
11. Forces exercising control of a commons must be capable of rapidly massing to engage in decisive action when and where control is threatened.

From the preceding review of maritime theory, we have 24 elements of analysis as we move forward to discuss the air domain. There are two distinct categories of elements of analysis taking shape. The first are requirements for developing national power in the domain. Consisting of both naturally occurring factors, such as the nature of a coastline or global positioning, these preexisting factors determine a nation's latent domain power potential. The second are factors over which nations have some degree of control, consisting of societal values and governmental policy toward the development, maintenance, and use of power within the domain. The full list of maritime elements of analysis follows in tabular form below and in Appendix I.

Table 3: Maritime Elements of Domain Analysis - Corbett

Maritime Domain Elements of Analysis		
	Mahan	**Corbett**
1	Domain power depends on the creation and maintenance of both strong military and commercial use of the domain.	Domain power is a subset of integrated national power; political considerations to strengthen all elements of the DIME during times of both peace and war guide its use.
2	International trade via a domain is critical to a nation's development of domain power.	Command of a commons lies in control of the lines of communication within it, either temporarily or permanently.
3	Lines of communication develop between commercial partners and become sources of strength and vulnerability within the domain.	Lines of communications are the vital pathways by which nations sustain their life and pursue national power (whole of DIME) in a global commons.
4	Defense of commercial lines of communication requires and encourages the development of strong military capabilities.	Offensive operations wrest control from an adversary; they are the purview of the stronger force but are complicated by an adversary's option to deny engagement, thus keeping command in doubt.
5	During conflict, exercising domain power guarantees one's access to lines of communication in the domain while denying access to one's foe.	Defensive operations deny an adversary its intended purpose and are inherently the stronger form of action, often the option of the weaker force.
6	Destruction of enemy capability to challenge one's access to the domain is critical and achieved through decisive action against enemy forces.	Isolation allows a nation controlling the commons to dictate a conflict's degree of escalation to match its political goals.
7	A nation must not divide its forces; concentration of force in the domain is necessary to destroy the enemy when the opportunity appears.	Being uncommanded is the natural state of global commons – weaker forces retain the ability to disrupt and challenge stronger forces locally and for short durations.
8	Geographical position affects a nation's domain power potential.	Control of geopolitically strategic points where lines of communication converge, such as geographic chokepoints, are critical to gaining and exercising command of the domain.
9	Physical conformation (including natural conditions and climate) determines a nation's ability to access a domain and its incentive to develop domain power.	Denying an adversary the use of a domain can occur through either prevention of entry or harassment while transiting lines of communication.
10	Extent of territory determines a nation's ability to gain and maintain exposure to the domain.	To control a commons, a nation must be capable of both gaining and exercising command of the domain – exercising command is the more critical of the two.
11	The number of population engaged in domain pursuits determines potential and the size of reserves.	Forces exercising control of a commons must be capable of rapidly massing to engage in decisive action when and where control is threatened.
12	The character of the people as well as their cultural and societal predispositions affects domain development.	
13	The character of the government (and national institutions) determines how effectively domain power is developed and used.	

This completes our review of maritime theory. The application of steam engines and steel hulls to the maritime domain expanded its use, making it a significant factor in creating national power. The application of modern technology to the air domain had a similar effect, opening that domain to international competition. We now move on to a discussion of aerial theory as presented by three of the seminal airpower theorists: Douhet, Mitchell, and De Seversky. As we will see, they were not only challenged with creating a theory for the use of airpower but also with providing justification for developing the domain as an element of national power.

Chapter 5: Airpower Theory

This chapter transitions from the maritime domain to discussion of the air domain and the theoretical models developed to address not only its nature as a global commons but also its unique overlying nature. As with the discussion of maritime theory above, this process focuses on analysis of the most prominent theorists from the early days of the domain's development. While no single air theorist has emerged who presents a comprehensive work to rival the landpower theory of Clausewitz or the seapower theories of Mahan and Corbett, there are three air theorists who have emerged as the leading voices on airpower thought: Air Marshal Giulio Douhet, Brigadier General William "Billy" Mitchell, and Alexander P. de Seversky.[1] Of these three, Douhet and Mitchell are the founding fathers of airpower theory development, producing seminal works from which later thinkers refined and adapted policy and doctrine. Douhet developed and championed the first airpower theory in his work *The Command of the Air*.[2] Writing shortly after Douhet, Mitchell similarly championed early airpower development. A few years later, Seversky packaged and refined Mitchell's and Douhet's thoughts, carrying them into the modern era, validating and adapting

[1] Harold Winton points out that there is no codified and systematic airpower theory due in part to the complexity of the air domain and its influence on the other operational domains and a lack of extensive historical experience from which to draw. Harold R. Winton, "A Black Hole in the Wild Blue Yonder: The Need for a Comprehensive Theory of Air Power," *Air Power History* Winter, no. 39 (1992): 32.

[2] Col Phillip S. Meilinger, USAF, Retired, ed. *The Paths of Heaven: The Evolution of Airpower Theory* (Maxwell AFB, AL: Air University Press,1997), xiii. Writing about: Douhet, *The Command of the Air*.

their concepts with the benefit of events during the early years of World War II (WWII).

All three of these writers formulated and wrote their theories of airpower during the early days of air domain development, the time between World War I (WWI) and the end of WWII. During this three-decade period, the pace of technological development in aircraft design transitioned the air domain and airpower from one of curiosity to one of vital importance for national security. Each of the three theorists developed an airpower theory focused on winning conflicts from the air by first gaining command of the air and then attacking vital enemy centers of gravity in order to force capitulation. The speed and maneuverability of air forces, relative to surface forces, provide unique offensive capabilities based on freedom of maneuver and the ability to bypass enemy defenses.

Douhet and Mitchell first identified these characteristics and sought to inject airpower into national strategic thought. Emphasizing the global nature of the air domain, Mitchell declared, "As air covers the whole world, aircraft are able to go anywhere on the planet … [and] have set aside all ideas of frontiers."[3]

Today similar statements can arguably be made of cyberspace and the electromagnetic spectrum. Mitchell's ideas focused American airpower theory and subsequent airpower theorists on the independent war-winning capabilities of aviation. It was his belief that the first battles of any future war would be air battles. The nation winning them would be practically certain to win the whole

[3] Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*, 4.

war, because the victorious air service would be able to operate without hindrance.[4]

An acquaintance and colleague of Mitchell, Seversky expanded and modernized early air theory, advocating the creation of long-range power projection using integrated domain control and force projection capabilities. His writings on air theory stress the necessity of preparing for air warfare and the necessity of establishing air dominance over the world in much the same manner as England dominated the seas in earlier centuries.

Like the maritime power theorists in the previous chapter, these three theorists developed their ideas in response to technological developments that suddenly opened the domain to new and expanded use. Each sought to guide national policy in developing domain power as a means to ensure national security. Unlike the maritime theorists, however, the air domain theorists were unable to reference a deep well of historical precedence and experience from both peacetime and war; there was no age of sail equivalent from which to draw fundamental lessons and identify critical principles. Instead, early airpower theorists had to rely on the relatively thin airpower experiences of WWI and make assumptions about future technological developments in the domain. In many ways, these early theorists were in a similar position to that of modern cyber theorists today. How they dealt with this limitation and the theories they developed as a result provide insight into contemporary cyber theory development. Each of these theorists and the vision of air domain power they

[4] ———, *Our Air Force, the Keystone of National Defense* (New York, NY: E.P. Dutton & Company, 1921), xix.

espoused informed and guided the transition of national security policy into the centrally coordinated, modern multiservice design we see in most nations today.

In keeping with the precedence of the previous chapter, this chapter addresses each theorist individually in the order of theory formulation.[5] Pulling elements of comparison from each theory, this process builds a list of airpower elements for comparison for use during a cross theory assessment in Chapter 6. Airpower theory developed simultaneously with the age of modern media, characterized by mass printing and wide distribution of articles via professional journals, newspapers, periodicals, and even radio interviews. Each of these theorists published and spoke extensively on their views and a complete detailing of each theorist and the evolution of their works over decades is beyond the scope of this work. Narrowing down the volume of their writings for consideration, this dissertation focuses on the major propositions from each theorist, reflected in their most enduring work. This assessment uses Douhet's theory from his work titled *The Command of the Air*.[6] Billy Mitchell's work of reference is *Winged Defense: The Development and Possibilities of Modern Air Power Economic and Military*.[7]

---

[5] Douhet originally released *The Command of the Air* in 1921 and updated it, refining the role of airpower, combat aircraft, and organization of national defense in 1927. The 1927 version is used here because it is the more mature version of this work. Although this version postdates Mitchell's writings, the basic theory of Douhet was formed and published in the 1921 version. Douhet is almost universally considered to be the first theorist to think deeply on airpower and commit his thoughts to writing. The influence of Douhet on Mitchell is the subject of some debate among scholars. It is undeniable, however, that many of the early airpower theorists were simultaneously developing their theories in exposure to each other's thoughts.

[6] Douhet, *The Command of the Air*. The text referred to here is a reprint of the 1927 version of Douhet's text as translated by Dino Ferrari and published in 1942, New York, by Coward-McCann. This version is a second edition.

[7] Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*. This version, used in my research, is an unabridged version of the original 1925 publication.

Finally, the work of Alexander de Seversky referenced here is *Victory Through Air Power*.[8]

This chapter begins with a review of the air domain and its key characteristics necessary for framing discussion of relevant airpower theories. It then assesses each author's theory, briefly discussing the relevant events shaping the theorist's perception of the domain in order to provide background and context for the work. With an understanding of each author's purpose and intent, discussion of the individual theory identifies elements of analysis for comparison in Chapter 6.

The air domain

The air domain, first opened to manned powered flight on December 17, 1903, has taken its place alongside the maritime domain as a vital part of any national security discussion. It is truly a global domain, overlying all other domains from the surface to the edge of space. Over the last 100-plus years of development, this domain's exploitation has influenced all four elements of the DIME (Diplomatic, Informational, Military or Economic), especially the military instrument of power. Airpower theorists, in developing their theories, had the novel challenge of simultaneously addressing both the development of domain power and projection of power from the air domain into the other domains.

Unlike the land or maritime domains, which have relatively well-defined borders and a limited ability to interact with each other, the air domain provides

[8] De Seversky, *Victory Through Air Power*. The version used for my research is an original copy, donated to the author's personal collection by Col. Raymond O'Mara to whom I am indebted.

direct access to virtually any point on the land or maritime domains, bypassing traditional defenses and borders. The air domain is free of geographic boundaries that define chokepoints and lines of communications on the land and within the maritime commons.[9] This increased access and interaction was unique at the time and plays a central role in airpower theory.

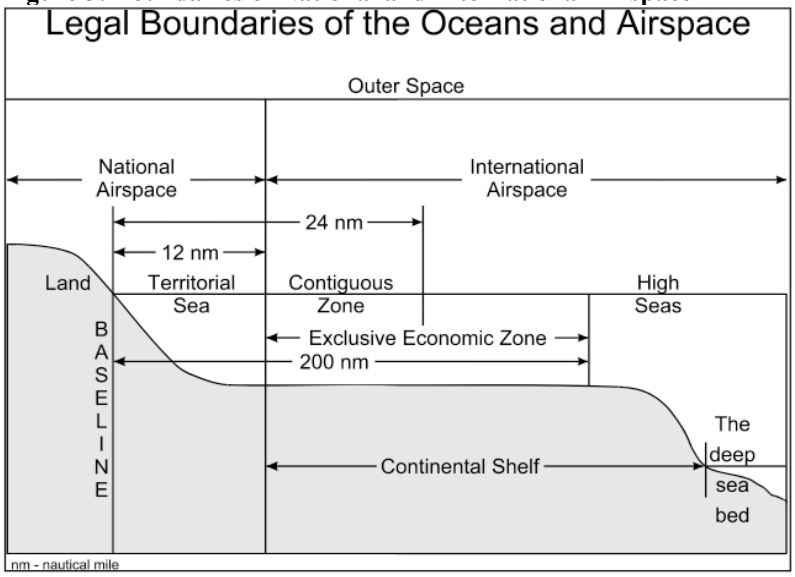
Another challenge faced by our theorists was the requirement to account for the decreased importance of distance and time because of speed and flexibility in airborne operations. This is not to say that time and distance become irrelevant, but that in their writings the theorists had to address these traditional planning factors less as barriers to interaction and more as limitations to be accounted for during domain operations. For example, physical limitations on aircraft range and performance provide restrictions on domain use. In other words, geography still matters, but rather than predictable chokepoints, it requires the creation of manmade chokepoints such as airports and international flight routes. These points of access to the domain serve to provide predictable, but not mandatory, lines of communication within the domain itself.

[9] During the early years of aviation development, aircraft were unable to overfly large mountain ranges, making this statement more applicable today than during the times in which our subject theorists wrote. These theorists, however, foresaw the day where high-altitude flight would remove the few remaining geographic restrictions on possible lines of communication.

Like maritime domain operations, entry into the air domain requires the use of technology. One significant difference is that dominant air technology provides for limited visits to the domain. Aircraft must return for refueling much more often than ships at sea. Keeping this in mind is important when comparing the use of force between the two domains. Blockade operations at sea rely on an extended presence that is impossible to replicate in the air.[10]

Like the maritime domain, airspace is a global common, subdivided into controlled and uncontrolled zones. Portions of the air commons over international territory remains uncontrolled, while those areas closer to national borders are governed by international agreements and customs developed to provide order to traffic and nations the ability to monitor and control access to their borders. The laws and customs of air domain control began in 1919 with the *1919 Paris Convention* and evolved over time to reflect modern uses of the domain for trade, commerce, and

Figure 3: Boundaries of National and International Airspace



[10] Maritime tethering to operating locations such as ports is much less significant than airpower assets, which must constantly fly between designated facilities and be conscious of the affect of weather not just within their immediate location but also at their intended destination.

national defense. The December 7, 1944, signing of the Convention on International Civil Aviation created the basis for modern international airspace law. In function, this convention is similar to the Law of the Sea treaty discussed in the previous chapter.[11]

While the details of international law concerning airspace control are largely outside the scope of this research, it is interesting to note that as within the air domain, international law provides for two types of airspace: national and international.[12] Nations exercise sovereignty over the airspace above their territory and along their borders; designated as national airspace. Unlike maritime custom, aircraft wishing to transit national airspace or enter it from international airspace do not enjoy rights to freedom of passage. Before entering, they must first request permission to enter and transit.[13] Outside of national airspace, aircraft, like ships upon the maritime domain, are free to operate without interference from other nations. Regardless of a line of communication's location, all traffic within the domain share its use (see Figure 5.1 for a graphic breakout of airspace over the maritime and land domains).

[11] Today the International Civil Aviation Organization (ICAO) monitors implementation of the conventions on airspace, coordinating and standardizing use of the domain.
[12] U.S. Department of Defense, "The Commander's Handbook on the Law of Naval Operations," 1-10.
[13] "Convention on International Civil Aviation," (1944).

Douhet

Background

Air Marshal Giulio Douhet, widely considered the seminal author and advocate of airpower, was born May 30, 1869 near Naples, Italy.[14] Born into a family of soldiers, teachers, and journalists, he grew up with access to education and an exposure to life in the military. He was a good student, graduating first in his class at the Genoa Military Academy and commissioned at age 19 as an artillery officer in the Italian Army. While serving, Douhet continued his education at the Polytechnic Institute in Turin, focusing on science and engineering, where he once again demonstrated his academic excellence when his thesis became a standard text at the school.[15]

Assigned after graduation to the Italian Army General Staff, he began to study and write on the role of technology in the military. During this time, the mechanization of military forces was a hotly debated issue among military professionals. Douhet came down firmly on the side of those in favor of mechanization, coming to see it as a way to overcome Italy's relative resource and manpower deficiencies when compared with other European continental powers. The use of mechanization to advance Italian national security at the lowest

[14] While many biographies, articles, and biographies provide background on Douhet, much of the presented here the author draws from research by Phillip Meilinger, a modern airpower historian, and thinker of note. Of particular use in preparing this section were Col Phillip S. Meilinger, USAF, Retired, *Airwar: Theory and Practice*, Cass series – studies in air power (Portland, OR: Frank Cass, 2003), and ———, *Airmen and Air Theory: A Review of Sources* (Maxwell Air Force Base, AL: Air University Press, 2001).
[15] ———, *Airwar: Theory and Practice*, 7-8.

possible cost is something he continued into his justification for his advocacy of airpower later in life.

In 1905 Italy entered the airpower age with the flight of its first dirigible, an event quickly followed by the 1908 acquisition and flight of its first airplane. With a ringside seat to these events, the technology-oriented Douhet quickly predicted that with the arrival of the airplane, the skies would become a battlefield of the future.[16] His belief in the correctness of this prediction and his advocacy of developing Italian airpower led to clashes with his superiors that would define the remainder of his life.

Douhet's prediction that the air domain would become a medium for conflict became reality in 1911 when Italy and Turkey went to war over Libya, a conflict that saw the first use of aircraft for reconnaissance, artillery spotting, transportation of supplies, transportation of personnel, and daytime and nighttime bombing.[17] Remarkably, most of the traditional roles of airpower we see today were all present during its first year of combat operations.

When the war in Libya ended, Douhet, already developing a reputation as an airpower advocate, received a tasking to write Italy's report on the meaning of the Libyan war for the future employment of aircraft for the Italian Army. This assignment led him to think deeply not only about the combat effectiveness of

---

[16] Meilinger intimates that Douhet predicted this soon after he became interested in aviation, something this author was unable to confirm. The opening sentences of his airpower theory as reflected in *Command of the Air* would, however, seem to confirm this sentiment: "Aeronautics opened up to men a new field of action, the field of the air. In so doing, it of necessity created a new battlefield; for wherever two men meet, conflict is inevitable" (Douhet, *The Command of the Air*, 3.) Meilinger's assessment is echoed in an earlier work: Louis A. Sigaud, *Douhet and Aerial Warfare* (New York, NY: G. P. Putnam's Sons, 1941), 19.

[17] Meilinger, *Airwar: Theory and Practice*, 8.

aircraft but also the organization and equipment of airpower forces. Recognizing the interrelation of civil and military development, at this early stage in his development of airpower theory, he began calling for the development of domestic industry in order to increase commerce and national security.

By 1912 Douhet's military career had advanced, placing him in command of an Italian aviation battalion. In this role, he continued to develop airpower thought by authoring an operational manual for the Italian Air Force entitled *Rules for the Use of Airplanes in War*, perhaps the first written guidance on the use of airpower during conflict. He did not produce this guidance without controversy. Characteristic of the difficulties that airpower advocates faced in overcoming entrenched schools of military thought, his superiors labeled him a radical and made him alter the document to remove all references to aircraft as a weapon, eventually exiling him to the infantry.[18]

Despite this exile, the outbreak of WWI found Douhet continuing to argue for a buildup of military aviation. By now a full colonel, he took it upon himself to write to superiors and government officials, arguing that Italy's lack of airpower emphasis flawed its approach to conducting the war. His public refusal to back down from his criticism eventually earned him a court-martial in 1916 and a one-year jail sentence. Despite this conviction, Douhet's airpower expertise was recognized and increasingly valued. Upon his release, Douhet became the Central Director of Aviation at the General Air Commissariat but quickly become dissatisfied with government service, retiring in 1918.

---

[18] Ibid., 9. Instead of labeling *weapons*, Douhet was required to label them *devices*.

Shortly after his retirement and the end of WWI, postwar analysis discovered that Douhet's criticisms regarding the government's conduct of the war had largely been correct, overturning his court-martial. Despite the restoration of his reputation and an accompanying promotion to General Officer, he did not return to active service, instead preferring to continue writing on airpower theory as a civilian advocate, completing and releasing his first edition of *Command of the Air* in 1921.

Douhet formulated and published his theory during the very early days of aviation, basing it upon his conclusion that WWI demonstrated the inevitability of total war, characterized by an unbreakable stalemate on the ground.[19] This belief animated his passion for airpower, which he viewed as the only means to restore mobility to modern warfare by overflying trenches and natural features on the ground to strike at the enemy. Douhet did not advocate for airpower as a replacement for surface forces, but instead as a means of obtaining the most return possible on the smallest investment in national security.[20]

In making this case, his challenge was multifaceted. He sought to educate ill-informed civilian and military personnel regarding the potential of airpower while simultaneously formulating a theory of airpower to guide development of national power in the new domain, all in the face of institutional and bureaucratic resistance to the diversion of resources and power from existing interest groups.

---

[19] ———, *Airmen and Air Theory: A Review of Sources*, 103.
[20] Sigaud, *Douhet and Aerial Warfare*, 21.

Theory

Drawing from the sparse but remarkably diverse use of airpower in Libya and during WWI, Douhet formulated a theory of airpower that does not lay out specified propositions for use in developing airpower but nevertheless influenced the development of European airpower during the interwar years.[21] From his observations and assessment of the use of military force in WWI, he draws the following five premises about future conflict:[22]

1) The war of the future will involve all nations and their resources.
2) Victory will go to the side that first succeeds in breaking the material and moral resistance of the adversary.
3) The nation whose armed forces most correctly identify what war will be like and train to meet its requirements will be the most successful.
4) War on land will be static in nature due to the increasing power of defensive arms.
5) Within the maritime domain, forces will fight a war of attrition until one side gains command of the domain, denying its access to the adversary.

Douhet recognized that modern war will be total war and predicted that like WWI, attrition-based struggles between surface forces will characterize future conflict. He sees airpower as a means to bypass the carnage of ground combat and forgo the maritime struggle promised in premises four and five above by returning mobility and decisiveness to conflict. However, his vision can only become a reality if a nation's decision makers accepted the future totality of war,

---

[21] Translation of Douhet's works into English and released in North America during the interwar period did not occur, casting doubt on their influence over Mitchell who wrote in the US during this period. They were, however, very influential in Europe, published in both Italian and French, influencing the development of the British RAF and the thinking of German military officers developing the Luftwaffe. See ibid., 16-17, and Meilinger, *Airwar: Theory and Practice*, 29-30.

[22] The list presented here the author paraphrased and adapted from Douhet's list. His list in *Command of the Air* follows a review of the characteristics of fighting on the land and sea during WWI. For the original list see Douhet, *The Command of the Air*, 175-7.

recognizing that the most efficient path to victory lies in the breaking of an enemy's means, and will to resist.

The heart of Douhet's airpower theory revolves around the absolute requirement for a nation to gain and maintain command of the air domain. Without command of the air, all other efforts to defend territory or pursue national security interests remain vulnerable to enemy actions. In his writings, he justifies this guiding principle through the exploration of several tenets of airpower: its ability to bypass fielded forces, speed, mobility, destructive nature, freedom from geographic restrictions, and ability to strike directly at the enemy's rear. Douhet wrote for a very clear purpose: to convince his audience that the development of airpower has forever changed warfare. Douhet's theory works to convince the reader that it is not the new technology of aircraft that changed warfare; it is the opening of the new domain. He wrote to demonstrate to military and civilian leaders the necessity of exploring and developing this new domain in order to understand how it affects the conduct of warfare.

> "To have command of the air means to be in a position to prevent the enemy from flying while retaining the ability to fly oneself."[23]

Even in the face of resistance from land and sea advocates bent on redirecting materials toward strengthening their own forces, Douhet set out to demonstrate that with the opening of the air domain, the nature of warfare has changed, altering the role of surface forces. No longer is the struggle between opposing armies working to subdue each other or naval forces competing for dominance. Through the air domain, a nation can bypass even the strongest

[23] Ibid., 25.

surface defense, Douhet theorizes, a proposition that threatened established land and maritime interests by calling into question their relevancy as decisive factors in warfare. For Douhet it is not a question of relevance, but simply that because technology enables use of the air domain, future battles between nations will be between peoples, not armies. The conclusion he hopes his readers will reach is that whole nations must be prepared to fight or to endure the consequences of fighting, regardless of where they are located in relation to the front lines. The real target of national struggles is therefore the will of the enemy population to continue accepting punishment to personnel, industry, and society inflicted from the air.

From Douhet's perspective, punishment of civilian populations is an unquestioned reality during future conflicts. The ability to bypass fielded forces and strike at what he terms "vital centers," such as industrial and governmental centers of power, blurs the lines between military and civilian personnel. The expansion of the war into three dimensions reduces the importance of distance and geography to operational planning and means that there are no defendable front lines, demarcated forward and rear areas, or vulnerable flanks.

> "Only the airplane can travel without restriction over the whole surface of the globe, needing only a point of departure and one of arrival."[24]

The speed with which air forces can appear and strike not only opens the entire nation to the ravages of war; it also complicates and confounds attempts at defending against air attack. An attacker can strike anywhere, at any target, using virtually any avenue of approach (line of communication) to transit to and from a

[24] Ibid., 77.

target area. This is not to say that Douhet did not envision chokepoints, just that geography does not play the same role in defining them as it does for the maritime theorists in Chapter 4. Areas of domain access – the airfields, for instance – become critical areas for targeting and defense. The same holds true for industrial and governmental centers vital to a nation's will and/or capability to resist. Defending these target types is necessary; they are targets for offensive operations by your air forces as they will be for your adversaries.

Using air forces to gain command of the air by targeting enemy airfields is a necessary first step to victory in any conflict and may be an appropriate first strike target in order to take an adversary by surprise. Airfields are targets for Douhet's first waves of attack. Destroying them prevents the enemy from accessing and using the domain. Once the enemy can no longer challenge for command of the air, a nation can freely target industrial and governmental centers to reduce a nation's will and ability to fight.

After gaining command of the air, a nation can begin the task of wearing down the enemy's will to fight without suffering the same destruction it is visiting on its foe. The difficulty in defending all a nation's vital points, Douhet points out, is that because the entire territory of a nation is open to attack, the number of sites requiring defense makes the task practically impossible.[25] The near impossibility of defense makes air forces inherently offensive in nature.

[25] He failed to foresee the effectiveness of surface based air defense, and because he wrote before the advent of radar and other early warning systems, he underestimated the ability of defensive air to find and engage attacking forces. Without forewarning of an attack, in order for an adversary to create an effective defense, it would have to defend everywhere in strength, a strategy that simply cannot be resourced.

Taken to an extreme, Douhet envisions that in the future, command of the air may be sufficient to end a conflict; nations might capitulate rather than suffer the inevitable destruction of their economic and social infrastructure. Airpower's offensive nature means that the only viable defense then becomes a strong offense.

Success for Douhet therefore depends on gaining command of the air. The decisiveness of any effort to gain command, he suggests, depends on:[26]

1) The abundance of aerial power a nation has
2) The level of technological and operational surprise a nation possesses
3) The relative strength of an adversary's airpower
4) The adversary's plans to use airpower in the conflict

In order for a nation to develop decisive airpower, Douhet suggests the development of two distinct types of air forces: combat and reconnaissance.[27] The type of combat power he envisioned is what we would consider today as heavy bombers capable of taking the fight directly to the enemy population and providing for their own airborne defense. Douhet's belief in the efficiency of these battle planes leads him to conclude that the diversion of resources into production of fighters is a waste of resources that can be better spent strengthening offensive capabilities and bolstering national will to continue resistance in the face of an attack. The one exception to investing in heavy combat

---

[26] Louis A. Sigaud, *Air Power and Unification: Douhet's Principles of Warfare and Their Application to the United States*, 1st ed. (Harrisburg, PA: Military Service Pub. Co., 1949), 60.

[27] Comparing the 1921 and 1927 version of *Command of the Air* reveals a change in Douhet's thinking, either a maturation of his thinking or a freedom to express a long-held belief now that he was well and finally separated from military service. In the 1921 version of the book, he advocates for a force consisting of heavy bombardment units to bomb the enemy, combat units to ward off enemy forces (fighters), and reconnaissance units to assist in targeting. For this comparison, see Meilinger, *Airwar: Theory and Practice*, 16-17.

forces is the use of reconnaissance aircraft to provide intelligence and identify targets for bombardment. Only after gaining command of the air does Douhet consider the diversion of air forces from offensive operations to supporting defensive operations and for support of surface forces.[28]

The addition of an entirely new domain to the national security calculus forced Douhet to address the organization and utilization of the various domain powers in support of national security objectives. During future conflicts, he perceives the role of surface forces as preventing enemy forces from achieving victory while airpower targets the enemy's will to continue fighting. This radical shift in the role of military forces means that unlike the maritime theorists, Douhet finds it necessary to include in his theory the rationale for the separation of airpower from other domains at an organizational level.

Douhet argues for the creation of a separate air force and the creation of a coordinating military organization along the lines of today's Department of Defense to oversee the development and use of each domain. Because the overall national means available for defense are restricted, apportionment of resources during both peace and war must occur with overall security objectives in mind.[29] During times of peace, left to their own devices, land and seapower services seek to maximize their own domain-centric power regardless of the overall utility of that power toward national security objectives. The result is that airpower development will suffer from neglect or from categorization as a supporting force

[28] This lack of specialization is noteworthy because it differs from the views of the following two theorists.
[29] Douhet presents his rational for a centrally organized national defense in Chapter 4. Douhet, *The Command of the Air*, 69-92.

for surface operations. During times of conflict, Douhet suggests, an overarching organizational structure will coordinate operations across the three operational domains and provide both direction and prioritization of effort.

In addition, Douhet advocates for direct government involvement in the development of civil aeronautics. This is evident when he writes, "All activities bearing directly on the national defense must be supported by the organs of national defense."[30] Here he is saying that civil aeronautics, like other national activities, requires support and encouragement from the state. For example, Douhet suggests that development of the infrastructure, industry, facilities, equipment, and corporations to take advantage of Italy's central geographic position as an air travel hub is in the national interest and benefit from direct government actions.[31] Similar to his assertion that defense efforts be coordinated, he also suggests that commercial domain development also requires creation of a government body at the cabinet level, separate from other bodies, with the authority to coordinate all aeronautical issues, regardless of their nature in order to encourage development both economically and militarily.

Douhet's elements of analysis

Douhet's theory of airpower is remarkable in that he conceived it during the very early years of air domain development. Because the domain and technologies supporting it were in their infancy, many of the concepts he

[30] Ibid., 72.
[31] Douhet discuss the rationale behind developing civil aviation to include government investment in the program as insurance for the future of national security, see ibid., 77-82.

advocated were visionary. Without a long and detailed reservoir of historical knowledge from which to draw, he begins by identifying how the air domain power differs from those of the land and sea domains. His writings reflect this process of differentiation from the surface domains and his struggles to overcome skepticism and parochial interests. Although his writings focus on development of airpower for Italy, from them we take lessons regarding development of power in a domain that is simultaneously emerging as a global commons. It is important to keep in mind that Douhet's theory assumes that post-WWI wars will be total wars, conflicts between nations and not wars between armies. Douhet's elements of analysis are the following:

1) Governments must encourage the development of commercial infrastructure and industry to develop national economic and military power.
2) Commercial and military interests in the global commons overlap, requiring national-level organization for military and civil development in a coordinated and efficient manner.
3) The ability to bypass fielded forces makes an enemy's will and capability to resist the strategic objective.
4) Command of a domain from which effects are projected provides protection and allows one to directly target an adversary's means, and will to resist.
5) In the absence of geography, chokepoints develop at access points to the domain.
6) Efficiently targeting an adversary's domain power requires targeting domain access points, not units currently within the domain or along lines of communication.
7) The elimination of geography as a factor in movement and increased speeds of travel reduce the warning and reaction time nations have to respond to attacks.
8) Increased mobility makes defense of a global commons resource-prohibitive.
9) The relative strength of domain power at the onset of conflict is a significant determinant of which nation will gain command of the domain; once reduced, it cannot be rebuilt quickly.
10) Forces in a global commons are primarily offensive in nature.

11) Given the offensive nature of forces, they should consist of combat power to deny enemy use of the domain and reconnaissance.
12) Forces designed for combat in a global commons must exist as a fully trained "capability in being" before conflict erupts.
13) Bypassing fielded forces allows direct targeting of all means of resistance, including a population's will to endure bombardment.
14) The lack of predictable targets and set lines of communication makes defense of global commons resource-prohibitive.
15) Resources expended on creating defensive capabilities divert resources from the development of combat power and the ability to gain command of the domain.
16) Destruction of the enemy's capability to use a domain is necessary to gain command – a good offense is the best defense.
17) Efficacy of national power development across all domains requires coordination across national interests.
18) Full development of domain power requires an independent organization within the military command structure to provide equal footing between all domains.

The air domain's ability to project power into the other domains, the combined effects of increased speed, the reduced influence of geography on Douhet's assessment of defense, and the domain's complete reliance on technology for exploitation drive this long list of elements of analysis. Adding these elements of analysis to the comparison table provides the following results:

Table 4: Air Domain Elements of Analysis - Douhet

Air Domain Elements of Analysis			
	Douhet	**Mitchell**	**Seversky**
1	Governments must encourage the development of commercial infrastructure and industry to develop national economic and military power.		
2	Commercial and military interests in the global commons overlap, requiring national-level organization for military and civil development in a coordinated and efficient manner.		
3	The ability to bypass fielded forces makes an enemy's will and capability to resist the strategic objective.		
4	Command of a domain from which effects are projected provides protection and allows one to directly target an adversary's means, and will to resist		
5	In the absence of geography, chokepoints develop at access points to the domain.		
6	Efficiently targeting an adversary's domain power requires targeting domain access points, not units currently within the domain or along lines of communication.		
7	The elimination of geography as a factor in movement and increased speeds of travel reduce the warning and reaction time nations have to respond to attacks.		
8	Increased mobility makes defense of a global commons resource-prohibitive.		
9	The relative strength of domain power at the onset of conflict is a significant determinant of which nation will gain command of the domain; once reduced, it cannot be rebuilt quickly.		
10	Forces in a global commons are primarily offensive in nature.		
11	Given the offensive nature of forces, they should consist of combat power to deny enemy use of the domain and reconnaissance.		
12	Forces designed for combat in a global commons must exist as a fully trained "capability in being" before conflict erupts.		
13	Bypassing fielded forces allows direct targeting of all means of resistance, including a population's will to endure bombardment.		
14	The lack of predictable targets and set lines of communication makes defense of global commons is resource-prohibitive.		
15	Resources expended on creating defensive capabilities divert resources from the development of combat power and the ability to gain command of the domain.		
16	Destruction of the enemy's capability to use a domain is necessary to gain command – a good offense is the best defense.		
17	Efficacy of national power development across all domains requires coordination across national interests		
18	Full development of domain power requires an independent organization within the military command structure to provide equal footing between all domains.		

Mitchell

Brigadier General William "Billy" Mitchell was born on December 29, 1879, into a wealthy family.[32] The grandson of a US congressman and son of a senator, he grew up with access to education and an exposure to domestic and international politics.[33] Mitchell, although considered bright, was an average student, preferring to spend his time in the outdoors and on athletics instead of academics – a trait that served him well in the rough-and-ready early days of his army career. He attended Columbia University but did not graduate, instead leaving college to enlist in the army during Spanish-American War at age 19.[34] Gaining a commission through his father's intervention, he became a second lieutenant assigned to the Army's Signal Corps. Mitchell's early career included assignments to Cuba, the Philippines, and Alaska, where he served with distinction and developed a reputation as an officer capable of taking on difficult tasks and seeing them through to completion.[35]

After the adventurous overseas assignments of his early career, his mid-career during the early 1900s was a mix of assignments to Army Staff College at Fort Leavenworth and an assignment to the Philippines, where he was the chief

---

[32] For a detailed account of Mitchell's early life, see James J. Cooke, *Billy Mitchell*, (The Art of War) (Boulder, CO: Lynne Rienner, 2002).

[33] He was actually born in France while his parents were living overseas prior to election to Congress and eventually the Senate. He learned to speak French at the insistence of his father, a skill that later made him a good candidate for observing airpower in Europe during WWI.

[34] Columbia later became George Washington University.

[35] Mitchell made his mark by laying telegraph wires across these areas, including the first wires across Alaska that were needed to support communications during the gold rush. He had gained a reputation within the Signal Corps as an officer capable of tackling the most difficult jobs. Upon his return to the continental United States at age 24, he received promotion to Captain, the youngest captain in the Regular United States Army. Cooke, *Billy Mitchell*, 37.

signal officer for the Department of the Philippines. In March 1912 at age 32, he received assignment as the youngest officer on the General Staff in Washington, DC. Assigned to the Signals Section, he brought to this job a budding understanding of the role communications play in military operations and national security, an awareness that would grow in the years to come.

At this time, Army Aviation existed as a subset of the Army Signal Corps. Despite army aviation's management by his organization, Mitchell took little notice of the early years of airpower development, remaining disinterested in taking a personal part in the development of the new domain even though as a member of the General Staff he received reports of aviation's growing utility in combat from Europe.[36] This disinterest ended early in 1916 with his assignment as the temporary chief of the Aviation Section. With a newfound interest in aviation, an increase in rank to major, and a concern about retaining credibility within the section for which he was now responsible, Mitchell decided to take flying lessons. Enrolling in flying school at age 38, he paid for the lessons out of his own pocket.[37] Now an Army aviator, in April 1917 Mitchell received orders to Europe as an official US observer of aviation operations during WW I.[38]

As the senior airman in Europe, Mitchell became the head of the American Expeditionary Force Air Service, eventually receiving a promotion to Brigadier General. In this position, Mitchell observed the organization and operations of airpower by both sides of the conflict. Additionally, he gained

---

[36] Ibid., 43, 50-51.
[37] Ibid., 51.
[38] Meilinger, *Airmen and Air Theory: A Review of Sources*, 8.

firsthand experience in the challenges of operating within the new domain.[39] Mitchell gained this experience rapidly, planning and execution of an almost 1,500-plane operation in support of the Saint-Mihiel offensive in 1918. This complex operation demonstrated the rapidly maturing and visionary nature of his thinking regarding the importance of the air domain to combat operations.[40] Through his wartime experiences, Mitchell developed a belief that airborne offensive action was the best means of eliminating enemy air capabilities and gaining control of the domain, a tactic most effective using centrally controlled forces operating under a single command.[41]

Mitchell's wartime experience garnered him recognition as America's top airman. Upon returning to the United States after the war, he continued to advocate for the development of airpower, a course of action that alienated both his flying and non-flying superiors. In the face of resistance from airpower skeptics and what he perceived as institutional resistance within the Army, Mitchell took it upon himself to begin a public and "vitriolic campaign to push airpower to the forefront of the American national defense effort."[42]

Mitchell felt that aggressive tactics were necessary because his position challenged status quo thinking on military operations. He threatened deeply held beliefs among military professionals regarding the roles and missions of each

---

[39] Unlike in the US, the Europeans were experimenting with independent air operations, perhaps under the sway of Douhet, whose writings had been translated into French and widely published on the continent.

[40] For a description of Mitchell's role in planning and executing this operation, see Roger Burlingame, *General Billy Mitchell, Champion of Air Defense*, They Made America (New York, NY: McGraw-Hill, 1952), 91-104.

[41] Mason L. Ripp, "General William Mitchell" (Air University, 1965), 57.

[42] Winton, "A Black Hole in the Wild Blue Yonder: The Need for a Comprehensive Theory of Air Power," 35.

service in future conflicts by calling for a build-up of airpower, which would decrease the importance of land and maritime forces. As a result, his arguments fell on largely unresponsive ears.[43] In an effort to win his case for development of a separate air service, he continued to elevate the level of his critiques on surface forces and sought a wider public audience through the publication of his opinions through both print media and public statements. The public nature of Mitchell's arguments demonstrated his understanding that changing War Department organization was as much a political fight as one of altering long held service roles and missions. He clearly understood the value of going over the heads of his War Department superiors to convince both the public and key policy makers of the correctness of his position. Like Douhet before him, Mitchell's passion for his arguments would eventually lead to a court-martial for insubordination.[44] Following the court-martial, Mitchell retired and continued advocating for the development of airpower until his death in February 1936.

Although Mitchell was not the only American airpower advocate of his day, he is the one most often associated with the struggle to create an independent

---

[43] The author does not intended to paint Mitchell as a loan voice of advocacy for greater autonomy and development of air forces. On the contrary, others such as Maj. General Mason Patrick, head of the Air Service, supported actions along these lines; he simply chose to pursue them in less dramatic fashion.

[44] Two events, the disappearance of a PN-9 aircraft in the Pacific attempting the first flight between the West Coast and Hawaii, and the crash of the dirigible *Shenandoah* due to severe weather in Ohio during early September 1925, prompted Mitchell to call reporters and criticize oversight of airpower development. He provided prepared remarks claiming "the incompetency, criminal negligence, and almost treasonable administration of the National Defense by the Navy and War Departments." Within two weeks, a court-martial of Mitchell for conduct prejudicial to good order and military discipline began. Eventually found guilty of the charge on December 17, Mitchell's sentence was five years of suspension from active duty without pay. For a detailed discussion of the politics and side stories surrounding the court-martial and the source of this information, see Alfred F. Hurley, *Billy Mitchell, Crusader for Air Power* (Bloomington, IN: Indiana University Press, 1975), 100-09.

air arm. It is Billy Mitchell, not his superior officers or peers, most often referred to during discussions of early airpower theory. Although he was prolific in both written and public statements concerning his views, he is best known to airpower theorists and practitioners for his work *Winged Defense: The Development and Possibilities of Modern Air Power Economic and Military.* Published in 1925, by his own admission this work is a collection of thoughts he had previously published in other places.[45] As such, it serves as a good overall portrayal of his airpower theory during the time of his greatest personal participation in the development of both airpower and airpower theory.

Theory

> "In the future, no nation can call itself great unless its airpower is properly organized and provided for, because airpower, both from a military and economic standpoint will not only dominate the land but the sea as well. Airpower in the future will be a determining factor in international competitions, both military and civil."[46]

Mitchell was the first American airman to pick up the mantle of airpower and both forcefully and publicly argue for its development. His ideas in many ways reflect what at the time were current thinking and the privately expressed beliefs of many airmen, both within the United States and overseas. His theory, as expressed in *Winged Defense,* is useful to the purposes of this research because it is a data point for thinking about the development of a new domain and domain-centric power. Where Douhet primarily wrote with a focus on Italy's

[45] Ibid., 100. In addition to numerous articles written by Douhet, he had previously published the book *Our Air Force, Keystone of National Defense* in 1921. Later, after retirement, in 1930, he published *Skyways,* which continued his advocacy for airpower independence and provided little new information.
[46] Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*, x.

development of airpower and had influence in Europe, Mitchell is an example of American thought between the World Wars and how significantly it influenced development of airpower on this side of the Atlantic. The theories of the two men are similar in many ways, a fact that provides some insight into the requirements for domain power theory overall and particularly the development of national power in a new domain.

While Douhet's theory is the more cogent of the two, what distinguishes Mitchell's theory from Douhet's is that he wrote based on extensive personal experience as an aviator during both peacetime and war and was thus better grounded in the history and experience available to an airpower theorist of his time.[47] A shortcoming of Mitchell's work is his failure to fully explore the effect of air domain development on other instruments of national power. Within *Winged Defense,* his discussions of the non-destructive uses of the domain are limited. Where it does appear, they focus on the development of industry, infrastructure, and commercial aviation to speed domain exploitation or act as a reserve force when necessary. Outside of stating that airpower can bring civilization to remote areas of the earth, Mitchell's theory leaves the reader looking for other benefits of airpower development across the DIME.[48] With that

[47] Harold Winton makes this point in a review of extant airpower calling Mitchell's work inferior to Douhet's because it does not tie itself in well with warfare in other domains. He does give Mitchell high marks, however, for defining airpower precisely and developing solid propositions about airpower, unlike Douhet. See Winton, "A Black Hole in the Wild Blue Yonder: The Need for a Comprehensive Theory of Air Power," 36.
[48] Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*, 26. "Just as power can be exerted though the air, so can good be done, because there is no place on the earth's surface that air power cannot reach and carry with it the elements of civilization and good that comes from rapid communications."

in mind, we now transition to a discussion of Mitchell's airpower propositions and insights.

Like Douhet, Mitchell's fundamental proposition is that "the influence of air power on the ability of one nation to impress its will on another in armed conflict will be decisive."[49] In addition to sharing a fundamental proposition, both theorists recognized that the coming of airpower heralded a move toward the totality of war: a fundamental change in conduct of war that would forever change the relative importance of surface forces to conflict between nations. From an organizational perspective, they both determined that this change not only required creating a separate air force, but also required a department of defense to coordinate development and use of airpower and, on the civilian side, an agency to provide overall synchronization of national aeronautical policy.[50]

Mitchell, like the maritime theorists in the previous chapter, was familiar with the works of theorists writing about other domains (maritime and land), using their works for inspiration. This familiarity no doubt underpinned his connection of airpower use to national objectives instead of tactical and operational goals and his advocacy of attacking an enemy's will to fight. His familiarity with extant maritime theory and the requirement for domain power development is clearly displayed in the opening lines of *Winged Defense.* In these

---

[49] Ibid., 214.

[50]Some historians claim that Mitchell was very familiar with Douhet's theory, while others dismiss the claim based on a lack of evidence that an English translation of Douhet thoughts existed at the time. Regardless of the influence Douhet is claimed to have had on Mitchell's thinking, most scholars admit that there is at least a possibility that the two airpower theorists met briefly in Europe between the wars. While the similarities between their theories are obvious to any reader, many can be found in Winton, "A Black Hole in the Wild Blue Yonder: The Need for a Comprehensive Theory of Air Power," 35-36.

lines, Mitchell states that the world has passed through a "continental era" (land-centric) and an "era of the great navigators" (maritime-centric); it now stands on the threshold of a new era, the "aeronautical era."[51]

> "Mitchell could recite Clausewitz's dictum on the objective of war, but he did so with a parochial twist. Airpower would wreck and enemy's will to fight by destroying his capability to resist, and the essence of that capability was not the army or navy but the nation's industrial and agricultural underpinnings."[52]

Although he does not mention previous theorists directly, his use of multiple references to concepts from maritime and land theories demonstrate the use of extant theory in attempts to bolster his positions, including the use of relevant historical examples across domain boundaries. His arguments are meant to demonstrate that relevant concepts such as siege warfare and direct attacks on a nation's war-making potential are more efficiently undertaken through the new air domain and by bypassing surface forces to strike directly at the enemy's will to fight. Mitchell does not advocate development of airpower for its own sake, but instead stresses that it is the most efficient means of achieving national security objectives; to him, airpower is simply a tool to support overall political objectives. Both airpower and command of the air are prerequisites for pursuit of national objectives within the surface domains. Airpower is a means to an end thought exertion of the influence upon events on the ground, not an end in itself.[53]

---

[51] Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*, 3.

[52] Mark A. Clodfelter, Lt Col, "Molding Airpower Convictions: Development and Legacy of William Mitchell's Strategic Thought," in *The Paths of Heaven: The Evolution of Airpower Theory*, ed. Col. Phillip S. Meilinger and School of Advanced Airpower Studies (US) (Maxwell AFB, AL: Air University Press, 1997), 96.

[53] Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*, 18. Mitchell writes: "A person cannot permanently live out on

Mitchell clearly categorizes airpower as a subset of overall national efforts, a concept borrowed from Clausewitz. Mitchell also borrows elements from Mahan's maritime power theory. Like Mahan's view that national seapower is based upon underlying fundamentals such as geography and national character, Mitchell's theory brings forth underlying fundamentals for airpower development.[54] Although Mitchell does not follow Mahan's lead by formally listing these fundamentals, the rough categorization of them below uses similar terminology to facilitate their comparison.

> "Air power is the ability to do something in or thought the air, and, as the air covers the whole world, aircraft are able to go anywhere on the planet."[55]

Geography and physical conformation: Like Douhet, Mitchell claims that the speed and flexibly of aircraft have altered the role geography plays in national security, reducing its influence and increasing the importance of time: "The advent of airpower has made every country and the world smaller. We do not measure distance by the unit of miles, but by the unit of hours."[56] In other words, from a military perspective, the air domain reduces the apparent strategic

---

the sea nor can a person live up in the air, so that any decision in war is based on what takes place ultimately on the ground." Mitchell does say that airpower may be capable of creating conditions on the ground that cause a nation to surrender but is less convinced than Douhet that future warfare may be fought and won solely in the air.

[54] Mahan's six factors from Chapter 4 are Geographical Position, Physical Conformation (including natural conditions and climate), Extent of Territory, Number of Population, Character of the People, and Character of the Government (and national institutions). The direct comparison to Mahan presented here is inspired by and adapted from Clodfelter, "Molding Airpower Convictions: Development and Legacy of William Mitchell's Strategic Thought," 101.

[55] Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*, 3-4.

[56] Ibid., 26. Mitchell goes on to say on page 130: "There is no part of the civilized world that cannot be reached at present in a fraction of the time that was required fifty or a hundred years ago. Within the last decade the advent of transportation has added a decidedly new element in the relations of nations to each other."

depth of a nation and minimizes its national defensive barriers, opening previously well-defended sites to sudden and devastating attack from the air.

Mitchell identifies three different unique geographic conditions for classifying countries and the role airpower will play in their conduct of war. First are islands subject to attack from a continent. Second are nations that share a land border with opponents and are reliant on trade and outside supplies for national well being. The final category consists of nations like the United States, self-sustaining and out of ordinary aircraft range.[57] In each of these cases, he shows that airpower has the potential to be a decisive factor in the conduct of war and that each requires the development of airpower focused on preserving the nation's ability to continue fighting and projecting power.

For example, he demonstrates the need to gain and maintain control of the air domain to protect not only the island nation itself, but also the surface lines of communication connecting it to the continent. Without this control, an island nation cannot continue to receive supplies to sustain its war effort, nor will it be able to exert power upon the continent through movement of land forces across the intervening span of water. If a continental power gains control of the air, the island nation will lose access to war-sustaining supplies and be at the mercy of an aerial siege/blockade. In this case, command of the air by a continental power may be sufficient to end the war. Considering that he formulated his theory before the WWII Battle of Britain, these are remarkable insights.

In the second case, where nations share land borders and surface lines of communication, the quick reaction of the air forces is necessary to: 1) contest

[57] Ibid., 10-11.

control of the air in order to, 2) prevent enemy destruction of your lines of communication and vital infrastructure while, 3) enabling your own interference with the opponent's war-making capabilities. Unless one side is able to force the other into surrender before mobilization can take place, there is a real possibility land combat will ensue. For Mitchell, this means that if one nation is prepared to immediately conduct aggressive aerial warfare and the other is not, the aggressive nation has a distinct advantage over its adversary. Immediate overwhelming action may prevent escalation of a conflict to include the surface domains.

In his third example, he characterizes a nation such as the United States in the early 1900s, a time in which he viewed an efficient air force as the only means to protect the nation from maritime attack and a prerequisite to project power.[59] Because air forces can dominate any approach to the continent by maritime forces looking to land troops, any ground conflict is extremely unlikely. In order to project power, nations will have to create a string of island bases to extend control of the air out to a point where it can provide cover for any invasion or launch direct air attacks upon its enemy without the need to secure a foothold upon an adversary's shore. His vision of future warfare is noteworthy when you

> "The only defense against aircraft is by hitting the enemy first, just as far away from home as possible. The idea of defending the country against air attack by machine guns or anti-aircraft cannon from the ground is absolutely incapable of being carried out."[58]

[58] Ibid., 213.
[59] Mitchell briefly outlines a campaign involving the United States, saying that the outcome would depend on the amount of airpower a nation can produce and apply. See ibid., 31. The ability of air forces to affect surface lines of communication would prevent movement of forces across for purposes of an invasion, he felt.

consider he wrote before the island-hopping campaign conducted by the US in the Pacific during WWII.

Like Mahan before him, Mitchell also suggests that geography combined with a nation's physical conformation plays a role in shaping a nation's underlying approach to national security and the type of forces and commercial industry it develops. In much the same manner as Mahan's *physical conformation* and *extent of territory* shaped a nation's incentive to develop maritime capability, the extent of territory, natural obstacles, and access to raw materials a nation possesses influence the development of aviation. Geography that requires an ability to cover long distances quickly, and obstacles that must be over flown, encourage movement of goods and personnel through the air. This provides incentive for a nation to develop airways, radio communications, extensive weather reporting, and commercial/military infrastructure to provide services to coordinate and organize movement by air.[60]

Offensive nature of airpower: Mitchell argues the three dimensional nature of airpower makes defense against aerial attack impractical. During the early 1900s within which he was writing this position was arguably true. Ground-based air defense weapons were in their infancy, and the belief among airmen was that for all practical purposes aircraft would always get through to strike their targets. The only defense against aircraft from Mitchell's perspective "[is] other aircraft which will contest the supremacy of the air by air battles" adding, "Once supremacy of the air has been established, airplanes can fly over a hostile country

[60] Ibid., 32-33. Mitchell discusses the requirement to have access to raw materials for aviation equipment on page 25 as part of the role a nation's industrial condition plays in determining airpower potential.

at will."[61] The lack of an effective defense, he argues, dictated that the best use of airpower is to strike at opposing aerodromes, industry, and support infrastructure with the expressed purpose of gaining command of the air while simultaneously striking at the enemy's will to fight by attacking vital centers of industry and government. Like Douhet, Mitchell is convinced that because defense in the domain is uncertain or even impossible, the best defense is a good offense; a nation must seek to gain command of the domain before its adversary can do the same.

Domain control: Unlike Douhet, Mitchell believed that air-to-air combat is an effective means of wearing down the enemy's air forces. Mitchell's WWI experiences convinced him that despite the vastness of the domain, it is possible to detect, intercept, and engage in combat between air forces.[62] Although the state of technology at the time of Mitchell's writing was inadequate for the task, over the next few decades his vision would prove correct, Air-to-air combat became the means for grinding down German air forces during WWII, beginning with the Battle of Britain and continuing through bomber raids deep into Europe.

Mitchell's belief in the utility of pursuit aviation leads him to advocate a mix of aircraft for creating domain power, including pursuit, attack, and bombers

---

[61] Ibid., 9.

[62] This section does not suggest that Mitchell failed to recognize the value of attacking air forces on the ground or the industries that create them, just a difference of emphasis. Mitchell recognized that because the entire nation was subject to attack, industry would be unable to create an air force during a time of war, and that attacking aircraft bases deprived the enemy of the equipment, airframes, and support infrastructure necessary to contest the air domain.

and heavily weighted (60%) toward pursuit.[63] This is a force structure at odds with Douhet's recommendation. Instead of Mitchell's mix, Douhet recommends air forces consisting primarily of heavily armed battle planes focused on strategic bombardment and capable of self-defense. These battle planes would then be re-tasked to surface support roles after achieving air superiority by attacking enemy aviation infrastructure.

The challenge for Mitchell in advocating destruction of enemy air power through force-on-force combat is not unlike that faced by Corbett: namely, how does a nation with the preponderance of domain power force an adversary's "fleet in being" to sortie forth and engage in combat?[64] Mitchell's solution is much like that of the maritime theorists – "finding a location of such importance to the enemy that he must defend it against bombardment attack by airplanes."[65] Where Corbett identified chokepoints formed by geography and ports as critical to lines of communication, Mitchell modifies the concept to account for the peculiarities of the air domain. Airdromes take the place of ports as a location where lines of communication come together, and rather than geographically determined vital

---

[63] For instance, Mitchell advocates the creation of pursuit aircraft (*fighter* in today's lexicon) for defense of the homeland from enemy bombers and for use to defend bombers and attack aircraft. See Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*, 182, 86, 88-90. Douhet, on the other hand, recommends the use of heavily armed battle planes that are capable of self-defense while primarily being used to bomb the enemy's population and infrastructure.

[64] Mitchell engages in an interesting discussion regarding the power of a "fleet in being" based upon his understanding of the affect German submarines had on Allied navies during WWI. By his count, thirty German submarines and ten thousand men kept one million men busy on the allied side trying to counter their potential to lay mines. For his full discussion, see ibid., 102-09.

[65] Ibid., 9.

locations, vital centers of industry and government provide critical locations that must either be defended or given over to strikes by the enemy.[66]

For Mitchell, the act of targeting enemy vital centers, forces concentration of aircraft for defense, resulting in great air battles providing the superior force an opportunity to establish domain control. Although the tactics to achieve control are Corbettian in appearance, domain control in this case is Mahanian in nature: the elimination of the opponent's ability to use the domain to threaten one's operations. Elimination of enemy use of the domain secures one's own freedom of action, ensures security, and allows one to dictate the nature and timing of conflict escalation in military terms. Only after achieving complete domination of the air domain can an invasion across the seas or land occur.[67]

Despite asserting that airpower's first mission is to gain air superiority, Mitchell did not believe cross-domain attacks must wait until achieving total command of the air. He acknowledges that the natural state of the domain at the beginning of a conflict is uncommanded and that the path to domain control is not instantaneous. Although Mitchell does not state this explicitly, he does imply that effective control can be temporary and/or local in nature to support operations in pursuit of strategic and operational goals.[68]

---

[66] The critical nodes for attack extend to airpower's ability to affect forces in other domains. Airpower can attack not only forces in the field but also their supply points and means of transportation. This concept extends even to Mitchell's discussion of submarines in which he recognized the power of striking at their bases and fueling stations rather than the ships themselves. See ibid., 99.

[67] Ibid., 102.

[68] Ibid., 164-66. He does this through his advocacy for use of pursuit aircraft to protect both bombers and attack aircraft from enemy interference while they accomplish their mission.

Government policy and domain power: Fearing that inaction was placing the US behind its peers, Mitchell wrote hoping to alert the nation's political leaders to the urgent need for creating domestic industry and a competent workforce focused on the air domain.[69] In Mitchell's words, "Once a nation has dropped behind in its [airpower] development, it is like making a stern chase, and [it is] a very difficult undertaking again to get the lead."[70] To shorten the time necessary for developing a national reservoir of expertise in the domain and to standardize training and infrastructure requirements, Mitchell called for the creation of a centrally organized and government administered national training system.[71]

Mitchell advocated government involvement not solely because of the size and complexity of the task, but also the cost of development. In order to offset the costs of developing the domain commercially he suggested the government assume some of the costs for what are essentially dual use facilities in time of war. For example, in order to encourage development of high-cost yet critical aspects of the commercial and industrial complex – airdromes, airways, factories,

[69] Mitchell saw that the nation's lack of experience with airpower, and its generally low levels of appreciation for airpower's potential, made it necessary for airpower theory to educate the nation on how to develop the air domain and the risks of failing to do so. He clearly recognized that the human elements of airpower – flight officers, support personnel, mechanics, designers, manufacturers, engineers, and inspectors – all take time to train and develop.

[70] Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*, 184.

[71] For a discussion of the requirement to development the expertise necessary for ordering, producing, and maintaining aircraft, see ibid., 191-98.

and commercial air carriers – Mitchell proposed government subsidization of commercial efforts.[72]

Government actions focused on creating commercial use of the domain, he suggests, creates a reservoir of human capital possessing talents and capabilities that the nation turns to in time of need. By seeking commercial development through incentives while simultaneously guiding development through standardization and regulation a government can leverage commercial competition to develop airpower sciences more rapidly than government efforts alone are capable of producing.[74]

> "In the future, no nation can call itself great unless its air power is properly organized and provided for, because air power, both from a military and an economic standpoint, will not only dominate the land but the sea as well. Air power in the future will be a determining factor in international competitions, both military and civil. American characteristics and temperament are particularly suitable to its development."[73]

In essence, Mitchell is echoing points made by Mahan regarding the development of seapower. By suggesting that airpower potential requires a government with the vision to recognize the importance of airpower to national security and then select policy options to both shape the state's national character and create domestic industries focused on the domain, Mitchell was seeking to create an air-minded nation similar to Mahan's seafaring nation.[75]

The US focus of Mitchell's writing brings him around to discussing the population's aptitude for aviation and aviation-associated industry. Here again he

[72] Ibid., 87-88.
[73] Ibid., x.
[74] Ibid., 149-51.
[75] Ibid., 93-94.

shadows the work of Mahan without the organizational elegance of Mahan's six factors for domain power potential. The character of America's population, Mitchell suggests, is ideally suited to aviation and aviation support because its cultural experiences instill discipline, courage, and teamwork into each citizen's personal character, providing a reservoir of pilots from which to choose. At the same time, the nation's industrial base provides a ready group of workers with the knowledge, skills, and abilities necessary to maintain aircraft.[76]

Doman Power Organization: Mitchell's proposition that airpower is capable of dominating the surface forces is accompanied by organizational recommendations for both efficiency and the maximization of domain power development across civil, military, and commercial sectors. In *Winged Defense*, Mitchell makes the case for separating management of military and civilian aviation development from that of other domains. In practical terms, his recommendation takes the form of a separate civil government organization overseeing commercial domain development and, from a military perspective, both a separate air force, co-equal with the land and maritime forces, and a department of defense to coordinate the development and use of all three forces.[77]

Mitchell argues that attachment of air domain assets to existing military services and government agencies limits their growth; each organization emphasizes its primary mission, viewing airpower as a supporting element.[78] Whether undertaken consciously or unconsciously, a lack of air domain emphasis

[76] Ibid., 172, 79. Mitchell lists strong national moral, patriotism, and love of country as requirements for withstanding the rigors of air combat, something, he says, of which the United States possesses the greatest reservoir in the world. See ibid., 25.
[77] Ibid., 113.
[78] Ibid., 112.

prevents full exploration and development of the new domain both commercially and militarily. Mitchell points out that not only are operations in the new domain different in a physical sense, but the design, experimentation, acquisition, and support for air forces are also radically different from that of other domains. Unless managed with a focus on the domain, these critical aspects of domain power development are unable to keep pace with developments in the field of aviation. Because of these differences, breaking air domain development and its associated budget away from restrictions imposed by non-airmen is a critical requirement for maximizing domain power, creating air-mindedness, and providing an industry focused on technological advances.

Mitchell's elements of analysis

Winged Defense is both a powerful argument for development of air domain power and a description of the steps necessary to accomplish the task. Mitchell's practical experience with aircraft provides him with the insight into the mechanics of developing air forces and their use that Douhet lacked. Like Douhet, many of Mitchell's concepts were visionary given the state of aviation technology during his time. Although not well documented here, he uses historical examples to support his conclusions and identifies the unique nature of the domain: its ability to directly influence the use of other domains. Despite the fact that his entire work is an argument to overcome organizational and parochial resistance to airpower development in the United States, lessons for development of a new

domain are numerous. From Mitchell's theory, one finds the following elements of analysis, many of which mirror those of Douhet:

1) Use of domain power should focus on defeating an adversary's will and capability to engage in conflict.
2) Power in a technology-dependent domain depends on military and commercial development of personnel, infrastructure, technology, and industry.
3) Development of personnel to exploit a domain is as important as the technology to enter the domain.
4) The willingness of a government to use incentives for stimulation of commercial industry and infrastructure determines domain power.
5) Commercial development of technology is faster and more efficient than government development.
6) Central guidance ensures that military and civil development occurs in a coordinated manner (Department of Defense, national civil administration).
7) Military and civil organization for exploitation of a domain must focus solely on that domain (separate service).
8) Geography determines domain power potential through access to resource, creation of incentives, development of national character, and force structure requirements.
9) Absent geography, chokepoints occur at points of entry into a domain.
10) Recreation of domain power during a conflict is not possible due to destruction of industrial means and long lead times.
11) Speed, flexibility, and the vastness of a commons complicate development of robust defenses, making highly mobile forces offensive in nature.
12) Defense of vital points in commons is necessary to ensure access/use of the domain (points of domain access and vital national infrastructure).
13) The lack of warning before an attack means that forces in the domain must constantly be prepared to defend vital points.
14) The ability to influence across domain boundaries decreases the importance of traditional defenses such as distance and reaction time.
15) Control of a commons can be temporary or permanent in nature, depending on operational objectives: Control is necessary for effective projection of power to another domain.
16) One type of force is incapable of fully exploiting a domain: Both specialized counterforce and attack units are required.
17) Gaining domain control requires elimination of the enemy's ability to enter the domain.
18) As long as a commons is uncontrolled, any point within the domain or along its seams is vulnerable to attack.

19) Control of the domain allows the controlling force to influence use of other domains across domain boundaries as desired.

Placed side by side on the elements of analysis chart, the similarity between Mitchell and Douhet's elements is apparent. Their writings share the requirement to educate and guide development of the domain by describing the effect of technology on the use of the domain, the domain's potential to influence other domains, and the need to gain domain control and projecting power across domain boundaries. They also share an emphasis on the requirements for centralized government involvement and the need to develop the domain in the face of institutional and organizational resistance.

Table 5: Air Domain Elements of Analysis - Mitchell

Air Domain Elements of Analysis			
	Douhet	**Mitchell**	**Seversky**
1	Governments must encourage the development of commercial infrastructure and industry to develop national economic and military power.	Use of domain power should focus on defeating an adversary's will and capability to engage in conflict.	
2	Commercial and military interests in the global commons overlap, requiring national-level organization for military and civil development in a coordinated and efficient manner.	Power in a technology-dependent domain depends on military and commercial development of personnel, infrastructure, technology, and industry.	
3	The ability to bypass fielded forces makes an enemy's will and capability to resist the strategic objective.	Development of personnel to exploit a domain is as important as the technology to enter the domain.	
4	Command of a domain from which effects are projected provides protection and allows one to directly target an adversary's means, and will to resist	The willingness of a government to use incentives for stimulation of commercial industry and infrastructure determines domain power.	
5	In the absence of geography, chokepoints develop at access points to the domain.	Commercial development of technology is faster and more efficient than government development.	
6	Efficiently targeting an adversary's domain power requires targeting domain access points, not units currently within the domain or along lines of communication.	Central guidance ensures that military and civil development occurs in a coordinated manner (Department of Defense, national civil administration).	
7	The elimination of geography as a factor in movement and increased speeds of travel reduce the warning and reaction time nations have to respond to attacks.	Military and civil organization for exploitation of a domain must focus solely on that domain (separate service).	
8	Increased mobility makes defense of a global commons resource-prohibitive.	Geography determines domain power potential through access to resource, creation of incentives, development of national character, and force structure requirements.	
9	The relative strength of domain power at the onset of conflict is a significant determinant of which nation will gain command of the domain; once reduced, it cannot be rebuilt quickly.	Absent geography, chokepoints occur at points of entry into a domain.	
10	Forces in a global commons are primarily offensive in nature.	Recreation of domain power during a conflict is not possible due to destruction of industrial means and long lead times.	
11	Given the offensive nature of forces, they should consist of combat power to deny enemy use of the domain and reconnaissance.	Speed, flexibility, and the vastness of a commons complicate development of robust defenses, making highly mobile forces offensive in nature.	
12	Forces designed for combat in a	Defense of vital points in commons is	

	global commons must exist as a fully trained "capability in being" before conflict erupts.	necessary to ensure access/use of the domain (points of domain access and vital national infrastructure).	
13	Bypassing fielded forces allows direct targeting of all means of resistance, including a population's will to endure bombardment.	The lack of warning before an attack means that forces in the domain must constantly be prepared to defend vital points.	
14	The lack of predictable targets and set lines of communication makes defense of global commons is resource-prohibitive.	The ability to influence across domain boundaries decreases the importance of traditional defenses such as distance and reaction time.	
15	Resources expended on creating defensive capabilities divert resources from the development of combat power and the ability to gain command of the domain.	Control of a commons can be temporary or permanent in nature, depending on operational objectives: Control is necessary for effective projection of power to another domain.	
16	Destruction of the enemy's capability to use a domain is necessary to gain command – a good offense is the best defense.	One type of force is incapable of fully exploiting a domain: Both specialized counterforce and attack units are required.	
17	Efficacy of national power development across all domains requires coordination across national interests	Gaining domain control requires elimination of the enemy's ability to enter the domain.	
18	Full development of domain power requires an independent organization within the military command structure to provide equal footing between all domains.	As long as a commons is uncontrolled, any point within the domain or along its seams is vulnerable to attack.	
19		Control of the domain allows the controlling force to influence use of other domains across domain boundaries as desired.	

Seversky

Major Alexander P. de Seversky (1894–1974) was born in Tiflis, Russia.[79] He grew up near Saint Petersburg, the son of a wealthy poet and actor whose love for mechanical things led the family to purchase two aircraft in 1909; perhaps the first privately owned aircraft in Russia.[80] Sent to military school at age 10, young Alexander eventually graduated from the Russian Naval Academy in 1914 at age 20. Commissioned an ensign, he served with the Russian Navy at sea for several months before his transfer to the flying service. His first aircraft solo in March of 1915 was the beginning of a lifelong passion for flight that would become the focus of his life.

Shortly after earning his wings, Ensign Seversky participated in his first combat mission, in July 1915. Shot down in an inauspicious beginning to his aviation career, his aircraft crashed into the sea. Rescued, he survived but lost his right leg below the knee.[81] After eight months of convalescing he returned to active duty with an artificial leg and received assignment to the Russian aircraft production program. As an aircraft designer, he worked on aeronautical devices, such as hydraulic brakes, split flaps, and adjustable flight controls, an experience that taught him the intricacies of aircraft design and production.[82]

---

[79] Much of the background information regarding the life of Seversky here is from Alexander Procofieff De Seversky, *Air Power: Key to Survival* (New York, NY: Simon and Schuster, 1950), 353-54. Information regarding his life is contained in a note about the author added by the publisher, see also Meilinger, ed. *The Paths of Heaven: The Evolution of Airpower Theory*. Historical note: Today Tiflis, Russia is called Tbilisi, Georgia.

[80] _____, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, 240.

[81] Ibid., 240-41.

[82] Ibid., 240.

Late in 1916, he returned to flying duty, participating in fifty-seven combat missions that included both bombing and air-to-air engagements that resulted in thirteen air-to-air kills.[83] His wartime military exploits earned him the Cross of Saint George, Imperial Russia's highest decoration. The now-Lieutenant Commander Seversky then moved to his next posting in Washington, DC, as part of the Russian Naval mission. These were turbulent times in Russian politics, and after the Bolshevik government took control in 1917, rather than returning to an uncertain future in Russia, he elected to stay in the United States, where he continued his involvement in aviation development.

Working in the aviation industry as a consulting engineer and test pilot for the War Department, Seversky became familiar with the American airmen of the day and was instrumental in the design of bombsights and the first air refueling systems.[84] Determined to stay in the US, he became a naturalized citizen in 1927 and promptly received a commission as a Major in the US Army Air Corps Reserves.[85] In 1931, he founded the Seversky Aircraft Corporation and served as its general manager and chief designer.

As the owner of a successful aircraft company, a well-known aviator, and a successful aircraft designer, Seversky continued to be intimately involved in the development of airpower within the United States. He used his access to military and civilian airpower leaders to share his views on aircraft and aviation

---

[83] De Seversky, *Air Power: Key to Survival*, ix.
[84] Ibid. Seversky met Billy Mitchell in 1921 and even claimed credit for suggesting the water hammer technique used to sink battleships to Mitchell. See Meilinger, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, 242.
[85] ———, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, 243. Seversky was very proud of his commission in the US military and preferred the honorific title Major for the rest of his life.

development. Unfortunately, while Seversky's government contacts attracted aircraft production contracts and his aircraft designs won awards, he was a less-than-ideal company administrator. Frustrated with his lack of attention to the company's operations, his own company board removed him as president in 1939 and renamed the company Republic Aviation.[86] Freed from Seversky's less-than-attentive oversight, Republic went on to become a successful aircraft company during WWII. Similarly, freed from the responsibilities of running an aircraft manufacturing company, Seversky's passion for airpower bloomed as he focused on writing and talking about airpower.

In 1942, soon after the Pearl Harbor attack, Seversky published his book titled, *Victory Through Air Power*.[87] Featured as a Book-of-the-Month Club selection, this work was well received and read by over five million readers; Walt Disney eventually turned the book into a movie.[88] Especially pertinent for the times was Seversky's core message: The use of long-range airpower to defeat Germany and Japan was less costly than either a land or a sea campaign. Here in Seversky's writing, we see his requirement to advocate and educate about domain power potential as well as appeal to public opinion in an effort to break down the traditional resistance to changes in bureaucratic power structures.

As an airpower theorist and advocate, Seversky had two advantages over both Douhet and Mitchell.[89] First, because he was not a serving military officer, he was free to discuss airpower theory and its national security implications

---

[86] Ibid., 245.
[87] De Seversky, *Victory Through Air Power*.
[88] Meilinger, *Airmen and Air Theory: A Review of Sources*, 129.
[89] ———, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, 246.

without the threat of court-martial: a price both Douhet and Mitchell paid.[90] Second, as both a successful pilot and engineer, he was less prone to the exaggeration of aircraft capabilities that plagued the previous two authors. For our purposes here, his writing is helpful because it provides an example of airpower thought committed to paper several decades later than the first two writers and at a time when the new domain had begun maturing from the early pre-theory stage and was taking shape as a more generally accepted body of knowledge. Entering WWII, the overall strategic understanding of airpower had matured to a point where air forces were organizing and equipping to fight from a domain-centric perspective through independent missions such as strategic bombing.

Theory

Seversky wrote *Victory Through Air Power* at a unique moment in the development of the air domain, a period of domain maturation similar to the state of cyber domain development today. Seversky's book uses both interwar experiences and lessons from the first few years of WWII to inform and support his propositions. He uses the example of German airpower to demonstrate both the advantages and shortcomings of airpower theory in use by the Europeans. He similarly uses Japanese airpower experiences to help demonstrate the

> "In the democracies the full growth of air power had been retarded by the inertia and the mental timidity of old-line naval and army leaders with whom the final decisions rested."[91]

[90] Seversky points out that not only can serving military officers be muzzled in their discussions, industrial leaders who rely on good relations with generals and admirals for business are also hesitant to present full-throated criticism. See De Seversky, *Victory Through Air Power*, 286-89.
[91] Ibid., 69.

advantages gained through early adaptation of a national security policy emphasizing air domain preeminence.

In many ways, Seversky's views on airpower mirror those of both Douhet and Mitchell before him. One critical similarity is the requirement for theorists in the new domain to directly address reflexive resistance to changes in traditional national security organization and operations. He is motivated to write in order to overcome institutional resistance to air domain development by educating the public about the vital need for airpower development and thus indirectly bringing pressure on Congress and the Executive Branch to act on its behalf.[92] His more extensive personal experience in combat and the production of aircraft, as well as the advantage of contemporary history, however, do provide for some subtle but important differences between their theories as discussed below.

A shortcoming of Seversky's theory is that like Mitchell before him, he does not fully develop the integration of the air domain with other elements of the DIME, instead focusing more directly on the creation of airpower in both its military and commercial sense without suggesting how this affects the uses of non-military levers of national power. It is easy to excuse this oversight by reflecting upon the circumstances within which he published the book, during the early years of WWII, immediately after Pearl Harbor. It is easy to assume that during this period, a theory of domain development focused on military

[92] An example of this appeal is a listing of his basic convictions, designed to appeal to public opinion and create a sense of urgency for action and national pride. See ibid., 6-7. Seversky believed that because a democratic public pays the price for war, they should be educated on the development of strategy to conduct war. Providing the necessary education was his duty. See Meilinger, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, 248.

requirements would have greater influence and acceptance than one appealing to less martial aspects of international relations.

Similar to the authors reviewed above, Seversky was familiar with contemporary theorists from the air, maritime, and land domains, weaving their concepts into his own theory. Naturally, he was familiar with the works of Douhet and Mitchell, comparing his observations with their works, even dedicating his book to Mitchell, with whom he had worked in the early 1920s. Using historical references not available to Douhet and Mitchell, he provides more refined and grounded observations, walking the reader through the reasoning behind his arguments. For example, to demonstrate inconsistency between Douhet's theory and actual us of airpower Seversky points out that popular uprisings did not follow Germany's bombing of civilians during the Battle of Britain.[93] He then goes on to show that this failure was due to Germany's inability to gain command of the air, itself a product of a shortsighted mix in force structure.[94] Seversky, however, does not limit himself to airpower analogies. Reaching outside of the aviation domain, he describes the air commons as an "air ocean" and pulls in concepts from Mahan, such as the delay between technological development and

[93] Douhet advanced the idea that bombing of populations would cause national moral to break down, resulting in a populist call for an end to conflict.

[94] De Seversky, *Victory Through Air Power*, 65. Here Seversky is challenging both Douhet's propositions that bombing an enemy populace will result in a cessation of hostilities and that a mono-airframe force, consisting of heavily armed bombers (battle planes), is the proper force structure. Although the Germans followed Douhet's advice and attacked an enemy's will to continue fighting through destruction of important and emotionally charged locations (such as the capital city of London), their force structure mix was inadequate to the task. Seversky says that in this case, the Germans did not possess integrated offensive forces to both bomb the city and gain command of the air. Their targets were not airpower-related, and their lack of fighters to accompany the bombers meant they were unable to destroy aircraft that repeatedly rose to defend the city. Seversky described the result as the wholesale slaughter of attacking German aircraft.

its military use and the "fleet in being" concept, to his observations on using and developing airpower.[95] He even ties in the maritime concepts of blockade through observations focused on airpower's ability to cut lines of surface communications.[96]

As with Mitchell and Douhet before him, Seversky believed that the introduction of airpower and the targeting of a nation's war-making capability meant that war had now become total in nature and would become increasingly destructive as nations continued to industrialize.[98] The more industrialized and reliant on lines of communication a nation is, he says, the more vulnerable the nation is to the air-driven total-war concept. With the emergence of airpower, warfare shifted from its historical pattern of overcoming an enemy's means to resist followed by occupation. Instead, modern warfare consists of gaining command of the air followed by destruction of the enemy as a functioning state.[99]

> "All experts agree that air power will play an ever more decisive part in determining the power balance among the nations of the earth."[97]

In presenting his theory, Seversky makes no formal claims to a recipe for airpower development per se. Instead, he weaves his observations together throughout the book and mixes them with pertinent examples that he hopes will appeal to the reader's common sense and develop the understanding that control of the air domain is a prerequisite for gaining control over the surface domains. Seversky, however, does devote an entire chapter to outlining the lessons for

[95] Ibid., 13, 182.
[96] Ibid., 9, 128-30.
[97] Ibid., 3.
[98] Meilinger, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, 258.
[99] De Seversky, *Victory Through Air Power*, 11.

American airpower development drawn from WWII experiences in Europe and East Asia. He hopes these lessons will guide the nation as it prepares for war and presents them in Chapter VI, "Air-Power Lessons for America." While these eleven lessons are not themselves propositions for comparison to other domains, they serve as a means to identify concepts at the heart of his airpower theory:[100]

1. No land or sea operations are possible without first assuming control of the air above.
2. Navies have lost their function of strategic offensive.
3. The blockade of an enemy nation has become a function of air power.
4. Only airpower can defeat airpower.
5. Land-based aviation is always superior to ship-borne aviation.
6. The striking radius of airpower must be equal to the maximum dimension of the theater of operations.
7. In aerial warfare, the factor of quality is relatively more decisive than the factor of quantity.
8. Aircraft types must be specialized to fit not only the general strategy but also the tactical problems of a specific campaign.
9. Destruction of enemy morale from the air requires precision bombing.
10. The principle of unity of command, long recognized on land and on sea, also applies to the air.
11. Airpower must have its own transport.

No land or sea operations are possible without first assuming control of the air above.[101] Seversky identifies this as a principle so widely demonstrated by events that it is the fundamental axiom of modern strategy. Within any given theater of conflict, the exercise of national will upon the surface is impossible if the adversary controls the sky. From this point forward, taking into account the enemy's ability to gain and maintain control of the aerial domain is necessary when determining relative capabilities to exert national will: "Mastery of the air must come first. The air component must establish its authority, or at least

[100] Ibid., 121-52.
[101] Ibid., 123-25.

neutralize the opposition air force, before the surface components can come into full play."[102]

Navies have lost their function of strategic offensive.[104] Defensive aircraft have made it impossible for maritime forces to approach enemy shores for purposes of bombardment or landing troops. They retain their utility for defensive actions beyond the cover of air, but even an adversary without a naval force can prevent their approach across the maritime commons by projection of power in the aerial commons. In other words, the strategic offensive in warfare now rests with aviation forces. Only by surprise are naval forces capable of approaching a coastline without first establishing control of the air. "In short, the struggle for possession of the coastlines, the initial offensive action, is by this time a function of aviation, not navies."[105] The nation's strategically offensive force is the one with the ability to attack an enemy at the greatest range and with the least warning.

> "It has not quite dawned on our military leadership that long-range aviation provides a 'shortcut' – that battleships, the naval equivalent of the Maginot line, can also be ignored by air power."[103]

[102] Ibid., 64-65. Seversky uses the example of the German blitzkrieg as an example of success on land (short-range and temporary command of the air) and their failure to gain air superiority over the English Channel (long-range and enduring command of the air) that prevented any attempt at invasion of Britain.
[103] Ibid., 204.
[104] Ibid., 125-28.
[105] Ibid., 128. On pages 34-37 and 126, Seversky makes the case that seapower is useless without first establishing control of the air. Here he describes Britain's inability to successfully challenge German moves into Norway and Scandinavia despite their overwhelming naval superiority. Although the British initially had success, once German forces were able to capture airfields and move aircraft into the area, they forced British naval forces to abandon their efforts in the face of aerial bombardment and retreat beyond the range of German aircraft.

The blockade of an enemy nation has become a function of airpower.[106] In the face of an adversary's land-based airpower, naval blockades are impossible. The use of long-range airpower, however, still provides the ability to interdict a target nation's lines of communication or attack his ports of embarkation or debarkation, meaning that adversaries can continue to hamper each other's ability to engage in commerce or enter into the domain. Airborne interdiction of trade along commercial and military lines of communication is not limited to the area immediately surrounding a nation's borders. It can occur at any point along the route between the ports of embarkation or debarkation that comes under cover of the aerial forces, making localized control over a portion of a critical line of communication sufficient to exercise blockade functions. By natural extension, this concept applies to the land domain and its lines of communication. Seversky points out that gaining control of the air provides an operating environment for instantaneous blockade of internal and external lines of communication. The addition of internal lines of communication to the blockade concept is a significant addition to the previously surface oriented external blockade concept.

Only airpower can defeat airpower.[107] Seversky presumes the ineffectiveness of ground and point defenses against attack. This leads him to conclude that destroying hostile aviation capability must occur either in the air or at its source within enemy territory. In other words, only air forces can defeat other air forces, a mission that becomes priority number one for an attacking

[106] Ibid., 128-30.
[107] Ibid., 130-31.

force. Success requires both an air-to-air capability and the commitment of sufficient forces to strike aerodromes, industry, and support infrastructure with the goal of gaining command of the air.[108] Seversky, however, also emphasized air-to-air combat as a primary means of destroying enemy air capability, a proposition based on lessons learned from the first two years of WWII and one that distinguishes him from Douhet and Mitchell, who favored attacking airfields and factories as the means to gain command of the air.[109]

Land-based aviation is always superior to ship-borne aviation.[110]

Aircraft adapted to the demands of a naval force – with short take-off distances, reduced loads, structural limitation – are inferior in performance to land-based aircraft. Here Seversky is relying on his engineering and manufacturing background to point out that forces with greatest range, speed, and armament hold the edge when contesting for control of the domain.[111] He does not claim that maritime-based airpower is useless – just that it will become increasingly less relevant as long-range aviation matures. For the meantime, he admits naval aviation has a role to play in controlling the commons beyond the reach of land-

[108] Seversky presents Germany's failure to properly focus efforts on destroying Britain's airpower as one of the reasons it was unable to realize Douhet's vision and bomb them into submission. See ibid., 72-73.
[109] Meilinger, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, 253.
[110] De Seversky, *Victory Through Air Power*, 131-36.
[111] Obviously he does not anticipate the qualitative gap between nations employing advanced technology to maritime aviation and those with a rudimentary air capability. We see this today in the capability of US naval airpower to operate along the coastlines of second- and third-world nations and their inability to operate in the face of advanced air defenses that require the use of land-based stealth airpower to overcoming. All things being equal, however, his statement remains true.

based forces. In the face of land-based forces, however, maritime airpower finds itself outmatched.[112]

The striking radius of airpower must be equal to the maximum dimension of the theater of operations.[113] At the limits of aircraft operating range, the great advantages of airpower, its speed and freedom of action are limited, reducing its operational flexibility. To overcome this limitation, a nation must create intermediate and advanced operating bases to serve as sources of communications, maintenance, and supply.

Creating these airdromes can proceed no faster than land forces are capable of gaining advanced territory, and once created, these advanced areas of operation are themselves vulnerable to enemy attack and require defense. Additionally, these forward bases consume resources, making them a drain on overall combat capability.

The process of gradually advancing the combat radius of airpower slows down surface operations and prevents the immediate direct application of airpower to critical enemy infrastructure. In other words, realizing airpower's true potential requires aircraft with a combat radius to reach the enemy and return to the home station without the need for intermediate bases. Here Seversky is arguing for the most efficient use of national resources in conducting a war.

Rather than expend resources to create intermediate bases, he suggests creating longer-range aircraft with the capability to directly engage the enemy

---

[112] Seversky uses the inability of British naval aviation to challenge German land-based airpower as an example of this early in his work when discussing lessons from early in WWII. See De Seversky, *Victory Through Air Power*, 35.
[113] Ibid., 136-40.

from within a nation's own national borders as the most efficient and effective method of building airpower.[114] He is also arguing to reduce the importance of geography and distance on a nation's ability to pursue national security objectives.

In aerial warfare, the factor of quality is relatively more decisive than the factor of quantity.[115] Here Seversky is emphasizing that in a highly dynamic domain, a qualitative edge allows a nation to set the terms of combat. In a dynamic environment, the attributes of the weapon systems set the limitations of what one can do and the options from which to choose. For example, "if you are faster than our adversary, you can engage him in combat at will and can withdraw at will. The initiative is in your hands."[116] Speed is not his only example of a qualitative edge, although it is the key to maintaining initiative; firepower is the key to successful engagements. The ability to successfully finish off an opponent once engaged is critical to developing domain control. In the absence of speed and firepower, Seversky says, factors such as maneuverability and rate of climb are purely defensive factors.

While Seversky identifies speed and firepower as the important qualities for a fighter aircraft, he also demonstrates the importance of qualitative advantages in bombers. In bombardment aviation, he says, "speed is secondary to

---

[114] For Seversky's discussion of the economy of increasing range instead of creating intermediate bases, see ibid., 138.
[115] Ibid., 140-43.
[116] Ibid., 140. Here he uses the example of the 25 miles-per-hour speed advantage British fighters had and how it allowed them to achieve dominance over the Germans during the battle for the air over the English Channel. This qualitative advantage enabled a British victory over a much larger German force.

load carrying capacity and defensive combat fire power."[117] Possessing bombers with the greatest load capacity, the longest range, and the most powerful defensive armament, he argues, will give a nation the advantage when attacking an enemy's vital centers – not sheer numbers. The challenge for gaining and maintaining a qualitative advantage is to design and manage a production and acquisition process that allows continual incorporation of the latest technology into weapon systems, he points out.

However, Seversky adds, the rapid pace of technology change in an emerging domain allows nations that find themselves behind in domain development to rapidly catch up. He writes that because technology is easily transferable, nations who are late starters can "skip intermediate stages of development and reach out boldly beyond the present confines of aviation types" to develop their capabilities quickly and without regard to outdated concepts or design.[118] It is necessary to outthink the adversary, create a proper mix of forces, a mix that allows one to both control, and project power from the domain simultaneously. It is the quality of the forces and their organization to task, not their quantity, that is important to domain control.[119]

Aircraft types must be specialized to fit not only the general strategy but also the tactical problems of a specific campaign.[120] Here Seversky is further differentiating himself from Douhet's battle plane concept. A challenge to

---

[117] Ibid., 141.
[118] Ibid., 5.
[119] Ibid., 6, 205. Seversky points out to his readers that the US is well behind the European powers in developing the air domain; however, unlike others that have locked in their designs for mass production, the US can take advantage of the latest technology and designs to organize airpower along the lines.
[120] Ibid., 143-44.

force development is striking a balance between minimizing the various types of aircraft in a fleet for the sake of efficiency, on one hand, and the specialization of aircraft to cover all tactical contingencies, on the other; this process results in a compromise of design. Specialization means that in order to maximize speed, range, altitude, or load-carrying capacity, one of the other factors must suffer.

To overcome this challenge, a nation must outthink the enemy by investing in specialization when the military objective is important enough to warrant the additional expense and effort.[121] This sort of foresight requires decision makers with prerequisite familiarity with tactical and operational demands as well as equipment capabilities, he argues – in other words, well versed in the domain and guided by theory.

Destruction of enemy morale from the air requires precision bombing.[122] Directly challenging Douhet's proposition that bombing of an enemy's population would shatter popular morale and the will to continue fighting, Seversky observes that early bombing efforts during WWII cast doubt upon that expectation. Contrary to expectations, civilians can "take it," he says. From his perspective, poor results from attempts to terrorize civilian populations through uncoordinated and imprecise bombing mean that the cost of these missions is greater than the benefits returned.

Instead, he advocates attacks focusing on critical elements of national infrastructure using precision bombing. The precision use of airpower fits in with

[121] To illustrate his point, he mentions Germany's use of general purpose bombers to strike England instead of creating specialized bombers for long- and short-range missions with various load and performance capabilities. See ibid., 144.
[122] Ibid., 145-47.

his concept of the air-blockade because it removes what he terms the implements and channels of normal life, resulting in the widespread loss of the will to fight. Following this logic, the more highly industrialized a society is, the more vulnerable it is to modern aerial warfare.[123] Seversky, however, is not closing the door on the use of indiscriminate bombing. He notes that its use can be provocative and therefore has a role in strategic and operational planning. For instance, raids focused on attacking adversary population centers are useful for drawing defensive forces up for aerial combat or exposing a government to widespread criticism for neglecting to defend a target–regardless of the operational and strategic benefits of preserving forces.[124]

The principle of unity of command, long recognized on land and on sea, also applies to the air.[125] In what the reader should recognize as an argument similar to Douhet and Mitchell before him, Seversky calls for creation of a separate air force to manage airpower development. Saying that the air domain makes no distinction between the land and sea beneath it, he describes the domain as a continuous "air ocean" without geographical barriers. Using this logic, he concludes that because the domain makes no distinction for the surface over which it exists, neither should a nation's organization to develop airpower; the use of meaningless artificial geographic characteristics are a holdover of two-dimensional surface-based thinking.

---

[123] Ibid., 147.
[124] To make his points, he uses the German bombing of London in an attempt to draw out the British for aerial combat and the Japanese bombardment of Manila in an attempt to force MacArthur to choose between preserving his limited air forces for combat support or dividing his airpower in order to demonstrate American commitment to the city. See ibid., 146.
[125] Ibid., 147-49.

Seversky's point is that continued application of two-dimensional thinking will not result in the development of airpower, but instead in the development of auxiliary weapons for surface operations. Unless separated from the constraints of support to army and naval operations, airpower will remain woven into surface forces and not fully developed.[126] Developing the expertise necessary for operations, training, and acquisition of air domain assets requires creation of a separate service, equal with the army and navy, and overseen by a secretary at its head.[127]

In addition to his calls for a separate service, Seversky joins our previous air theorists in calling for the creation of a department to oversee and coordinate all military forces, integrating their development, operations, and training.[128] Distinguishing his calls for creation of a defense department from the need to create a separate air force, he uses the German High Command as an example, pointing out the successful use of centralized oversight, before the advent of airpower, to provide coordination and unity of command.

Airpower must have its own transport.[129] Seversky argues for development of organic airborne transportation infrastructure within the military to facilitate movement of personnel and materials quickly within and across operating theaters. Development and acquisition of aircraft specialized for such movements, he argues, speeds up delivery of critical assets, and improves military

[126] Ibid., 269.
[127] Ibid., 187, 292.
[128] Ibid., 256-57.
[129] Ibid., 149-52.

flexibility.[130] This line of reasoning ties back into his arguments for the creation of a separate air force capable of envisioning and championing full development of the domain.

In addition to the eleven lessons above, it is possible to derive several additional propositions from Seversky's work. The requirement for national, commercial, and industrial development in creating a domain power is a theme he returns to several times. Although unlike Mitchell, he does not overtly advocate for direct government support and aid in developing the commercial sector, he does point out that the government plays a vital role on setting standards and coordinating civil-military development.[131] For instance, he states that in times of war, airpower forces use commercial infrastructure extensively, and therefore commercial "development must be scientifically meshed into the military-aeronautical structure."[132] This is, however, a continuation of the government-commercial integration theme developed by the previous theorists. Like Mitchell, Seversky is arguing that a nation must begin to see itself as an airpower nation, looking toward development of air domain capabilities across academic, industrial, and governmental sectors as the bedrock of its future national security.[133]

Similar to Douhet and Mitchell before him, he identifies that occupation of territory is not the goal of modern warfare – destruction of the enemy's ability to

---

[130] He uses the example of Germany's successful delivery of troops, equipment, and supplies in Norway and Crete to highlight his point.
[131] De Seversky, *Victory Through Air Power*, 294-95.
[132] Ibid., 295.
[133] Adapted from Meilinger's comment that Seversky believed "America must see itself as an airpower nation and look skyward for its destiny." See Meilinger, ed. *The Paths of Heaven: The Evolution of Airpower Theory*, 268.

fight is.[134] Because airpower can directly attack enemy vital centers, as long as command of the air is in doubt, support to surface forces squanders limited airpower resources. Although such support significantly aids surface operations, it ties up an inherently strategic weapon.

Like Mahan and Douhet before him, the speed and flexibility of air forces reduces the importance of distance and geography, making every part of the globe vulnerable to air attack. This constant vulnerability makes isolationism as previously practiced impossible–no longer are the oceans insurmountable barriers to attack.[135] Rather than continuing to ignore this fact, he recommends embracing it, saying that overcoming these geographic boundaries places the United States at the commercial crossroads of the world for traffic across the oceans and over the poles.

Fundamentally, Seversky argues three items. First, the aerial commons changes warfare because it bypasses enemy surface forces, allowing direct attack of the enemy's war-fighting capability. Second, airpower and domain development requires a separate and distinct organization within the government to manage its development though creation of standards and integration of both military and commercial use of the domain. Finally, the military requires organizational oversight in the form of a department of defense to integrate and/or coordinate development and use of military forces.

---

[134] Ibid., 252.
[135] De Seversky, *Victory Through Air Power*, 19-21.

Seversky's elements of analysis

Victory Through Airpower was a powerful book, published at a critical time in the development of the air domain. Its use of contemporary examples from the early years of WWII helped connect the theory of airpower it proposes with the required policy actions and recommendations for developing airpower as the United States entered the conflict. The elements of analysis drawn from Seversky's work are very similar to those of the previous air theorists but include some unique aspects based on an additional 20 years of experience in the domain. Some elements of analysis reflect combinations of Seversky's eleven recommendations for the development of airpower that apply universally to domain development; others the author infers from the full text. The elements of analysis are:

1. Gaining command of a domain and projecting power across domain boundaries require different forces.
2. Gaining control of the domain requires denial of the enemy's ability to enter the domain or complete destruction of his domain forces.
3. Enduring control of the domain is only possible through attrition and eventual destruction of the enemy's domain-centric forces.
4. Domain control consists of two phases: gaining control of the domain followed by projection of power from the domain.
5. Cross-domain power projection allows control or blockade of lines of communication in other domains.
6. New domain theory must simultaneously educate and advocate for domain power development.
7. Commercial technology development is superior to government development.
8. Transportability of technology means late adaptors can jump ahead of those with locked production of equipment.
9. Speed and flexibility reduce the importance of geography.
10. Efficient use of national resources means development of forces with the longest range and greatest striking power possible.

11. Government involvement to set commercial standards is necessary to coordinate commercial/government use of the domain.
12. National strategic forces are those with the greatest range and power.
13. In technology-driven competition, marginal quality advantages are relatively superior to quantity.
14. Forces and personnel must be specialized to fit not only a nation's general strategy but also the tactical problems of a specific campaign.
15. Destruction of an enemy's means to resist is more effective than directly targeting his morale and population directly.
16. The principle of unity of command applies to all domains.
17. Creation of a separate domain-centric force is necessary for proper domain power development.
18. The projection of power across domain boundaries alleviates the need to develop dominant domain-centric forces in all domains.
19. Blockade of internal lines of communication is possible because overlying domains mean overlying boundaries.

The addition of this final set of elements to the air domain analysis continues several themes: advocating for a separate service, requiring commercial and military coordination in development of the domain, and requiring a nation to gain control of the air domain during the first stages of a conflict. More so than the other authors, Seversky's elements also emphasize the ability to project power across domain boundaries in order to control lines of communication and not just to attack an enemy's physical infrastructure as a means to victory. The completed chart of air elements appears below and as Appendix II.

Table 6: Air Domain Elements of Analysis - Seversky

Air Domain Elements of Analysis			
	Douhet	**Mitchell**	**Seversky**
1	Governments must encourage the development of commercial infrastructure and industry to develop national economic and military power.	Use of domain power should focus on defeating an adversary's will and capability to engage in conflict.	Gaining command of a domain and projecting power across domain boundaries require different forces.
2	Commercial and military interests in the global commons overlap, requiring national-level organization for military and civil development in a coordinated and efficient manner.	Power in a technology-dependent domain depends on military and commercial development of personnel, infrastructure, technology, and industry.	Gaining control of the domain requires denial of the enemy's ability to enter the domain or complete destruction of his domain forces.
3	The ability to bypass fielded forces makes an enemy's will and capability to resist the strategic objective.	Development of personnel to exploit a domain is as important as the technology to enter the domain.	Enduring control of the domain is only possible through attrition and eventual destruction of the enemy's domain-centric forces.
4	Command of a domain from which effects are projected provides protection and allows one to directly target an adversary's means, and will to resist	The willingness of a government to use incentives for stimulation of commercial industry and infrastructure determines domain power.	Domain control consists of two phases: gaining control of the domain followed by projection of power from the domain.
5	In the absence of geography, chokepoints develop at access points to the domain.	Commercial development of technology is faster and more efficient than government development.	Cross-domain power projection allows control or blockade of lines of communication in other domains.
6	Efficiently targeting an adversary's domain power requires targeting domain access points, not units currently within the domain or along lines of communication.	Central guidance ensures that military and civil development occurs in a coordinated manner (Department of Defense, national civil administration).	New domain theory must simultaneously educate and advocate for domain power development.
7	The elimination of geography as a factor in movement and increased speeds of travel reduce the warning and reaction time nations have to respond to attacks.	Military and civil organization for exploitation of a domain must focus solely on that domain (separate service).	Commercial technology development is superior to government development.
8	Increased mobility makes defense of a global commons resource-prohibitive.	Geography determines domain power potential through access to resource, creation of incentives, development of national character, and force structure requirements.	Transportability of technology means late adaptors can jump ahead of those with locked production of equipment.

9	The relative strength of domain power at the onset of conflict is a significant determinant of which nation will gain command of the domain; once reduced, it cannot be rebuilt quickly.	Absent geography, chokepoints occur at points of entry into a domain.	Speed and flexibility reduce the importance of geography.
10	Forces in a global commons are primarily offensive in nature.	Recreation of domain power during a conflict is not possible due to destruction of industrial means and long lead times.	Efficient use of national resources means development of forces with the longest range and greatest striking power possible.
11	Given the offensive nature of forces, they should consist of combat power to deny enemy use of the domain and reconnaissance.	Speed, flexibility, and the vastness of a commons complicate development of robust defenses, making highly mobile forces offensive in nature.	Government involvement to set commercial standards is necessary to coordinate commercial/government use of the domain.
12	Forces designed for combat in a global commons must exist as a fully trained "capability in being" before conflict erupts.	Defense of vital points in commons is necessary to ensure access/use of the domain (points of domain access and vital national infrastructure).	National strategic forces are those with the greatest range and power.
13	Bypassing fielded forces allows direct targeting of all means of resistance, including a population's will to endure bombardment.	The lack of warning before an attack means that forces in the domain must constantly be prepared to defend vital points.	In technology-driven competition, marginal quality advantages are relatively superior to quantity.
14	The lack of predictable targets and set lines of communication makes defense of global commons is resource-prohibitive.	The ability to influence across domain boundaries decreases the importance of traditional defenses such as distance and reaction time.	Forces and personnel must be specialized to fit not only a nation's general strategy but also the tactical problems of a specific campaign.
15	Resources expended on creating defensive capabilities divert resources from the development of combat power and the ability to gain command of the domain.	Control of a commons can be temporary or permanent in nature, depending on operational objectives: Control is necessary for effective projection of power to another domain.	Destruction of an enemy's means to resist is more effective than directly targeting his morale and population directly.
16	Destruction of the enemy's capability to use a domain is necessary to gain command – a good offense is the best defense.	One type of force is incapable of fully exploiting a domain: Both specialized counterforce and attack units are required.	The principle of unity of command applies to all domains.
17	Efficacy of national power development across all domains requires coordination across national interests	Gaining domain control requires elimination of the enemy's ability to enter the domain.	Creation of a separate domain-centric force is necessary for proper domain power development.
18	Full development of	As long as a commons is	The projection of power across

	domain power requires an independent organization within the military command structure to provide equal footing between all domains.	uncontrolled, any point within the domain or along its seams is vulnerable to attack.	domain boundaries alleviates the need to develop dominant domain-centric forces in all domains.
19		Control of the domain allows the controlling force to influence use of other domains across domain boundaries as desired.	Blockade of internal lines of communication is possible because overlying domains mean overlying boundaries.

The review of air theory presented here briefly touches on the writings of these three theorists yet identifies fifty-eight elements of analysis for comparison both to each other and across domain boundaries. In addition to the maritime theorist's focus on the role of geography and human factors in developing domain power, the air theorists add discussions of governmental organization and cross-domain power projection. Having identified elements of analysis from both the air and sea domains, this review now transitions to an assessment of these elements in order to identify common themes both within each domain and across the domain boundaries. After identification of these common elements of analysis in Chapter 6, Chapter 7 assesses their suitability to guide cyberpower development.

Chapter 6: Extant Domain Analysis

The preceding two chapters identified elements of emphasis and relevance from within the maritime and air domain theories. Appendices I and II reflect the results of this individual domain analysis. The task of this chapter is to apply the process of methods of agreement and methods of difference to tease out both universal and unique elements of domain power from the five subject theorists highlighted in this dissertation. This effort creates the intellectual basis for this research project's animating theme: determining if extant military domain theory can serve as the theoretical basis from which to develop cyber policies and strategies.[1]

This chapter begins by grouping together common intellectual trends from within the elements of comparison developed in Chapters 4 and 5 to identify common universal trends and outlying elements for further analysis. The chapter then moves to a second assessment of the individual elements of domain power, using the methods of agreement to group these elements thematically. This alternate application of the methods of agreement identifies broad independent variables responsible for determining a nation's domain power potential (which becomes the dependent variable). The outcome is the creation of a model for use in determining a nation's potential for becoming an enduring power within a domain.

---

[1] As a reminder to the reader, the research questions presented in Chapter 1 are:

Q1: What is the theoretical basis from which to develop cyber policies and strategies?

Q2: Can existing military domain theory inform the development of a starting point for a domain control theory of cyberspace?

Assessing Individual Elements of Analysis

This section consists of two distinctly different applications of methods of agreement to evaluate the elements of comparison generated in Chapters 4 and 5. First, the elements are each grouped with similar elements to identify common ideas and concepts. Combining these groupings creates one general element reflecting the overall intellectual thrust of these similar items. The second analytical perspective is to group all elements by general theme. This analysis identifies areas of common emphasis across the domain theories that will presumably travel over into the creation of cyber domain theory.

The discussion of maritime domain theory in Chapter 4 identified a total of thirteen elements of analysis from Mahan and eleven from Corbett for twenty-four maritime elements. Similarly, the review of the air domain theories in Chapter 5 identified eighteen elements of analysis for Douhet, nineteen for Mitchell, and nineteen for Seversky, a total of fifty-six separate air elements, and a grand total of eighty individual elements of comparison across both domains. Before beginning this chapter's first assessment, it is important to note that the number of elements and their widely varied nature preclude a detailed discussion of each element from each theorist. Fortunately, the elements across all five theorists are generally similar in nature, lending themselves to grouping by theme and subject matter.

In order to analyze these elements in an orderly manner, each is identified in the text below by the name of the author from which they are drawn and the row number appearing on the left-hand side of each domain's element chart in the

Appendices (Maritime Elements: Appendix 1; Air Elements: Appendix II). For example, **Mahan 1** refers to Mahan's elements of analysis, row one, as found in Appendix I: *Domain power depends on the creation and maintenance of both strong military and commercial use of the domain*. Having established this reference system, we now begin the process of identifying common elements of domain power.

Common elements of domain power

Placed side-by-side in tabular form (see Appendix I and II), a thorough reading of all eighty elements generated in Chapters 4 and 5 identifies common concepts that reappear across the five theories and across both domains. These patterns consist of comparative elements that are stated or phrased uniquely but are nevertheless intellectually similar. Combined together, these intellectual family members become *Common Elements of Domain Power,* constituting propositions for creation and use of domain power in a global commons.

The results of this simple comparative exercise, a list of eleven common elements of domain power, appear below.[2] To allow the reader to recreate the inductive mental associations that generated these common elements, the accompanying footnotes list each of the individual elements of comparison that contributed to their synthesis for cross-referencing with Appendices I and II. A full tabular form of these groupings appears in Appendices III.

[2] Here generalized elements for domain power are created using inductive reasoning applied to specific examples gleaned from the five reviewed theories. In Chapter 7 deductive reasoning applies the elements produced here to the cyber domain in order to identify relevant points of focus for cyber theory development.

Common Elements of Domain Power

1. The use of domain power to exercise domain control ensures freedom of action within the domain while denying the adversary freedom of action. Cross-domain power can exercise cross-domain control.[3]
2. The objective of exercising domain power in a commons is to affect an enemy's will and means to resist.[4]
3. Governments must emphasize strategic development of domain power through incentives, coordination of military/civilian development, and treaties as part of its long-term national strategy.[5]
4. Domain power development is a subset of overall national power across the DIME.[6]
5. Simultaneous military and commercial domain development are necessary to become an enduring domain power.[7]
6. Creation of domain power must occur before a crisis or conflict begins.[8]
7. Control over chokepoints where lines of communication converge or terminates is the most efficient means of exercising domain control and leads to enduring domain control.[9]
8. The exercise of domain power is a multi-step process: first, gaining command of the domain, and then exercising command of the domain (to include projection of power across domain boundaries).[10]
9. Gaining domain control means eliminating the enemy's ability to enter the domain or use its lines of communication.[11]
10. A nation's geography affects its domain power potential, vulnerability to attack from the domain, influence over lines of communication, and incentive to develop domain power.[12]
11. A nation's population affects domain power through the creation of domestic reserves of both personnel and knowledge available in times of need.[13]

The intellectual continuity demonstrated by the reoccurring nature of these elemental themes, between theorists and across both domains, suggests that these

[3] Mahan: 5; Corbett: 2, 3, 6; Mitchell: 9, 17, 18, 19; Seversky: 18
[4] Corbett: 3, 6; Douhet: 13, Mitchell: 1; Seversky: 15
[5] Mahan: 13; Douhet: 2, 9, 12, 17; Mitchell: 2, 4, 6, 10; Seversky: 11
[6] Corbett: 1; Douhet 2, 17; Mitchell: 6; Seversky 10
[7] Mahan: 1, 2, 3, 4; Douhet: 1; Mitchell: 2, 4, 5; Seversky: 7, 11
[8] Mahan: 13; Corbett: 1, Douhet: 4, 10, Mitchell: 1, 10, 13; Seversky: 8, 14, 15
[9] Mahan: 3, 4, 8, 9: Corbett: 2, 3, 8; Douhet: 5, 6; Mitchell: 9, 12; Seversky: 2
[10] Corbett: 10; Mitchell: 14, 15, 16, 18, 19; Seversky: 1, 4
[11] Mahan: 6; Corbett: 6, 9; Douhet: 9, 11; Mitchell: 9, 10, 17, 18; Seversky 1, 2, 3
[12] Mahan: 8, 9, 10; Corbett: 8; Mitchell: 8
[13] Mahan: 11, 12; Mitchell: 2, 3

eleven common elements are universal to theories of the domain control of a global common and therefore have the potential to travel into the cyber domain.

Domain and theorist unique elements

Despite the overwhelming commonality of the elements of comparison, there are differences between theorists and domains that merit discussion. The following sections identify and discuss these variations in intellectual concepts and disagreements in order to determine their suitability for inclusion as an element of domain power. Domain unique characteristics or domain-centric technology causes some of these disagreements. A few, however, result from a particular insight on the part of one of our theorists. What follows are eight brief sections of analysis: one based on an element that is domain-specific, five that focus on elements of disagreement across domains or theorists, and two unique elements of analysis that appear in only one of our theories yet show potential for cross-domain application.

Domain-specific element

- Domain power development requires the creation of domain-specific governmental institutions and cross-domain coordinating bodies (separate service, Department of Defense, domain-specific commercial oversight).[14]

Unique to the air domain, this element of comparison plays a prominent role in the theories of Douhet, Mitchell, and Seversky. It is the animating theme from their writings and stems from the perceived need to overcome existing organizational resistance to the air domain's development. Entry into the air

[14] Douhet: 17, 18; Mitchell: 6, 7; Seversky: 14, 17

domain required the use of radically new technology and challenged conventional relationships and roles within both military and civilian organizational structures. For these reasons, their writings worked to both educate and advocate, developing a common understanding of the domain.

The maritime theorists' failure to include the requirement for a separate service is understandable, as navies were already in existence during their time of theoretical development. The maritime theorists' lack of focus on the requirement for a Department of Defense–like coordinating body, providing oversight of national power development through coordination of multiple domains, is a bit more puzzling. This failure likely stems from their reliance on traditional inter-service relations. They had no need to focus on the issue because the new maritime technologies presented a minimal threat to long-established bureaucratic spheres of responsibility.

Without insight into the difficulties of creating national power in an entirely new domain, the omission is likely one of oversight. Because the challenges faced by our air theorists will likely be repeated during the opening of any new national security domain, this element of analysis will be added to our list as: *Domain power development requires the creation of domain-specific governmental institutions and cross-domain coordinating bodies.*

Elements of disagreement between theorists and domains

1. The first area of disagreement is over the nature of forces and the relative strength of both offensive and defensive operations within the domain.

This disagreement is the result of clashing elements of analysis from both the maritime and air theorists.

a. First is the maritime assertion that defensive operations are the stronger form of warfare, making offensive operations the purview of the stronger force.[15]

b. Second is the air theorists' assertion that the ability to bypass traditional defenses and strike across domain boundaries makes domain forces offensive in nature.[16]

Disagreement over the nature of forces in the two domains occurs because during the early decades of air power, air defense capabilities were practically nonexistent (the period when our theorists were writing). For the air domain theorists, the addition of a third dimension revolutionized warfare, enabling a nation to reliably bypass traditional defenses and quickly strike anywhere, making defense impractical.

Without a true defensive capability in the domain, knocking out an adversary's ability to use the domain becomes the only means of defense. Destroying the enemy's domain-centric forces then becomes the priority and according to our air theorists, makes air domain force offensive in nature.

Today, with the benefit of extensive airpower history and an understanding of the maturity of air defense weapons, we know that air domain power is not inherently offensive in nature. Air defense assets can deny an enemy access to vital points and can wear down an attacking force, effectively

---

[15] Corbett 4, 5. Appearing directly in Corbett's theory, this sentiment is in line with traditional land domain thinking. While it is true that a pendulum swing between offensive and defensive armament can affect this statement, in general this is an accepted fact for surface forces. For a discussion of the advantages of defense, see Clausewitz, *On War*, 357-59.

[16] Douhet: 3, 8, 10, 15, 16; Mitchell: 11, 14, 18; Seversky: 9, 10

eliminating an adversary's airpower through defensive action. Seversky begins to touch on this with his discussion of the Battle of Britain but never quite makes the intellectual leap to disagree with Douhet and Mitchell.

Additionally, the ebb and flow of technology means that in any domain, the balance between offensive and defensive capabilities is fluid. For almost every advance in technology, a counter development swings the pendulum in the other direction. As a result, over the long term, the balance between offensive and defensive forces on the sea, land, and air has constantly shifted. In the end, the only conclusion is that the nature of force in both domains is technological in nature; fluctuations in technology result in changes in the dominant characteristic of force.

With that in mind, determining and anticipating the dominant characteristic of force is an important point of discussion for any theory intended to guide policy makers in developing domain power. Identifying the current and future role of force is an integral part of domain power development. For this reason, we include an element of analysis capturing that determination: *The state of domain technology determines the dominant character of domain forces*. When combined with *Common Element* 6 above, this element informs theorists and policy makers about the potential domain power strategies a nation can and should pursue.

2. A second element of disagreement among theorists is the proper target for offensive operations directed at an enemy's will and ability to resist.

Again, closely tied in with *Common Element* 12 above, this discussion informs proper domain strategy and force development. Unique among the

theorists here, Douhet advocates the use of force against a nation's general population in order to break their will to fight.[17] He is theorizing that a population will not stand for destruction of its way of life.

Seversky, Douhet's fellow air theorist, through an analysis of the Battle of Britain, directly counters this proposition. In *Victory Through Air Power*, Seversky provides an example in which an urban population endured aerial bombing without bringing pressure on their government to cease hostilities. Mitchell also addresses this issue, directly rejecting the targeting of a population in favor of focusing on a nation's means to resist, which in turn will reduce their will to continue fighting.[18]

In their writings, the maritime theorists present a view that is similar to Mitchell's. They advocate for attacks on military forces to reduce an enemy's means to resist and for restrictions on trade, using blockades and interdiction, to decrease a nation's will and ability to resist.

The outright discrediting of Douhet's proposition by Seversky, in conjunction with the positions expressed by our other theorists, means that Douhet's proposition is not universal.[19] It will not be included as an element of domain power.[20]

---

[17] Douhet: 13, 14
[18] Mitchell: 1
[19] Douhet envisioned all-out war using poison gas against civilians in addition to attacks against a city's physical infrastructure. A reader may argue that Douhet's vision has been realized with the invention of nuclear weapons. This argument is valid in total existential warfare but is unlikely to play a significant role in guiding the development of cyber theory, cyberpower, and cyber forces.
[20] Added to the lack of theoretical and historical support for its inclusion is that with the benefit of further experience in total war, it is apparent that Douhet overestimated the

3. A third source of disagreement between elements is the degree of control over a domain that a nation should pursue during conflict.

In Mahan's theory, he suggests that without destruction of an enemy's fleet it will retain the capability to strike within the global commons, disrupting use of the domain; essentially, he is advocating the pursuit of permanent domain control.[21] Corbett takes a more nuanced approach. He accepts that permanent domain control is beneficial but points out that pursuit of national interests may require only temporary or local control over a domain (such as in the vicinity of a convoy).[22] Obviously, there is a discrepancy among the maritime theorists.

The air domain theorists all fall down on the side of Mahan, suggesting that the enemy's retention of any capability to use the domain is unacceptable.[23] They, like Mahan, advocate the use of domain-centric forces in pursuit of permanent domain control as a necessary first step before domain exploitation. A key component of this majority opinion is the assumed inability to reconstitute forces rapidly.[24]

---

fragility of modern society and that international legal, social, and moral norms prohibit the type of campaign Douhet envisioned – regardless of the domain in question.

[21] Mahan: 6, 7. This shapes policy toward the development of large fleets consisting of capital ships capable of engaging and destroying an enemy fleet.

[22] Corbett: 2, 7, 9. Corbett too recognizes the potential to destroy an enemy's domain capability, saying that permanent domain control is a possibility, just not necessarily a necessity. His arguments are over the scope of control necessary and the proper apportionment of national effort. Corbett emphasizes exercising domain control, which emphasizes the development of forces consisting mostly of cruisers vs. the capital ships Mahan prefers.

[23] Douhet: 4, 8, 10, 11, 15; Mitchell: 12, 15, 17, 18, 19; Seversky: 2, 3, 4. The airpower theorists point to the lack of defensese against any enemy use of airpower; If the enemy can enter the domain, it can strike your vital points.

[24] Large-scale production of forces in both domains requires advanced technology and large production processes. These processes require long lead times to ramp up to full production under the best of circumstances.

Despite Corbett's arguments, the overwhelming theme among these theorists is to pursue complete domain control as an initial phase of operations.[25] As a result, the extent of domain control possible will be designated a common element of analysis and included in this discussion as: *The pursuit of domain control is the primary function of domain-centric forces*.

4. The fourth source of disagreement occurs between the maritime and air theorists over the existence of geographically created chokepoints along lines of communication.

Both maritime theorists emphasize the role of geography in creating lines of communication and chokepoints where lines of communication converge.[26] While in many cases these critical locations are at the terminus of a line of communication (the domain access port), this is not always the case. Often a geographic feature will create natural chokepoints, the control of which allows efficient denial of a line of communication to enemy forces.[27]

Air theorists, on the other hand, point out that the three-dimensional nature of the domain has eliminated geographic chokepoints in the aerial commons. Aircraft are free to choose any course between points (range permitting), which eliminates the discussion of geographic chokepoints as important to air domain control. Instead of using geography, the air theorists narrow the vital points within the air domain down to the domain access point: the airdrome. Gaining domain

[25] Domain supremacy is today's modern term for the level of overwhelming control our theorists advocate.
[26] Mahan: 3; Corbett: 3, 8
[27] Examples include Hormuz Strait, Strait of Malacca, Panama Canal, Suez Canal, Strait of Gibraltar, Cape Horn, and the Cape of Good Hope.

control using vital points in the aerial domain then focuses on denying the adversary's access points while protecting one's own[28]

The key differentiation here is the lack of geography as a factor in the creation of aerial lines of communication. Air domain theorists do not dispute the existence of vital points. They simply dismiss the role of geography, focusing instead on the intersection of lines of communication. Eliminating any reference to geography, a common element of domain power included here is: *Vital points exist as convergences of lines of communication.*

5. The fifth and final disconnect analyzed here concerns the projection of power across domain boundaries. The maritime theorists barely touch upon it, yet it is central to all three air domain theorists.

The reviewed maritime theorists focus on the conduct of maritime operations to gain and maintain control of their domain. Mahan almost exclusively identifies the role of maritime power as *control of the sea*. Corbett expands upon this point to discuss the role of maritime power in support of operations ashore. To Corbett, maritime operations play a supporting role to a nation's efforts ashore; he believed that victory ashore is the primary means of achieving national security goals. Despite this position, he had little to say regarding the ability of maritime powers to directly project power into the land domain. The arguments of both our maritime theorists are for the creation of a strong maritime power but do not focus on doing so at the expense of power in other domains.[29]

[28] Douhet: 5, 7, 14; Mitchell: 9

[29] Mahan did argue that an island nation with a strong maritime capability did not have a need for strong land defenses; it could isolate itself from its adversaries. That, however, is

Air theorists, on the other hand, identify the projection of power across domain boundaries as a primary role for air forces in pursuit of national security objectives.[30] The speed and flexibility of air forces, combined with the ability to bypass traditional defenses, give them the capability to directly target the enemy's means and will to resist. By directly targeting vital centers, airpower, unlike maritime power, has the capability to rapidly bring a conflict to termination on its own. Our air theorists' calls for a separate service and a department of defense are actually intended to ensure development of airpower at the expense of surface forces for this very reason.[31] In other words, a strong air force is capable of reducing the need for a strong naval and land force.

Obviously, these maritime theorists were writing in an age before long-range rockets and sea-launched missiles. Had these technologies existed, they would have likely altered their theories to include a discussion of cross-domain power projection and emphasized its creation in order to affect vital points ashore. We can infer this because both Mahan and Corbett clearly understood that control of vital points created control over a commons. Essentially, the failure to develop cross-domain capabilities capable of affecting vital points is to forgo an essential element of domain power. Therefore inclusion of a common element of domain power capturing this understanding is warranted as: *The capability to project power across domain boundaries affects an adversary's will and ability to resist in other domains.*

---

not the same argument the air theorists make about the airpower eliminating or reducing the requirement for maritime and land forces.

[30] Douhet: 3, 4, 13; Mitchell: 1, 14, 18, 19; Seversky: 1, 4, 18, 19

[31] Douhet: 2, 17, 18; Mitchell: 6, 7; Seversky: 16, 17

Unique theoretical elements

1. The more domain power relies on the use of technology, the more quickly and easily a nation can become a domain power.[32]

Two of Seversky's elements of analysis inspire this unique element. First, there is his insight regarding the importance of qualitative over quantitative advantages during the Battle of Britain. The second point is his recognition that by 1942, the rapid pace of technological change affecting aircraft performance meant German and Japanese aviation technology was inferior to new technology due to outdated production designs. This provided the United States an opportunity to quickly obtain a qualitative edge.

Here he is arguing that the proliferation of technology means that the balance of power within a domain can change quickly. Through proliferation, new technology can make current domain power obsolete. Keeping abreast of domain power technology, and investing in its development and maintenance therefore requires coordination of government, industry, and human capital in order to gain and maintain a leadership position. Intuitively, this will become increasingly true as the technological dependency of domain-centric power increases: *Rapidly changing and highly dynamic technology makes creation of enduring domain power problematic.*

2. International trade is critical to development of domain power.[33]

While all five theorists hit upon trade and commercial development to some extent, Mahan is unique in his discussion of international trade as a means

[32] Seversky: 8, 13
[33] Mahan: 2, 3

to gather domain power. He argues that a robust fleet in the maritime domain is a means of creating domain power through constant interaction and association. A strong and competent navy, protecting a robust and professional commercial sector, leads other nations to ship goods within that nation's hulls and to sail under its protection. Today, we would label this a phenomenon of soft power. What Mahan is saying is that as a nation's commercial presence within a domain grows, its influence grows. Through repeated commercial interaction, a nation passively and actively sets standards and norms that others adopt. Knowing this, we will include Mahan's element as: *International trade is critical to creating domain power.*

Gathering the elements together provides 18 common elements of domain power. Developed through deductive analysis these elements are a promising indicator that extant domain theory for the global commons can serve as a basis for the development of cyber theory. The list of these eighteen common elements appears as Appendix IV and in the table below.

Table 7: Common Elements of Domain Power

	Common Elements of Domain Power
1	The use of domain power to exercise domain control ensures freedom of action within the domain while denying the adversary freedom of action. Cross-domain power can exercise cross-domain control.
2	The objective of exercising domain power in a commons is to affect an enemy's will and means to resist.
3	Governments must emphasize strategic development of domain power through incentives, coordination of military/civilian development and treaties as part of its long-term national strategy.
4	Domain power development is a subset of overall national power across the DIME.
5	Simultaneous military and commercial domain development are necessary to become an enduring domain power.
6	Creation of domain power must occur before a crisis or conflict begins.
7	Control over chokepoints where lines of communication converge or terminates is the most efficient means of exercising domain control and leads to enduring domain control.
8	The exercise of domain power is a multi-step process: first gaining command of the domain and then exercising command of the domain (to included projection of power across domain boundaries).
9	Gaining domain control means eliminating the enemy's ability to enter the domain or use its lines of communication.
10	A nation's geography affects its domain power potential, vulnerability to attack from the domain, influence over lines of communication, and incentive to develop domain power.
11	A nation's population affects domain power through the creation of domestic reserves of both personnel and knowledge available in times of need.
12	Domain power development requires the creation of domain-specific governmental institutions and cross-domain coordinating bodies.
13	The state of domain technology determines the dominant character of domain forces.
14	The pursuit of domain control is the primary function of domain-centric forces.
15	Vital points exist as convergences of lines of communication.
16	The capability to project power across domain boundaries affects an adversary's will and ability to resist in other domains.
17	Rapidly changing, and highly dynamic technology makes creation of enduring domain power problematic.
18	International trade is critical to creating domain power.

Common Themes of Domain Power

We now transition to the second analytical perspective introduced above. In this section, we use methods of agreement to look at all eighty elements of comparison and group them, not by intellectual thread as in the previous section, but instead by general theme. Compared in this way, five dominant thematic groupings appear: 1) government's role in domain power development, 2) geography's role in determining domain power potential, 3) population factors in determining domain power, 4) the use of domain power, and 5) domain-specific characteristics. Using the tables in Appendices I and II as before, individual elements falling into each of these five conceptual bins are identified by the associated theorist and then row within the appropriate *Elements of Comparison* table in Appendices I and II. It should be noted that that some elements appear multiple times, across different groupings, because they cut across multiple themes. The thematic breakdown is as follows:

- Government's role in domain power development
  - Mahan: 1, 2, 3, 4, 13
  - Corbett: 1
  - Douhet: 1, 2, 17, 18
  - Mitchell: 2, 3, 4, 5, 6, 7
  - Seversky: 7, 11, 13, 16, 17
- Geography's role in determining domain power potential
  - Mahan: 8, 9, 10
  - Corbett: 8
  - Douhet: 5, 7
  - Mitchell: 8, 9, 12, 13
  - Seversky: 9
- Population factors in determining domain power
  - Mahan: 2, 11, 12
  - Corbett: 1
  - Douhet: 2, 14
  - Mitchell: 2, 3
  - Seversky: 14

- ❖ Use of force to gain and exercise domain power
  - Mahan: 6, 7
  - Corbett: 2, 4, 6, 9, 10, 11
  - Douhet: 3, 4, 6, 8, 10, 11, 12, 13, 14, 15, 16
  - Mitchell: 1, 11, 15, 16, 17, 18, 19
  - Seversky: 1, 2, 3, 4, 5, 10, 12, 13, 14, 15, 18, 19
- ❖ Domain-specific characteristics
  - Mahan: 4, 5
  - Corbett: 4, 5, 7, 10
  - Douhet: 3, 7, 8, 9, 10, 13
  - Mitchell: 9, 10, 12, 13, 14
  - Seversky: 6, 8, 18, 19

These thematic bins provide insight into consistent areas of discussion related to the development and establishment of domain theory across the maritime and air domains. The first three bins focus on factors that directly influence the development of domain power and appear consistent across both domains. For instance, the government's role in creating and maintaining domain power is an underlying theme in many of our elements of comparison.

To various degrees, all five of our theorists emphasize the role of government in driving a nation to develop human capital and take advantage of its natural endowments. Beyond that, however, the government also sets a strategic vision, apportioning resources, and organizing national efforts across the DIME.

Similarly, geography's role in determining domain power potential is a reoccurring theme, within both the elements of comparison and the texts of the reviewed domain power theories. Obviously, access to required natural resources and a central location along lines of communication are critical factors in the development of domain power. Even more important, however, from a theoretical standpoint, is understanding how geography channels the use of a domain (as it

does with maritime operations) or influences a nation's predisposition to develop domain power.

Like the preceding two bins, population factors are important to a nation's ability to take advantage of natural endowments and follow through on governmental efforts to create domain-centric power. As a variable, population is not simply a measurement of the raw number of citizens a nation has. This variable also includes the human capital necessary for domain power development. A large nation that lacks personnel with the prerequisite knowledge, skills, and ability to man, operate, and create domain-centric forces is as limited in its ability to create domain power as one with a small population.

> "Virtually all air theorists have noted that a definition of airpower or aerospace power must include far more than simply machines. It includes also a robust aerospace industry, airframes, engine, avionics, and equipment manufacturers. In addition, air power must also encompass the myriad workers in the commercial and private aviation sectors."[134]

The final two bins, the use of force and domain-specific characteristics, capture elements of comparison that are focused less on development of domain power than on the use of power. These are catchall categories, but that does not diminish their importance; rather, it speaks to the need for domain theory to include domain unique discussions related to the characteristics of each operating environment. The customization of domain theory, by including unique domain-specific elements, helps provide a greater understanding of the domain. An increased understanding in turn informs actions taken by governments as they work to create enduring domain power.

[34] Meilinger, *Airwar: Theory and Practice*, 217.

The consistency of the first three bins, and their central role in our theorists' writings, calls for a more in-depth discussion of their relation to overall domain power development. What follows is an unexpected finding that ties together common themes of government, geography, and population across all five theorists and both domains to suggest a model for assessing a nation's enduring domain power potential.

An Enduring Domain Power Model

Beginning with Mahan's theory of maritime power, it quickly becomes apparent that, to varying degrees, all five of the authors reviewed here hit upon the role of government and geography in determining a nation's domain power potential. Population as a factor is not quite as obvious. While all five authors touch upon population's role in creating domain power, only Mahan and Mitchell delve deeply into its importance. Reflecting back to the review of their theories in Chapters 4 and 5, the reader will remember their respective calls to create seafaring and air-minded nations. The strength and similarity of their arguments appearing across two different domains provide justification for its inclusion as a dominant theme. Further bolstering population's case for inclusion is the fact that these same themes can be inferred from the other three theory's discussions concerning the character of a nation's population, the importance of developing human capital, and the requirement for specialized skills among a nation's citizenry.

If these three dominant themes: government, population, and geography operationalize the elements of analysis, then domain power potential is a function

of government, population, and geography. Of course, each of these three dominant independent variables of domain power potential can be further broken down into non-dominant variables, as we will discuss below.

Domain power potential = Government + Geography + Population

The government variable

The government variable is the most important of the three, because as argued by our theorists, over the long term, it shapes how efficiently a nation utilizes both its population and natural geographic advantages to create domain power. This dominant variable is a function of three non-dominant independent variables that appear in both maritime and air domain theory: industrial policy, regulation, and development of a dedicated bureaucracy. For example, industrial policies such as the subsidization of industry, favorable taxation, and the creation of international treaties encouraging trade are all factors that affect a nation's willingness and ability to develop domain power.

Closely related to industrial policy is the use of regulations to set standards and provide predictable norms of operation within a domain. Predictability and regulation encourage fair commercial competition, which creates a domestic environment friendly to the commercial development of the domain. Increased commercial use in turn leads to the creation of commercial infrastructure and helps contribute to domain leadership.

Finally, the will and capability of a government to create an efficient domain-centric bureaucracy is essential to domain power development. A

functioning bureaucracy not only coordinates the use of industrial policy and regulation, but also coordinates development of domain power across military and commercial lines. It plays the honest broker, providing guidance for allocation of resources and settling disagreements between interest groups who see domain power development as a threat to their own goals.[35]

The geography variable

Geography, as a variable, is itself a function of two non-dominant variables that help determine a nation's predisposition toward domain power. First are the natural endowments of the nation. Natural endowments consist of factors such as access to raw materials and the size and physical layout of the nation. Without domestic raw materials, a nation's domain power potential relies upon its ability to trade for the raw materials necessary to undertake and sustain commercial and military production. Finally, the physical layout of a nation helps determine the population's incentives to exploit the domain for trade and defense.[36]

The second variable is a nation's exposure to the domain, both its physical access to the domain and the nation's location in relation to trade routes or

[35] The bureaucratic element is most apparent in the organizational arguments of the air domain theorists when they call for the creation of a separate service and a functioning department of defense to oversee the allocation and use of resources.

[36] Examples from our authors are England's status as an island nation that served as an incentive to develop maritime power for both defense and trade. France, on the other hand, had better conditions for growing necessary food supplies, and its extensive landlines of communication reduced its incentive to develop maritime capabilities for anything more than military purposes. An air example would be America's development of long-range aircraft to reach across oceans in order to engage adversaries before they can threaten the homeland.

chokepoints. A nation's ability to access a domain and use it for commercial and military purposes is as important as its incentives to do so. An example of this is the importance Mahan placed on good ports and waterways for creating maritime domain power. Along the same lines, the geographic positioning of a nation along chokepoints and along major lines of communication provides the opportunity and incentive to develop domain power. A nation can take advantage of this domain power to either keep a line of communication open or close it as necessary during times of conflict.

The population variable

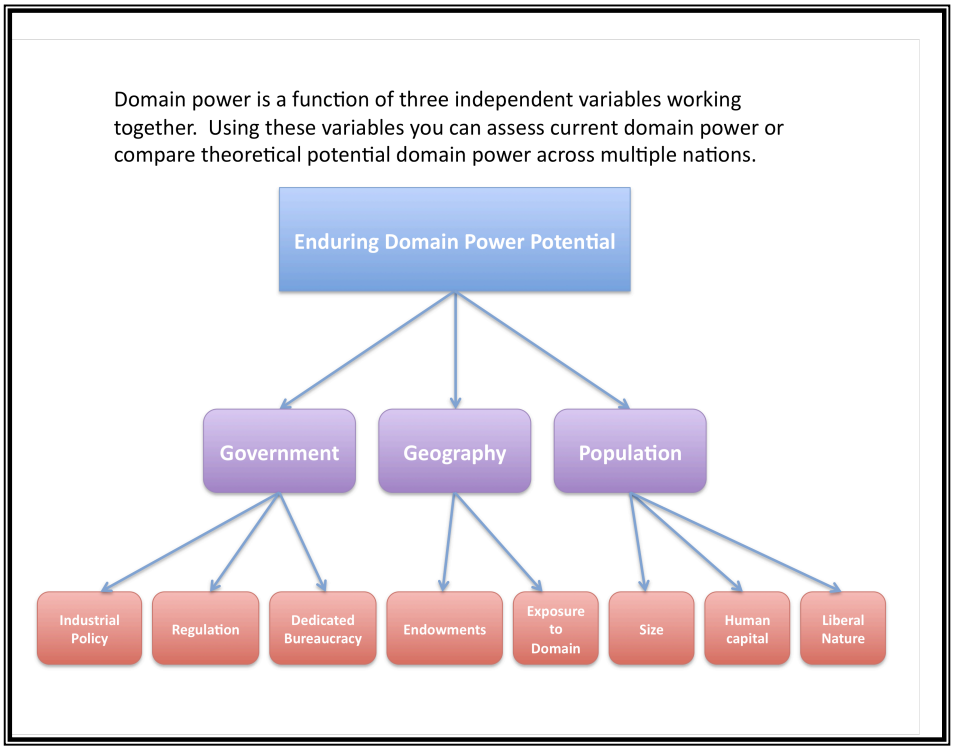
As with the previous variables, the population variable is a function of several non-dominant variables: population size, human capital, and the citizenry's liberal character. Obviously, size refers to the sheer volume of the population, or how large a pool of resources from which the nation has to draw. Regardless of how a nation's geographic endowments or the strength of its government's commitment to create domain power, without personnel to operate domain-centric systems, the upside of its domain power potential is limited.

The creation of human capital refers to both the specialization of domain-centric operators (sailors and aviators) and supporting personnel. Our theorists each emphasized that the creation of domestic industries and commercial use of the domain provide a reserve from which to draw military power in times of need. Tied in tightly with the government variable, the development of domestic human

capital in domain and domain-associated industries is a critical factor in determining a nation's ability to create enduring domain power.

Finally, the liberal nature of a nation's citizens provides a predisposition toward adopting a new domain technology and a willingness to venture forth to use it in new and creative ways. A liberal nature can result from many factors, such as an economic necessity for trade, geographic vastness, or, as in the American case, historical roots in Europe. Regardless of its origin, a liberal perspective provides an outward-looking approach that lowers cultural and social barriers to creating and exploring domain power potential. Taken together, the three independent variables of government, geography, and population are good indicators of a nation's domain power potential. A graphic depiction of their relationship follows:

Figure 4: Enduring Domain Power Potential



This completes the deductive development of elements and variables of domain power. Taking the 18 common elements of domain power developed here and this model of *Enduring Domain Power Potential,* we move to an inductive discussion of cyber domain theory in the following chapter.

Chapter 7: Evaluation of the Cyber Domain

Along with the tools developed in Chapter 6, this chapter uses deductive reasoning to establish the validity of extant theory as a basis from which to begin creating cyberpower theory. The chapter begins with a brief review of the key cyber domain characteristics established in Chapter 3. It then proceeds to a discussion of the similarities and differences between the cyber domain and both the maritime and air domains.

Following the identification of similarities and differences, the chapter continues with an evaluation to determine how well each of the eighteen common elements of domain power travels into the cyber domain. The purpose of this evaluation is twofold: 1) find out if the element travels well into the cyber domain, and 2) determine what cyber theory characteristics this element will address and how cyber theory will incorporate these characteristics.

Having addressed each element, the chapter then moves on to discuss the creation of enduring domain power. Using the domain power potential formula developed in Chapter 6 as a template, we discuss the role of the government, geography, and population in creating cyber domain power.

Following the discussion of domain power potential, the chapter briefly reviews the suitability of each of the two domains and the five individual theories to serve as a model for development of cyber domain theory. Finally, the chapter concludes with a short description of how Winton's five criteria for military theory fit the development of cyberpower theory based on what we have learned from our analysis.

The Cyber Domain

Chapter 3 adopted the following definition of the cyber domain:

> *A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information communication technologies*.[1]

The adoption of this definition established certain characteristics about the cyber domain that the reader should keep in mind during this dissertation's comparisons of cyberspace and other domains. These same characteristics are useful in the follow-up assessment of each of the eighteen elements of domain power. Cyberspace is:

- A domain within the information environment
- Physical in nature
- Characterized by the use of the electromagnetic spectrum to create, manipulate, and move information, giving the domain a virtual nature
- Reliant on technology for its existence, entry, and exploitation

With these characteristics in mind, we now move on to a discussion of the cyber domain's similarities and differences from the maritime and aerial domains. This discussion provides a useful starting point for the application of the eighteen commons elements of domain power developed in Chapter 6.

The Geography of Cyberspace

Quite simply, the cyber domain consists of computer networks and everything connecting them together. Following this general statement with an exacting description of the domain is a difficult prospect. Most cyber scholars admit as much, which is why the definition above provides for both physical and virtual aspects of the domain. The

[1] Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," 28.

domain's geography is constantly changing as new technology makes portions obsolete while simultaneously creating new topographic features.[2] Efforts undertaken to describe the geography of the domain are an inexact science at best. Rather than an exact description of the domain, David Clark, an MIT professor involved in much of the Internet's early development, provides some useful models that help frame the conceptual understanding of the domain.

Clark points out that the computer does not create cyberspace–the interconnection of computers does.[3] Linkages between computers, both physical connections and the coding that allows them to exchange data, define the Internet. Clark uses a four-layer model to describe these linkages:

1. **Physical:** This layer is characterized by the computers, wires, fiber-optic cables, etc., that link systems together.
2. **Logical:** Logical components of code create applications, which in turn provide a service by organizing, manipulating, and routing information over the physical layer of cyberspace. These service applications become platforms that programmers combine in innovative ways to create higher levels of services, a process that is continuously advancing.[4]
3. **Information:** This layer takes many forms: documents, photos, books, music, video, etc.
4. **People:** The top layers of the Internet, where people generate and use information. The character of the users drives the demand for innovation and further developments at other layers.

Attacks, Clark says, can come at all four of these layers: destruction of physical infrastructure, corruption of logical processes, distortion of information, and the compromise of people. Separately, Clark describes the Internet as having both inner and

[2] Geography refers to both physical interconnections and virtual feature such as firewalls and programming language incompatibility. Both the physical and virtual geography of the domain determine where information can travel.
[3] Clark, "Characterizing Cyberspace: Past, Present and Future."
[4] For instance, operating systems allow the creation of data storage and retrieval programs, which in turn allow the creation of more sophisticated programs using this organized data. At each level of sophistication, applications from previous levels combine to perform new and unique services.

edge components. On the edge are the personal computers and servers that use and store information. These systems are what most users and laymen think of as the Internet. The actual heart of the Internet, however, is the combination of physical infrastructure and routers that control the flow of information packets through the network.

Although Clark does not say so, when looking at these two conceptual models for cyberspace–one of layers and the other consisting of an inner and outer circle–we see that both rest upon the foundation of physical infrastructure. Animation of this physical infrastructure is by the use of routers to control the flow of information between computers and data storage on the periphery. The organized flow of information through the domain's internal physical/virtual geography allows computers to access, manipulate, and use data in other locations regardless of where they are located within the world.

Keeping this explanation in mind, from a domain power standpoint, we can then say that the geography of the Internet consists of the physical infrastructure and the routing systems that interconnect elements of the rim. The geography therefore has physical and logical components, much as to what our definition alludes. All users of cyberspace share the physical network and routers controlling the flow of information globally. This is of what the global cyber common consists. Framing the common this way is important to our application of the eighteen elements of domain power later in this chapter.

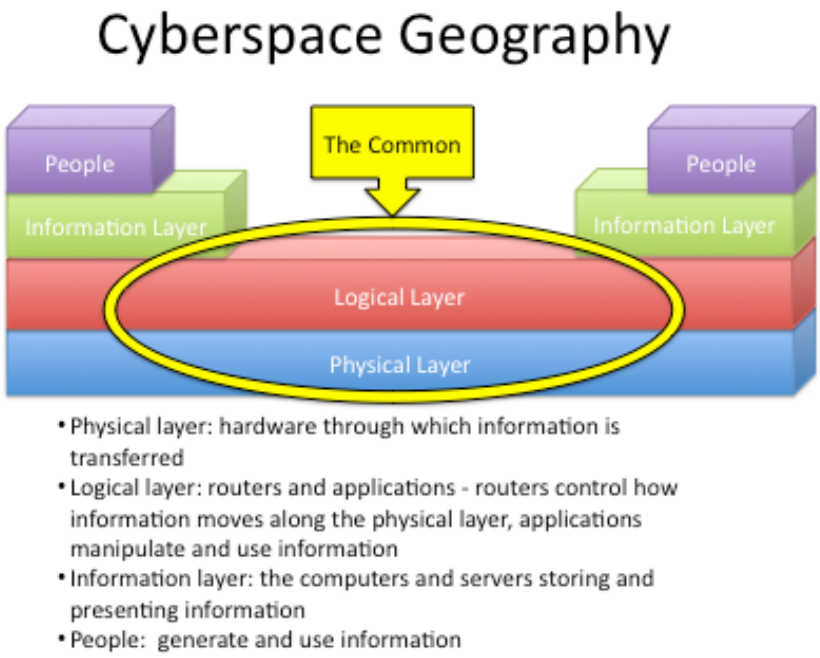


Figure 5: Cyberspace Geography[5]

Key to this insight is that the geographic features between any two points within the domain are not permanent. Changing routing commands, or physically disconnecting a system, changes the internal geography of the domain and can even isolate parts of the cyber commons from each other. Additionally, although in the West we think of cyberspace being global and constantly available, in truth, much of the world less integrated into the global network. The domain is not pervasive; in some places, the connection between a local network and the global grid is intermittent. In others, networking computers and keeping them physically disconnected from the global

[5] This model is the author's creation, limiting the common to the physical infrastructure shared by all users as the medium through which cyber traffic flows. Defining the common as the shared portions of the physical and logical layers of the domain enables discussion of how to control traffic within the domain. Owners and operators of individual computers and data storage systems share them when and if they choose. These edge components of the domain are not common to all users; instead, they are points of access much like harbors or airfields, subject to transit at the whim of the operator/operator.

information grid creates completely autonomous cyber domains.[6] Keeping the geography of the domain in mind, and the existence of the global commons as the space between edge users, we now move on to comparing the cyber domain with the maritime and aerial domains.

Comparing Cyberspace with the Maritime and Aerial Domains

Each of the following sections contains two subsections: one describes similarities between the maritime and cyber domains and the other describing differences. Understanding how the cyber domain and the extant domains to which we are looking for theory development guidance are alike and unalike will aid our application of the eighteen elements of domain power below.

> "Much like the Internet is becoming today, in centuries past the sea was a primary domain of commerce and communication upon which no one single actor could claim complete control. What is notable is that the actors that related to maritime security and war at sea back then parallel many of the situations on our networks today. They scaled from individual pirates to state fleets with a global presence like the British Navy. In between were state-sanctioned pirates, or privateers. Much like today's "patriotic hackers" (or NSA contractors), these forces were used both to augment traditional military forces and to add challenges of attribution to those trying to defend far-flung maritime assets. In the Golden Age of privateering, an attacker could quickly shift identity and locale, often taking advantage of third-party harbors with loose local laws. The actions that attacker might take ranged from trade blockades (akin to a denial of service) to theft and hijacking to actual assaults on military assets or underlying economic infrastructure to great effect."[7]

The maritime domain

Similarities:

[6] In many cases, this sort of "air-gapped" system is used to process classified or proprietary information.

[7] P.W. Singer and Noah Shachtman, "The Wrong War," (2011), http://www.nextgov.com/nextgov/ng_20110815_3244.php.

1. First and most important both domains require technology to enter, transit, and/or exploit. Furthermore, this technology is complex, requiring the widespread organization and coordination of human capital, industry, and government agencies over the long term. Standards and norms of operation ensure a smooth flow of traffic within both domains. Creation of these standards occurs through both government action and informal agreement between users of the domain.
2. Like the maritime domain, the cyber domain is critical to all four elements of the DIME. Both facilitate diplomacy and can be used to signal diplomatic intent.[8] Both are methods of transferring immense quantities of information. Each is also a military domain, used to conduct military operations or to aid allies. Both are widely used to distribute goods and services globally.
3. Like the maritime domain, the cyber domain is available to any user with the technology available to enter into the domain. Both consist of vast amounts of borderless territory, some of which is controlled, some of which is uncontrolled. Users are free to roam the domain at their will as long as they do not impinge on another user's sovereignty.
4. Cyber lines of communication transit sovereign territory in much the same way as maritime lines of communication. In both cases, the flow of goods along these lines of communication remains unimpeded during the course of normal transit operations (to use a maritime analogy, like moving through the Panama Canal). If, on the other hand, information is terminating in a particular sovereign territory (maritime analogy: unloading at the port), the movement of goods may be subject to national jurisdiction

[8] Movement of diplomats and information by maritime power in the pre-telephone and pre-electronic ages defined international relations. The technology enabled expanded use of the maritime domain in the late 1800s and in the early 1900s made it the Internet of its time.

and rules. An example of this sort of local restriction is filtering done by the Great Firewall of China. This firewall prevents select information from displaying in that country but allows routing of the same information through the country on to extraterritorial destinations.

5. In both domains, the movement of goods and information are what make the domain useful. The existence of the domain itself is unimportant–the ability to use the domain is. As with movement upon the maritime domain, while transiting cyberspace, goods are vulnerable to interception. They are moving through unsecured territory and unmonitored by the sender while en-route. A failure of information packets to arrive at a destination will be the first indication that they have been lost along the way.[9]
6. Both the maritime and cyber domains contain chokepoints that funnel movement down to predictable geophysical locations. Within the maritime domain, geographic boundaries to the seas provide this funneling effect. Within the cyber domain, this funneling is the result of physical infrastructure limitations. International communications flows almost exclusively through undersea fiber-optic cables.[10] These cables have the advantage of being less expensive than satellite

[9] Information does not flow as a continuous stream through the cyber common. Before transmission, the sending computer separates data into small packets; sending each packet to a destination address where they are re-assembled upon arrival. Not all packets need to take the same route between any two points as long as they arrive at the same location. Variations in the path each packet follows are determined in real time by routers at the logical layer of the Internet. These routers use up-to-the-millisecond information to determine the best routing available for each packet they handle. While there is a preferred flow of information, re-routing can and does take place. The protocol most often used on the Internet is the Transmission Control Protocol (TCP) and relies on confirmation of receipt back to the sender of the original packet.

[10] Ninety-five percent of international Internet and telecommunications traffic flows via undersea cables. See U.S. National Security Telecommunications Advisory Committee, "Cybersecurity Collaboration Report," (Washington, DC: Executive Office of the President, 2009), 20.

communications, fast, and reliable; there is no viable alternative.[11] There are however, a limited number of cables spanning international and transcontinental distances. The cables that do span these distances force the intersection of cyber lines of communication down into well-defined undersea crossings that become chokepoints in the domain. As an example, the majority of all financial transactions between London and New York arrive "in an 18-inch pipe underneath an unprotected manhole next to 60 Hudson Street in downtown Manhattan."[12] Obviously, such physical chokepoints provide opportunities to exercise control over cyber lines of communication.

Differences:

1. First, the cyber domain is man-made. It requires technology and constant attention to remain in existence. Without constant maintenance to the domain's physical infrastructure and updating of its routing protocols, the domain would cease to operate. Creation of the domain, its expansion, and its improvement are not natural phenomena; they occur only as long as users see mutual benefit in maintaining the domain's existence.
2. Unlike the sea, the cyber domain does not have well-defined edges. The maritime domain generally ends at the shore or banks of a waterway. It has a known size and shape that provides consistent, predictable chokepoints along maritime lines of communication. Access and entry ports for the maritime domain are well known or

[11] Michael Sechrist, *Cyberspace in Deep Water: Protecting the Arteries of the Internet by Creating an International Public-Private Partnership* (Cambridge, MA: John F. Kennedy School of Government, 2010), 16. Sechrist also says "Most countries prefer undersea cables to satellites for many reasons. Satellite communication is comparatively too expensive, slow, and unreliable. For example, satellites add at least 400 milliseconds to any transmission."
[12] Ibid., 20.

expensive and time-consuming to build. Consequently, documentation for each major point of entry exists. This allows other nations to monitor and plan to counter a potential adversary's access to the domain. The same is not true for the cyber domain. The cyber domain is constantly growing and has no size limit. The addition of transmission lines, creation of new Internet service providers, laying of new undersea cables, and launching of satellites all create a larger domain with a new geography. At the periphery, every web-enabled cell phone, each networked photocopier, and every Internet connected appliance add access points to the domain making it impossible to identify and monitor the use of the domain on a large scale.

3. Distance in the maritime domain plays a significant role in determining how any two points interact. In cyberspace, distance is almost meaningless because movement occurs at the speed of light; everything is adjacent to everything else.
4. Outside of territorial waters, the maritime domain is unowned. Within cyberspace, almost all of the physical and virtual components of the domain are privately owned or in the hands of major corporations. Each of these actors is free to do what he or she wishes with his or her own systems. Owners and operators are free to set their own rules of use and to police or regulate actions as they see fit. When disputes over proper use of the cyber domain arise, there are no cyber treaties along the lines of the UNCLOS to provide guidance for their resolution.
5. Perhaps the most important difference between the domains is the cost of entry. Entry into the cyber domain is cheap, and the costs of organizing people, equipment, and organizations to create and sustain cyber domain power are low when compared to

the maritime domain.[13] What this means is that nations with relatively limited resources can still pursue cyber domain power, vastly increasing the pool of potential competitors for domain control.

6. Finally, because we are looking at domain power theory, it is important to point out that the seminal maritime theorists were writing and thinking about a domain with a long history from which to draw examples. The policy makers whom maritime theorists sought to influence were very familiar with the domain, if not the technology involved, and also comfortable with the bureaucracy set up to organize its use. Because of this, maritime theories focus on the creation and use of domain-centric power. They do not focus on educating about the domain, its dominant technologies, or its potential to alter existing national security relationships.

The aerial domain

As with the maritime domain, the aerial and cyber domains share similarities and differences. Many of these similarities and differences are the same as those noted above between the maritime and cyber domains. As with the review above, we begin with domain similarities before moving on to identify noteworthy dissimilarities.

Similarities:

1. The air and cyber domains both require the use of technology to enter and sustain a presence within the domain. As with the cyber-maritime comparison above, the creation of domain power requires organization and coordination of personnel, corporations, and the government for exploitation on a large scale. Unlike with the

[13] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 97.

maritime domain, however, in both the air and cyber domains, a failure of the domain's animating technology terminates the ability to exist within the domain.

2. Both domains gained prominence due to rapid advances in technology that opened them to exploitation over a short period.[14] As a result, theorists in the cyber domain will face many of the same challenges faced by air theorists in the mid-1900s. Cyber theorists will need to combine theory of domain power with descriptions and education about the domain. Moreover, they will be required to sell the importance of their policy recommendations to an audience with a very low level of understanding of the domain. Airpower writers sought to make their point by emphasizing aviation's ability to target the enemy's vital centers directly, affecting its will and ability to fight from the opening moments of a conflict. Cyberpower's similar ability to bypass traditional borders and front lines promises a like capability for use in capturing a policy maker's attention.
3. Both domains are critical to the DIME and accessible to anyone with the technology to do so. Also similar to the comparison with the maritime domain are the risks of transitioning through the air domain. The transit of uncontrolled spaces exposes personnel and goods to the potential for interception and manipulation, often without discovery until after the event has occurred.
4. Routing within the air and cyber domains follows more strictly defined rules of the road than those of the maritime domain. Government administered air traffic control systems direct traffic over sovereign territory to make most efficient use of existing airways. Within the cyber domain, routing similarly stresses efficiency using

[14] *Opened* is the key word here. Development of new technology expanded man's ability to use the maritime domain beyond the limitations of sail. Air and cyber technology actually opened new domains for man's use.

organized traffic control over en-route packets of information. This means that once a cyber or air unit enters the domain, its movements follow directions provided by an outside source.[15] From the perspective of domain power development, this means that any actor with the capability to influence routing protocols has the ability to define the flow of traffic within the system.

5. The air and cyber domains also share the characteristic of manmade chokepoints. The absence of aerial geography means that chokepoints occur most often at the entry/exit points for the domain, not along the common internal lines of communication.
6. The air domain is expansive and uncontained, much like that of the cyber domain; it does not have well-defined borders of a set size and shape.[16] Both air and cyber penetrate the borders of surface domains allowing movement between two geographically separated points without requiring control over the surface domains in between.
7. The speed of movement in the aerial domain reduces the importance of distance in determining how nations interact. Obviously, forces operating in the aerial domain do not proceed at the speed of light. This similarity is important to keep in mind however, as we search for a basis upon which to begin building cyberpower theory.
8. Finally, both the aerial and cyber domains share the capability to project power into the surface domains. This gives them both the capability to affect movement with the

[15] Without physical geography to constrain them, aircraft are free to deviate from these instructions. During peacetime operations, legal ramifications for noncompliance serve to ensure the orderly flow of air traffic.

[16] There is no widely agreed upon upward limit to airspace. Neither does space have an agreed upon beginning altitude. Use of the 100-kilometer (52-mile) above sea level mark for record keeping purposes is common, but this is not a legally defined border. It is however, the lowest altitude that an object can orbit and is there for a candidate for any eventual formal definition as the upper limit of airspace. For a brief description of this debate see Dolman, *Astropolitik: Classical Geopolitics in the Space Age*, 115-16.

other domains, an important similarity to keep in mind as we determine what parts of airpower theory inform the cyber development process.

Differences:

1. Movement within the air domain is subject to more significant monitoring and control than either the cyber or maritime domains. Unlike movement along established lines of communication in the maritime or cyber domains, legal prohibitions prevent entry and transit through sovereign airspace without prior coordination.
2. The technology required to enter into the cyber domain is much less expensive to acquire and maintain than the technology necessary to enter the aerial domain.
3. Unlike the cyber domain, the aerial domain is static. It is not growing in size, nor is its geography changing with the addition of each new user. Entry and exit points for the domain are relatively well documented and predictable to allies and adversaries alike.
4. When required, aircraft can deviate from the routing instructions used to organize the smooth flow of traffic through the domain. Cyber traffic, constrained by physical and virtual geography, is unable to find alternative routing on its own.

Keeping these similarities and differences in mind, we now move on to discuss how the eighteen Elements of Domain Power developed in Chapter 6 relate to the cyber domain.

Elements of Domain Power in the Cyber Domain

The following section addresses each of the common elements of domain power in the order they appear within Appendix IV. These discussions provide insight into domain factors and strategic concepts that future cyber theorists must consider in their

work. Collectively, these discussions also establish that the eighteen elements of domain power, derived from extant military domain theories, are useful for framing and beginning the development of cyber domain theory, answering the research questions posed in Chapter 1.

1. *The use of domain power to exercise domain control ensures freedom of action within the domain while denying the adversary freedom of action. Cross-domain power can exercise cross-domain control.*

We learned from our maritime and air theorists that a nation can exercise control over a domain by preventing its adversary from using the domain to advance its national security interests while simultaneously advancing the nation's own. In order to exercise control over a domain, our theorists suggested a nation must control access to and/or movement through the domain.

They suggested two approaches:

1. Control the flow of traffic within the domain by controlling chokepoints along major lines of communication.[17]
2. Prevent an enemy from entering the domain, either through destruction of its domain-centric forces or by controlling the domain's entry and exit points.[18]

Regardless of the method applied, the intent of each theorist is the same, to control vital points within the domain. Control of vital points allows a nation's forces freedom of action while denying an adversary the same privilege.

---

[17] Primarily a maritime approach where control over lines of communication interest within the global common. The lack of geographically defined chokepoints and endurance in the aerial domain makes this difficult to consistently employ.

[18] Our air theorists stressed the destruction of enemy forces. Destruction of an enemy's fleet was a goal for our maritime theorists but, for all practical purposes, they approached denial of the domain through the blockade of ports. This option is not available to air forces due to limited domain endurance.

The use of power across domain boundaries to control movement within another domain is a unique aspect of this study's reviewed airpower theories. Projecting power across domain boundaries enables control over vital points in adjacent domains. Exercising control over vital points allows restriction of traffic flowing along a line of communication without requiring the use of domain-centric forces. An example of this cross-domain capability is the use of airpower for interdiction missions and for attacking an adversary's critical transportation infrastructure, such as a bridge or tunnel.[20] It is important to note that the exercise of cross-domain power does not necessarily require control over the domain from which power is projected. With this in mind, does domain power in cyberspace consist of controlling lines of communications? Can cyberpower exercise cross-domain control over vital points in adjacent domains?

> "Line of Communication - A route, either land, water, and/or air, that connects an operating military force with a base of operations and along which supplies and military forces move."[19]

Cyberspace has become an indispensible part of modern international interaction. Every lever of the DIME depends on the flow of information through cyberspace in some manner. Even a temporary loss of access would deal a significant blow to a cyber dependent nation's ability to pursue national security objectives.

Above we introduced a model of the cyber domain consisting of four integrated levels. From a domain control standpoint, this means that a nation's access to and use of lines of communication depend on all four levels operating simultaneously. These four

[19] U.S. Department of Defense, "Department of Defense Dictionary of Military Associated Terms Joint Publication 1-02," 200. Lines of communication, as we know from our discussions of the previous theorists, are not simply military in nature. The same definition applies to commercial routes of movement.

[20] Interdiction: An action to divert, disrupt, delay, or destroy the enemy's military surface capability before it can be used effectively against friendly forces or to otherwise achieve objectives. See ibid., 170.

layers each provide adversaries an avenue of approach to gain control over lines of communication within the domain.

First, an adversary may physically disconnect lines of communication. Whether accomplished by use of force or simply by shutting down critical components, this approach effectively denies an adversary the ability to use the domain.[21] Because the domain ceases to exist, this is less an exercise of control than a denial of access. The downside of this approach is that it results in the loss of domain access for all parties, adversaries, allies, and neutrals alike.

A second means to gain and exercise domain control is to target the logical layer of the cyber common, where routers determine where packets of information move and what lines of communication they follow. Control over routers at vital points along lines of communication enables diversion of Internet traffic, preventing it from reaching its intended destination. This is not an all-or-nothing action like the destruction of physical infrastructure above. This method permits a nation to exercise control over the domain, allowing some traffic to pass while denying others. This approach is less permanent than physical control but preserves the use of the domain for pursuit of one's own objective.

Attacking the information layer of cyberspace is a third means of gaining and exercising control over cyberspace. Altering stored data or processing programs prevents the exchange of useful information and reduces an adversary's ability to use the domain to its advantage. This approach has less utility in restricting an adversary's overall use of the domain. Instead, it focuses on disrupting individual systems such as targeting or command and control. The use of cyberpower to exercise domain control in this manner

[21] This approach is a candidate for cross-domain attack such as breaking a fiber-optic cable with air strikes.

has the advantage of being very precise. Given enough intelligence and time, this method targets specific adversary systems and operations.[22] Improperly or indiscriminately used as a means of exercising cyber control, alterations in databases or control programming can have unintended consequences.

Targeting the fourth layer, people, focuses on disrupting their ability to both create and access information, and targets their ability to correctly interpret the information they receive. Taking many forms, this approach may run the spectrum from eliminating key personnel responsible for maintaining systems, all the way down to stealing passwords and injecting false commands into a network to create distrust among users. This approach is an inexact means of gaining and exercising control over the domain. It is more useful for disrupting an enemy's use of the domain, or their control over a portion of the domain, than it is as a form of control in itself.

Based upon the discussion above, I conclude that during periods of extended conflict, the most enduring means of gaining and exercising domain control is to target the physical and logical layers of the Internet.[23] At the physical layer of the domain, its vital points are geo-located infrastructures that act as chokepoints through which significant portions of cyber traffic flow. Beachheads for transoceanic cables are one such point, and for the most part, they are unsecured against attack. A nation that physically controls these locations has the potential either to destroy them or alter their

[22] The STUXNET virus is an example of a targeted use of cyberpower. In this case, its use was not to exercise domain control as much as to produce cross-domain effects. STUXNET is mentioned here because it provides a well known example of how effectively cyber operations can target an adversary's systems given enough time and money for mission planning. For a good discussion of the virus and its creation see Michael Joseph Gross, "A Declaration of Cyber-War," *Vanity Fair* (2011), http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

[23] Targeting of the information and/or people layers of the domain is less likely to create lasting control over the domain. Targeting at these layers is more appropriate for achieving specific outcomes within the domain.

programming to control the routing of information. The destruction or redirection of information at a few Tier I Internet service providers (ISP) within a nation provides effective control over a nation's use of the domain.[24]

Obviously, the cyber domain is subject to domain control through the targeting of lines of communication. Targeting can occur using cyber domain power to alter routing commands. It can also take the form of cross-domain threats such as the physical destruction of infrastructure. For a nation seeking to develop domain power, defending lines of communication is a critical task. Well-defended lines of communication are more reliable and increase a nation's domain power.[25]

Does this element of domain power travel to the cyber domain? Yes.

What does this means for cyber theory development? Based on the discussion here I conclude the most efficient means of exercising domain control to ensure freedom of action and deny the enemy the same, is through physical and virtual chokepoints along

[24] Richard Clark points out that there are different levels of ISP that own and operate the connecting infrastructure of cyberspace. Divided into three groupings, Tier I providers own and operate the high capacity lines that carry the majority of long distance communications. Tier II and III providers are progressively smaller and more localized. For example, within the US there are six Tier I providers: Verizon, ATT, Quest, Sprint, Level 3, and Global Crossing. These six companies carry almost all cyber transmissions at some point during their movement within the US. Smaller Tier II and Tier III companies provide local access to the domain, feeding into the larger Tier I systems that connect the world. This translates to vital points on the Tier I systems being more lucrative targets than those of the smaller operators. If an adversary takes out or controls a Tier I intersection, it has significantly altered the geography of the domain. Clark discusses Internet vulnerabilities in Chapter 3 of his book: Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat To National Security And What To Do About It*, 1st ed. (New York, NY: ECCO, 2010), 69-101.

[25] As Peter Schwartz points out, a well-defended Internet encourages increasingly responsible use of the domain; in turn, this increases the domain's value. A failure to defend the domain risks its degeneration into a Wild West scenario with few rules and little visibility into what is occurring across the domain. Such deterioration would increase the time and effort required to secure the domain when needed, decreasing its value as an enabler of the DIME. See Peter Schwartz, "The Role of Architecture in Internet Defense," in *America's Cyber Future: Security and Posperity in the Information Age*, ed. Kristin M. Lord and Travis Sharp (Washington, DC: Center for New American Security, 2011), 233.

lines of communication within the domain common. Cyber theorists must identify and describe what constitute lines of communication in the domain. In addition to chokepoints within the common, they must also identify vital points and chokepoints across all four layers of the domain. Theorists must grapple with the type and duration of control appropriate within the cyber domain with each category of chokepoint. Discussion of each approach must relate cyberpower use to overall national goals spread across all domains. Theorists should highlight the costs and benefits of exercising control through physical destruction of cyber infrastructure as a means of controlling the enemy's access to the domain. Finally, theorists must point out that securing the domain requires protection of government and commercial systems necessary for exercising and maintaining overall national power.

2. *The objective of exercising domain power in a commons is to affect an enemy's will and means to resist.*

Aligned with Clausewitz's famous dictum, our maritime and air theorist tie the use of force to the pursuit of political objectives. Maritime efforts such as blockading commerce and aerial efforts such as attacks on critical infrastructure are exercises of domain control to reduce an adversary's will and means to resist. Shying away from direct attack on populations, our theorists focus on reducing a nation's ability to resist, which decreases its will to resist.[26]

The penetration of cyberspace into almost every aspect of global commerce, diplomacy, and military operations means that it has become a critical aspect of a nation's means to resist aggression. It also means that cyber domain power is a candidate for use in targeting an enemy's will and means to resist.

[26] Douhet is an exception as previously discussed in Chapter 6.

Attacking an adversary's cyber-enabled critical infrastructure, such as electrical grids, communications systems, and water supplies, directly affects a nation's means to resist, and theoretically, will erode its will to continue fighting. Beyond major industrial systems however, cyberspace can be used to target programming that runs weapons systems, causing them to fail at critical moments with few collateral effects on surrounding systems or a civilian population.[27]

The more cyber penetrated a nation is, the more vulnerable it will be to cyber attack. The irreversibility of most nations' movements toward cyber controlled infrastructure and cyber enabled information flows means the use of cyberpower to target a nation's means and will to resist are likely to increase in the future. Much as Douhet predicted populations would be unable to withstand aerial bombing, some cyber prognosticators warn that America will be unable and unwilling to endure cyber disruption. While the war winning effect of cyber operations may be debatable, it is certain that cyber operations are able to affect both a nation's means to resist and its will to pay the price of continued resistance.

Does this element of domain power travel to the cyber domain? Yes.

What does this mean for cyber theory development? Cyber theory must explain the use of cyberpower to affect an enemy's means and will to resist. Theorists must describe how cyber actions tie in with operations across the DIME, highlighting appropriate types of targets–industry, government, military, etc. Cyber theory must couch this discussion within the context of international law and the customs of warfare.

---

[27] An example of this is Israeli's suspected use of electronic and cyber attacks against anti-aircraft systems during a 2007 raid upon a suspected Syrian nuclear installation. Many observers suspect that hidden back doors fabricated into the anti-aircraft system's microprocessors was responsible for their failure to see incoming aircraft. See Sally Adee, "The Hunt for the Kill Switch," *ieee Spectrum* (2008), http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0.

3. *Governments must emphasize strategic development of domain power through incentives, coordination of military/civilian development and treaties as part of its long-term national strategy.*

Maritime and air theorists identify government involvement as a critical requirement for creation of enduring domain power. Ranging across the full spectrum of government affairs, these recommendations included the negotiation of treaties to encourage trade, incentives for development of industry, an emphasis on education, and organization of bureaucratic structures within government. These actions, theorists suggest, are important to developing a nation's prerequisite knowledge, skills, and infrastructure for supporting domain operations. Over the long run, institutions spring up around industries and regulation takes hold and creates a friendly business environment encouraging organization of domain industries. Eventually, these efforts change a nation's character, ingraining use of the domain into its culture and leading to domain mindedness in the population.

This same approach applies to development of cyberpower. As with other domains, the government creates regulatory conditions within which industry flourishes. It also provides strategic guidance and recommends budgets for the development of civil and military power. The difference between cyberpower development and that of previous domains is that, in most cases, the government finds itself following and regulating commercial development instead of incentivizing it.

Instead of encouraging infrastructure and research, the government's role is to incentivize and regulate cyber security and redundancy. Government regulation and policy must focus on controlling development in a manner that favors national security and retains sovereignty over critical pieces of infrastructure. The domain is developing on its own through commercial incentives and competition; how a nation turns this

commercial development into enduring power is the function of government policy. The government's role in creating cyberpower is as important as it is to creating power in the other domains. To successfully develop enduring cyberpower, a nation must harness the domain's commercial development, encouraging service to national security interests through regulation and incentives.

Does this element of domain power travel to the cyber domain? Yes

What does this mean for cyber theory development? Cyber theory will have to describe and explain the role of government in creating domain security and domain power. It must identify the requirement for a long-term national strategy focused on developing key aspects of the domain's network infrastructure and cyber oriented domestic industry. A key aspect of this effort must be discussion of the domain's commercial led nature and identification of how government policy balances security and development concerns across the cyber-reliant DIME.

4. *Domain power development is a subset of overall national power across the DIME.*

Our extant theorists' works call for development of domain-centric power as a subset of overall national power. Corbett, for example, stresses maritime power's ability to strengthen other elements of national power. The airpower theorists point out that increased mobility and speed have a transformative effect on diplomacy and economics, not just their domain's marshal prowess. Airpower theorists also take great pains to discuss the importance of integrating civil, economic, and military development into overall development of national power. In each case, our theorists argue that development

of their domain is both a vital and efficient use of national resources but not the only power a nation requires.[28]

There is no reason to believe that development of the cyber domain is an exception to this general rule. The domain's strategic utility is "its ability to manipulate an adversary's perception of the strategic environment during both peacetime and war."[29] Using misperception and deception, cyberspace enables other instruments of national power to directly achieve policy objectives. To fully integrate cyberpower into national power, its development must be part of an overall national security strategy.[30]

Cyberpower's enhancement of the DIME makes it a critical enabler for all forms of national power. The rapidly increasing reliance of each element of the DIME on cyberspace means that some method for overseeing and integrating widely varied cyberpower requirements is necessary. Efficient use of national resources, therefore, demands that cyberpower development occur in the same integrated manner as the domains that have come before.

Does this element of domain power travel to the cyber domain? Yes

What does this mean for cyber theory development? Cyber theory will tie the development of cyberpower to the development of overall national power. A cyber theory should describe the use of cyberpower to enhance the other elements of national power

---

[28] For instance, despite claims by airpower theorists that direct attacks on critical infrastructure can cause an enemy to capitulate, they recognized the need to retain land forces to hold against invaders while air efforts take effect.

[29] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 103-04.

[30] Strategic use of the domain may include the use of cyberpower to aid a nation's economic development or provide an edge during treaty negotiations. Examples of such peacetime usage of cyberpower for espionage and data theft are the so-called Aurora and Night Dragon attacks. These apparently Chinese sponsored attacks went after major oil and gas companies in the US and worldwide to steal "research and development, software source code, and manufacturing know-how." See Clark, "China's Cyberassault on America."

and predict the use of cyberpower in conjunction with other sources of national power during times of peace and war. It must do this while simultaneously tying in the development of cyberpower to efficient uses of national resources. As an enabling power for the entire DIME, the domain's development requires coordination across the whole of government.

5. *Simultaneous military and commercial domain development are necessary to become an enduring domain power.*

We learned from our earlier theorists that the development of enduring domain power requires a nation to possess both military and economic might. The maritime theorists emphasize the requirement to defend commercial forces transiting the maritime domain. The air theorists stress development of technology and the creation of domestic industry. Both sets of theorists stress the need to create domain mindedness.

A domain minded population generates the political will to pursue domain power as part of long-term national policy and creates a reserve of personnel from which to pull. Moreover, our theorists suggest that by creating both military and commercial power in a domain, a nation sets standards of operation and rules of conduct. It also establishes international expectations favorable to its particular domain-centric desires.

Seversky points out that as a nation's reliance on a domain increases, its vulnerability to attacks upon that domain increase. The United States Department of Defense recognizes this, stating in its Joint access document: "threats to cyberspace subsequently increase vulnerabilities for militaries that rely on cyberspace technologies"[31]

This element of domain power transfers well into the maritime domain if only for the fact that most critical infrastructure in the cyber domain is owned and operated by private individuals

[31] U.S. Department of Defense, "Joint Operational Access Concept," 50.

and corporations. The pace of commercial cyber development has outpaced military development. This reverses the historical US "military leadership" approach to domain power development. In many ways, the military is the one scrambling to develop its domain power and is reliant on commercial assistance to do so.

Government attention is necessary for creation of military domain power and to secure critical infrastructure. Any failure to simultaneously develop military power and cyber security requirements risks the creation of a commercial heavy imbalance in cyber domain power. A nation that is cyber dependant yet unable to protect cyber infrastructure or project power via the domain is vulnerable to attacks upon the domain.

Israeli security adviser Isaac Ben-Israel points out that a nation must develop cyber security alongside development of commercial domain use. He notes that the most vulnerable targets for cyber attacks are a nation's critical infrastructure, such as power generation, water supply, telecommunications, transportation, hospitals, banks, etc.[33] In the United States, like most countries, these critical pieces of a nation's infrastructure are in private hands. From a governmental standpoint, the challenge is to develop a strong private-public partnership to secure these systems. The difficulty for a nation like the US is that under a capitalist system it is difficult to convince owners of these systems to invest heavily in defending against an attack that may never come.

> "U.S. space and cyberspace capabilities depend significantly on commercial systems and adversaries in some cases will purchase space capabilities on the same platforms used by U.S. joint forces"[32]

[32] Ibid., 12.
[33] Grauman, "Cyber-Security: The Vexed Question of Global Rules," 9.

Regulation is one example of how a government can create systemic incentives for simultaneous commercial and military development of the cyber domain. Creating and enforcing regulations to secure critical infrastructure, for example, has the same effect on national security as do calls from our air theorist to provide incentives for developing airways and airfields. They will create a stronger, more durable national infrastructure from which to exercise domain power during times of conflict. Commercial lead development of the domain and cyber's integration into vital infrastructure requires simultaneous military, civil, and commercial development coordinated and guided through government oversight.

Does this element of domain power travel to the cyber domain? Yes.

What does this mean for cyber theory development? Future cyber theory must identify the importance of commercial, civil, and military domain power in creating cyberpower. It should recognize the unique commercial lead in developing the domain and account for this by defining the federal government's role in ensuring that military and security development keep abreast of the latest changes in technology.

6. *Creation of domain power must occur before a crisis or conflict begins.*

Creation of ships and aircraft takes time, effort, and investment of significant national resources. Training of personnel to operate and man these systems is equally time consuming and costly. Quite simply, the complexity of modern maritime and aerial forces means that their development and use takes years, if not decades, from beginning to end. During conflict, a nation without maritime or airpower, or a nation whose maritime or airpower are destroyed, has little chance of generating them quickly under wartime conditions. Knowing this, our reviewed theorists point out that a nation prepared to take command of a domain at the beginning of a conflict is in a position to retain

command and use it to advance its own interests. Is the generation of cyberpower similarly complex and difficult to accomplish during times of conflict?

Above, element 3 discusses the importance of government guidance in setting strategic direction for development of the cyber infrastructure and human capital necessary for creating enduring cyberpower. We also learned in our discussion of element 5 that commercial and military development goes hand in hand toward creating domain power. Coordinating and guiding these actions are a function of government oversight and take time and effort to produce results.

Once produced however, cyber forces are more easily regenerated than the ships and planes our extant theorists seek to protect. Quick repair of disrupted databases or repair of corrupted routing systems can restore a nation's lost cyberpower.[34] However, insights into an adversary's network and the cyber operations necessary for planning and executing cyber attacks or mounting a cyber defense are not easily and quickly obtained.

The skills for operating offensively and defensively in the cyber domain are as specialized and difficult to create, as those for the other domains. Mapping an enemy's cyber networks to gain an understanding of how they operate takes patient and continuous effort. For example, if you intend to use cyberpower to take down a nation's electrical infrastructure, you must have the necessary backdoors in place, and the enemy's terrain mapped out, before a conflict begins. The creation and placement of specialized logic bombs, ready to go off when commanded, requires advance preparation and continuous reevaluation. Once an adversary identifies vulnerabilities in its systems

[34] The theories of maritime and air power reviewed here assume the sinking of ships or destruction of aircraft permanently reduce an adversary's domain power. The only way to permanently destroy an enemy's cyberpower is to destroy the domain, something that affects the cyberpower of the aggressor nation also. Interfering with an adversary's use of cyberpower is a more likely use of cyber force.

and programs, it will undertake efforts to remove them, making continuous analysis and mapping of enemy systems a requirement.

Careful preplanning for using cyberpower is as critical as it is in any other domain. Failures to carefully consider the effects of a cyber attack raise the risk of injuring one and one's allies along the way. Cyber domain forces must constantly retain a high level of readiness because offensive and defensive operations in cyberspace are likely to commence long before combat in the other domains begins.[35] Cyber attacks must be preplanned, ready to execute when called upon. Once combat begins, any changes an adversary makes to their cyber networks may invalidate preplanned attacks and make new attacks impossible.

Does this element of domain power travel to the cyber domain? Yes.

What does this mean for cyber theory development? Cyber theory needs to predict the use of cyberpower early in any conflict and describe the domain's unique requirements for offensive and defensive preparation. Taking advantage of speed and flexibility, cyber operations may be the opening salvos of any conflict. Cyber theory must capture this and explain the requirements for extensive peacetime planning to continuously create and maintain cyberpower.

7. *Control over chokepoints where lines of communication converge or terminates is the most efficient means of exercising domain control and leads to enduring domain control.*

Each extant domain theorist devotes a portion of his theory to discussing the importance of controlling movement within the domain. At the macro level this study discussed control over lines of communication in the first element of domain power above. That discussion identified that chokepoints occur where lines of communication

[35] U.S. Department of Defense, "Joint Operational Access Concept," 19.

converge or terminate. Controlling those chokepoints in the extant domains is the most efficient means of exercising domain control. Building on that discussion, this section will discuss the role of chokepoints as an efficient means of controlling the flow of traffic within the cyber domain.

The reliance of the cyber domain on the continuous interconnection of lines of communication makes the use of chokepoints an ideal means to control traffic. Both physical and logical in nature, cyberspace chokepoints narrow down the expansive domain, and all the information flowing through it, into clearly identifiable physical locations. While in most cases alternative routings between any two points exist, the majority of international cyber traffic flows on a finite number of physical cables.[36] An example of a cyber chokepoint is the previously discussed 18-inch pipe under New York City that carries 90% of Wall Street's financial traffic to London. Exercising control over this cable would provide an adversary influence over America's economic element of power and perhaps have long-lasting consequences for the global economy.

Like chokepoints in the maritime domain, cyber chokepoints greatly reduce the number of locations a cyberpower must control in order to exercise effective domain control. Attacks on the information and people at other levels of the domain model may be effective as a means of exercising control over narrow portions of the domain, but they

[36] There are currently twenty-nine active transoceanic cable beachheads on US shores. Most cable systems fall into three categories: linear (single path), ring (dual-path redundancy) and mesh (multiple interconnections). Linear systems are vulnerable to interruption due to a lack of redundancy. Many ring systems can assume the majority of disrupted traffic if one side of the loop is broken. Mesh systems, with multiple interconnections, are the most redundant but are cost-prohibitive for use over transoceanic distances. A full description of cable routing is beyond this work. A short description of routing structures and a map of the 29 transoceanic cable beachheads in the US can be found here: Sechrist, *Cyberspace in Deep Water: Protecting the Arteries of the Internet by Creating an International Public-Private Partnership*, 100-03.

are less efficient than controlling a few vital points within the cyber common.[37] Understanding this, I conclude that controlling chokepoints where cyber lines of communication converge is the most efficient means of exercising cyber domain control.

Does this element of domain power travel to the cyber domain? Yes.

What does this mean for cyber theory development? Conservation of effort in any domain is a component of strategic planning. Cyber theory needs to identify the use of chokepoints as the most efficient means of exercising control within the cyber domain. It should discuss various types of control possible and the use of control over these chokepoints to enable and enhance the use of power within other domains.

8. *The exercise of domain power is a multi-step process: first gaining command of the domain and then exercising command of the domain (to included projection of power across domain boundaries).*

Beginning with Mahan, our theorists stress the need to control the domain, securing it for one's own use, as a necessary first step. After securing control over the domain, effort shifts to exercising control over the domain. The requirement to mass naval and air forces in order to seize control over strategic points or eliminate the adversary's ability to use the domain drives this two-step process. It also drives discussions about the ideal force structure a nation should maintain. We saw this in our discussion of Mahan and Corbett above. Corbett writes in some part to counter what he sees as Mahan's overemphasis on building ships of the line to gain control over the domain, without sufficient attention to exercising control.

[37] Sechrist provides an example of a cyber chokepoint in his discussion of worldwide cable routing diversity. According to Sechrist, 31° 11.738′ N, 29° 54.108′E are the coordinates that identify the intersection of El Horreya and El Nabi Streets in Alexandria, Egypt. Calling this the center of the fiber world, he notes that within that building five cables converge. This building is the single location for cross-connection of all Internet cables between Africa, Europe and Asia. According to his study, 80% of all Europe to Middle East traffic passes through this point. Ibid., 43.

With reference to the cyber domain, the nearly instantaneous timeline for operations makes the differentiation between the two phases of conflict difficult. This discussion has previously established that gaining control over chokepoints in the cyber domain allows the controlling nation to deny an adversary use of the domain. With this in mind, we can say that it is necessary to first gain control over these vital points before using them to exercise control over the movement of information along lines of communication. One caveat: Because many cyber attacks occur as first strike operations, the use of cyberpower to gain control of the cyber domain simultaneously exercises command of the domain to enable operations within other domains.

Does this element of domain power travel to the cyber domain? Yes.

What does this mean for cyber theory development? Cyber theory must explain the requirement to quickly gain control over the domain as a necessary first step before exercising control over it. Moving to control an enemy's use of the domain quickly will prevent him from executing preplanned uses of cyberpower against you. This discussion should focus on influencing force structure development and investment of resources. Theorists must also explain where control over the cyber domain fits into the timing and execution of national power in the other domains.

9. *Gaining domain control means eliminating the enemy's ability to enter the domain or use its lines of communication.*

We learned in our discussions of extant theory that denying an enemy access to a domain is the primary means of gaining and maintaining domain control. In the maritime and air domains, absolute control is theoretically possible. There are a limited number of access points to each domain and it is difficult to replace destroyed aircraft or sunken ships.

Complete elimination of an enemy's ability to enter the cyber domain, on the other hand, is not a realistic means of gaining control over the domain. First, the number of access points makes complete denial of access impossible. Elimination of an enemy's access from any particular location is a temporary action; they can be back up-and-running from a new point of access, using different networks within hours.[38] Additionally, by definition, cyberspace is the interconnection of systems, not the entire system itself. Outside of the global Internet we commonly consider cyberspace, there are many isolated domains running by themselves–some contested, some not. Eliminating an adversary's ability to access all possible cyber domains is a nearly impossible task.[39]

A more realistic approach to cyberspace control is to accept that an adversary will have access to the domain; one should focus on controlling the flow of traffic through the domain. Much like controlling a maritime chokepoint, one can deny transit to enemy cyber traffic while retaining access for oneself and neutrals. This will not prevent the enemy from processing and transmitting information; it will however, degrade its ability to use the domain giving one an advantage. In essence, this is cyberspace superiority, not cyberspace control.[40]

Superiority of this type will most likely be temporary, an adversary will retain the ability to enter the domain and eventually find a way to work around or overcome any restrictions put into place. This sort of temporary superiority is more like Corbett's

---

[38] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 97.
[39] If an adversary has a self-contained command and control system for example, physically disconnected from other cyberspace systems, then you would have to know about and directly target that system to actually control cyberspace (provided you can get access to it).
[40] Cyberspace superiority: "The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, sea and space forces at a given time and sphere of operations without prohibitive interference by an adversary." U.S. Department of Defense, "Joint Operational Access Concept," ii.

approach to domain control than the majority view expressed by Mahan or any of the air theorists. Exercising control in cyberspace will focus on achievement of specific and limited objectives, after which the domain will most likely revert to its naturally contested state. I conclude that total control over the domain is not a realistic or effective use of cyberpower.

Does this element of domain power travel to the cyber domain? No.

What does this mean for cyber theory development? Cyber theory must identify that an adversary will retain access to the domain and explain the exercise of control over the domain to minimize an adversary's ability to use it. Cyber theory must discuss various levels of control and superiority, across all four levels of the domain, describing when and how each contributes to a nation's exercise of domain power while denying the enemy opportunities to use the domain for its own purposes. Changes in technology as well as the continued growth of the domain will make this a difficult process. Theorists are likely to settle on gaining an advantage in the domain, not denying it, as the proper use of domain power. Total destruction, the only guaranteed way to deny an enemy access to the domain, is an unlikely course of action for exercising control over the domain because it also denies one's own access to it.

10. *A nation's geography affects its domain power potential, vulnerability to attack from the domain, influence over lines of communication, and incentive to develop domain power.*

Maritime and air theory deal with geography as it appears on a globe. In maritime theory, a nation's distance from and position along surface lines of communication are important considerations for its development of maritime power. A nation's incentive and potential to develop airpower is also a function of geography. The requirement to project

power over long ranges, need to transit vast distances for commerce, and the need to overcome natural obstacles all contribute to a nation's incentive to develop airpower.

In cyberspace, the link between geography and domain power is not as clear. Earlier in this chapter, we learned that the geography of cyberspace is determined more by hardware linkages and routing logic than geophysical positioning. Geophysical positioning does have a role to play. For instance, crossing the Atlantic or Pacific Ocean requires traffic to use one of a finite number of transoceanic fiber optic cables (there are twenty-nine beachheads in the US).[41] Each cable becomes a line of communication and a chokepoint. The United States is fortunate to have several cables on each coast providing redundant and therefore robust cyber communications. This is not true for all nations or all regions of the world.

In 2008, a ship dragged its anchor in the Mediterranean, cutting three cable systems that carried about 90% of all data between Europe and the Middle East.[42] The result of these cuts was a 50%-100% reduction in cyber traffic to nations in the Middle East. More importantly, the United States government's ability to project power into the region across the DIME decreased. The Defense Intelligence Agency lost 60% of its connectivity to the region and US Air Force unmanned aerial vehicle operations temporarily slowed to a halt due to reduced bandwidth. Occurring during a time of war, this reduction in cyber connectivity affected the US government's ability to exercise power across several domains. In 2009, the severing of another cable, the only one connecting West Africa to the rest of the world, caused significant disruptions to the region's banking, government, and phone systems. Obviously, the geography of

[41]For a map of these cables see Sechrist, *Cyberspace in Deep Water: Protecting the Arteries of the Internet by Creating an International Public-Private Partnership*, 100-03..
[22]For a description of this event and its affect see ibid., 9-11 and 120.

cyberspace differs from geography in previous domains. As these two examples demonstrate, disruption of cyberspace geography has far-reaching and often unpredictable consequences.

Because Internet geography is manmade, its creation and destruction are a continuous process. Nations have the ability to create their own geography and therefore their own domain power potential. Rather than focusing on geospatial relationships, it is more appropriate to consider the robustness and redundancy of a nation's cyber geography when determining cyberpower potential.

Interestingly, this geography not only includes internal and external connections within a nation's geographic borders, but also the linkage of entire regions to the rest of the world. In our example above, the destruction of one cable cut off all of West Africa from cyberspace. Even with significant domestic investment, once cut off from the rest of the world any West African nation's cyberpower immediately became useless outside of the region.

Before moving on, it is appropriate to note that physical geography does play a role in determining a nation's required investments for creation of cyberpower. For example, an island nation is obviously reliant on a finite number of cables connecting it to the overall global grid. These cables are points of vulnerability during times of conflict and place upward limits on data transmission during times of peace. From the discussion above, one concludes that a nation's cyber geography is a significant determinant of its domain power, and domain power potential.[43]

[43] A well-connected nation does not automatically have domain power; it has domain power potential. It may not choose to develop balanced commercial and military use of the domain, forgoing true domain power. Additionally, a nation with domain power may suddenly find changes in domain geography alter its ability to exercise that power.

Does this element of domain power travel to the cyber domain? Yes – but with different geographic connotations.

What does this mean for cyber theory development? Cyber theorists must recognize that domain power concepts, such as lines of communication and vital points, need to be discussed in terms of cyber geography. Describing the effect of nearly instantaneous communications with such common terms as size, distance, and location will help to differentiate cyber geography from traditional geography and will demonstrate unique characteristics of the domain. Cyber theory must also describe the process for creating cyber geography and the role geography plays in determining both a nation's cyberpower potential and its incentives to become cyber-faring. Policy makers must be able to use these explanations to create policy designed to build a nation's cyber geography appropriately.

11. *A nation's population affects domain power through the creation of domestic reserves of both personnel and knowledge available in times of need.*

During discussion of our extant theorists, Mahan and Mitchell especially, we learned that for a nation to create and maintain power in a domain, its population must be involved with the domain. Either directly or indirectly, a significant portion of the population employed in domain-centric pursuits creates a reserve of manpower to call upon in times of need. A domain-centric mindset also creates pressure on governments to take an interest in the domain and invest in developing it further. Further development, in turn, creates a larger reserve of manpower to operate, service, maintain, and build domain-centric forces.

The requirement for large manpower investments to create cyberpower is less clearly defined than in either the maritime or air domains. Writers concerned with cyber

security point out "Given a handful of extremely talented hackers, a relatively effective intelligence agency, and a pot of funds to hire cyber mercenaries and insiders, many nations could compensate for their smaller size by letting an army of computers go to war for them."[44] They are certainly correct, at least in the short-term military sense of domain power. The rapid proliferation of cyber technology and the relatively cheap infrastructure investments required to access the domain mean that even non-state actors can purchase and employ cyberpower by use of a relatively small group of cyber professionals. Similar contemporary examples of this approach are the use of cyber activists by Russia in its conflicts with Georgia and Estonia, and China's use of semi-government sponsored hacking groups to stealing information.[45] However, are these actions really creating national cyberpower?

Missing in this calculation are requirements to invest in and maintain cyberpower over the long term. We have already discussed the importance of cyber geography in creating and maintaining cyberpower. Creating and maintaining a cadre of personnel to service this infrastructure is akin to creating maritime and aviation industry workers. It requires a well-educated population with prerequisite science, technology, engineering, and mathematics backgrounds.[46] While a nation can purchase cyber infrastructure,

---

[44] Clark, "Software Power: Cyber Warfare is the Risky New Frontline."

[45] Robert A. Miller and Daniel T. Kuehl, "Cyberspace and the "First Battle" in 21st-century War," *Defense Horizons* 68 (2009), for a discussion of China's hacking groups see Lolita Baldor, "Government-backed Hacker Teams do Most China-based Data Theft," *USA Today* (2011), http://www.usatoday.com/tech/news/story/2011-12-12/chinese-hackers/51830840/1.

[46] Education is a vital component of national security; it provides a foundation for creating human capital with the skills necessary for creating domain power. In the cyber field, this is especially true; workers require an advanced understanding of the sciences. One estimate predicts that information technology workers will be among the top five federal hiring requirements, about 800,000 workers between 2011 and 2018. These new workers are required to design, implement, and maintain information systems. Without a large and well-educated population, supporting this requirement would be impossible. For a discussion of education's role in national security and recommendations for improving the American education system, see Myra Howze Shiplett et al.,

without the expertise to create and maintain that infrastructure domestically over the long term, that nation is conforming to another's standards of operation. It is also reliant on that nation's willingness to provide goods free of programming backdoors and other means of access that are beyond the scope of this discussion. The expense of operating a robust and redundant network of systems requires a commercial and civilian population base to justify the expense of the long-term effort. A small population would not need a large robust system, nor would commercial industry invest in such a system without government-provided incentives.

Additionally, cyberpower is a latent power, most often put in place well before a conflict begins and ready for use if called upon. This sort of long-term commitment requires extensive and continuous mapping of any potential adversary's' networks and infrastructure to identify vital points and vulnerabilities for exploitation. Developing and cultivating the expertise to gather and maintain the intelligence necessary for planning and executing cyber attacks requires the long-term commitment of loyal personnel. It also requires coordinated oversight and integration with other elements of national power; a nation is unlikely to entrust mercenary warriors with this task.

Ultimately, numbers prevail. As in the other domains, a large, well-educated, outward-looking population provides a deeper pool from which to draw cyber professionals. It provides the commercial and political impetus to develop redundant cyber systems and an industrial base through which to exercise domain power. In the end, a larger population is more likely to have a sufficiently high number of domain-minded

---

"A Well-educated Workforce: Vital Component of National and Economic Security," in *Economic Security: Neglected Dimenson of National Security?*, ed. Sheila R. Ronis (Washington, DC: National Defense University Press, 2011).

personnel willing and able to dedicate their efforts toward creating and maintaining domain power.

Does this element of domain power travel to the cyber domain? Yes

What does this mean for cyber theory development? At this point in the domain's development, a large, well-educated population is an advantage in developing domain power. When creating a theory, cyber theorists must address population size, technological familiarity, education, and cultural sensitivities in determining a nation's cyberpower development. They must also differentiate the creation of domain power from the use of the domain for espionage and cybercrime conducted by state or non-state actors. Cyber theory will need to define where these actions fit in with overall cyberpower and the pursuit of national security.

12. *Domain power development requires the creation of domain-specific governmental institutions and cross-domain coordinating bodies.*

This element of domain power was the subject of analysis in Chapter 6 due to its prominent nature in air domain theory and its absence in maritime theory. Air domain theorists point out that the opening of an entirely new domain requires creation of domain-centric organizations to properly manage the domain's development and use. Existing bureaucratic organizations, airpower theorists' claim, are unwilling to develop capabilities that compete with their own core missions. Our airpower theorists' calls for domain-centric organizations extend across military and commercial sectors in an attempt to coordinate simultaneous development of the two.

From a theory development standpoint, the development of cyberpower has many similarities with the development of airpower. It is a new domain for international competition, is technology-driven, and has the potential to alter how all elements of the

DIME are used. Additionally, like the development of airpower, development of military cyberpower began as an enabling and supporting function for extant domain powers. As a result, it too is at the mercy of institutional bureaucracies that pursue cyber development as a means of increasing their own domain power.

One significant difference between the early years of cyberpower and airpower development is that, with cyber, the commercial sector has taken the lead in domain advancement. Without a means to provide guidance and regulation to commercial industry, a nation risks losing control of its cyber domain development in a way that will benefit commercial interests, while at the same time putting national security at risk.[47] Additionally, penetration of the domain into all institutions and all levels of national and state governments means that coordination across many different interest groups must take place. As various legislative and regulatory agencies seek to exert control over the domain and associated commercial industries, a central coordinating authority will be invaluable. Without one, the required cross-government integration of efforts to develop overall national cyberpower will not take place. As a result, commercial development of

[47] There are indications that senior civilian leadership is increasingly aware that protection of commercial systems and critical infrastructure is a critical part of cyberpower development. The challenge for policy makers is to decide how to encourage commercial operators of critical infrastructure to account for cyber security requirements when building new systems. In the unveiling of the nation's new cyber strategy, Deputy Defense Secretary William Lynn noted the increasing reliance of military operations on commercial cyberspace lines of communication and critical infrastructure. Acknowledging that these commercial systems are subject to attack, he emphasized that the current cyber strategy emphasizes a joint response across civil government, the Department of Defense, and the private sector. See David A. Fulghum, Paul McLeary, and Bill Sweetman, "Cyber Strategy More of a Wish Than a Plan," *Aviation Week & Space Technology* (2011), http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/awst/2011/08/01/AW_08_01_2011_p28-352024.xml&headline=Cyber%20Strategy%20More%20Of%20A%20Wish%20Than%20A%20Plan&next=20.

the domain will follow purely financial incentives without regard for national security interests.

It is apparent that the same domain development challenges faced by our airpower theorists are present in development of the cyber domain. It is equally clear that historical experience with airpower development points to the benefit of creating domain-centric organizations for championing and coordinating development of domain-centric power for both military and commercial use. We can therefore safely assume that this element of domain power travels well into the cyber domain.

Does this element of domain power travel to the cyber domain? Yes.

What does this mean for cyber theory development? Following the model of our airpower theorists, cyber theory must explain the rationale for creating domain-centric management functions within both military and civil government institutions.[48] It should explain the ways in which integrated commercial and military development increase national cyberpower and increase overall national cyber security. Unlike the airpower theories, cyber theory should discuss the role of government in guiding commercial led development of the domain to balance cyberpower's commercial and military interests.

13. *The state of domain technology determines the dominant character of domain forces.*

[48] Based on the decades-long struggle for independence by airpower and the now 60-year-plus treatment of the space domain as an adjunct to existing military power, actually establishing a separate service or creating a new government agency seems unlikely. Without some external event to rally around, there are too many cyber-related interest groups spread across government agencies to develop a consensus on roles and responsibilities of any new organization. Despite this pessimistic statement, a large step forward in providing coordinated, non-service-centric perspectives on military cyber development has taken place. The establishment of Cyber Command is in some ways similar to setting up the Army Air Corps – an acknowledgement that this domain requires focused and coordinated oversight in order to develop effectively. On the commercial side, we have not yet seen the development of full-fledged cyber oversight or a regulatory body. Establishment of a Cyber Czar is an indication of growing awareness within the Executive Branch that some form of cross-government cyber coordination is required.

At the time of their writing, each of our reviewed domain theorists made judgments about the nature of force in his respective domain. With the benefit of hindsight, we see that in actuality they were judging the dominant character of force in the domain based on current technology. Over intervening years, we have come to understand that as technology changes, so does the dominant character of force.[49]

Within the cyber domain, current technology does create a dominant characteristic of force; it favors offensive use of cyberpower. There are a number of reasons this is true.[50] First, cyber defenses rely on computer protocols that are themselves vulnerable to exploitation. Rather than work to fix these vulnerabilities, the emphasis of cyber defense is on detecting threats as they occur, not in securing the underlying vulnerabilities in the system that make these attacks possible.

Even with defenses in place, it is difficult to detect, analyze, and respond to cyber attacks. The speed of attacks in cyberspace makes providing active defense extremely difficult. While the defense requires 100% success, in many cases the offense needs only one success. Moreover, attacks can originate from any point in the cyber domain, making it impossible to create effective defenses by focusing on a single adversary. Even after identifying a potential adversary, because attribution in cyberspace is difficult, deterrence or threats of punishment are challenging. Finally, the penetration of cyberspace into almost every aspect of a nation's civil and military systems makes the job of providing

---

[49] Our maritime theorists write that defensive operations are the stronger form of warfare. Offensive operations, they claim, require a significant massing of domain power to break defensive positions. During the decades following Cobbett's writing, submarines came along, throwing doubt upon their claims. Our aerial theorists make the opposite claim. A lack of defensive options leads them to emphasis airpower's offensive nature. Eventually, air defense weapons improved to provide effective defensive operations, once again throwing our theorists claims into doubt.

[50] The five reasons listed here are adapted from Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 98-9.

defense across such a wide array of targets, and all four layers of the Internet, a nearly impossible job.

That state of domain technology determines the dominant character of force in cyberspace. Understanding the role technology plays in determining the dominant characteristics of force in the cyber domain is important to the theory development process. It allows cyber theorists to create plausible operational scenarios that serve as illustrative points for justifying investment in the domain. These scenarios lend operational credibility to the theory, making it easier for the community of scholars and operators to find common ground. Finally, it helps them predict changes in technology that will alter the character of cyberpower, making it either neutral or defensive. Successfully predicting the change will provide an advantage to properly prepared nations. These are important factors to consider when moving a domain beyond the pre-theory stage.

Does this element of domain power travel to the cyber domain? Yes.

What does this mean for cyber theory development? Emerging cyber theory needs to address the dominant offensive characteristics of cyberpower. It will explain the role of technology in determining the dominant characteristic and describe what changes in technology would swing the pendulum back in favor of the defense. Cyber theory must also describe the role of both government and commercial industry in providing a nation's cyber defense.[51]

14. *The pursuit of domain control is the primary function of domain-centric forces.*

[51] Currently the responsibility to defend the .mil domain rests with the pentagon. Responsibility for defense for the .gov domain lies with the Department of Homeland Security. Commercial cyberspace users are largely responsible for providing their own defense.

Maritime and air theorists both stress the requirement to first secure control of the domain. They each also suggest that control over their domain is possible only by use of domain-centric forces. They reach these conclusions because at the time of their writing, each believed it was possible to gain control over a domain through its denial to an enemy. Further, our theorists operated from an assumption that no other domain was capable of projecting power into their domain, making the use of domain-centric force the only means of gaining control.[52]

The same underlying assumptions do not apply to the cyber domain. In reality, it may be impossible to deny the cyber domain to an adversary or to gain total control over it. The domain is simply too large and dynamic. Instead of domain control, gaining temporary or local superiority is the more likely function of cyber forces.[53]

Additionally, exercising control over an enemy's use of the cyber domain is possible through cross-domain operations. For instance, destruction of an enemy's physical infrastructure or the seizure of chokepoints can disconnect an adversary from the global grid. This frees up cyber forces to concentrate on exercising domain control or execute cross-domain attacks.

Another important consideration in determining the primary role of cyber forces is that they are unlikely to be used alone as a coercive instrument of national power.[54] Their true value is as an enabler for overall national efforts across all domains and all

---

[52] Had modern airpower existed when Mahan and Corbett were writing, they would have been unable to discuss gaining maritime domain control solely through maritime power. The ability of airpower to project force across domain boundaries made attack upon maritime forces a large part of their domain theory arguments for a separate service.

[53] "Superiority in any domain may not be widespread or permanent; it more often will be local and temporary." See U.S. Department of Defense, "Joint Operational Access Concept," ii. One way to achieve local superiority in cyber is to compartmentalize the domain to deny or restrict access as is often done with systems for processing classified data.

[54] Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 104.

levers of power.[55] In this role as an enabler, the opening cyber salvos of a conflict will not focus on simply gaining command of the cyber domain. Instead, they will focus on degrading an enemy's ability to use its own elements of the DIME.

For all these reasons, it is not possible to conclude that the primary function of cyber domain power is to gain control over the domain. In addition to a cyber force's role as an enabler, they must also focus on defending critical domestic infrastructure and vital points. At best, cyber forces will split their time between gaining command of the domain, defending it, and exercising domain power operations in support of other elements of national power.

Does this element of domain power travel to the cyber domain? No.

What does this mean for cyber theory development? Cyber theory must describe the domain's role in support of offensive and defensive operations across all elements of the DIME and all domains. Cyber theory should account for this unique aspect of its domain power and describe the type of forces necessary to carry out varying operational roles within a contested domain.

15. *Vital points exist as convergences of lines of communication.*

Maritime and air theory clearly demonstrate that vital points within their domain are created where lines of communication intersect. We have discussed this in-depth concerning the cyber domain, concluding that the convergence of physical lines of communication are indeed vital points within cyberspace. The multilayer make-up of the

[55] Corbett took this approach to seapower. He wrote, "Since men live upon the land and not upon the sea, great issues between nations at war have always been decided – except in the rarest cases – either by what your army can do against your enemy's territory and national life, or else by the fear of what the flee makes it possible for your army to do." Corbett, *Some Principles of Maritime Strategy*, 16.

cyber domain, however, means simply defining vital cyber points as the convergence of lines of communication is too narrow.

Vital points within cyberspace also exist at the logical and information layers of the Internet. The movement of information from one location to its proper destination along the Internet relies on two distinct databases, both of which are vital points. One is the domain name system that assigns Internet addresses to each cyberspace location.[56] The domain name system acts like a phone book for the Internet, matching names with the computer address assigned to each location. Altering the database that looks up the correct address for each domain name will send all traffic for that site to the wrong location. Obviously, that database becomes a vital location, requiring protection or control depending on your intentions and interests.

A second database comes into play once information is moving within the system toward a destination address. The Border Gateway Protocol (BGP) in combination with routers acts as the postal sorter of cyberspace. Essentially, the BGP database is a list of Internet service providers and the domain addresses each supports. As information packets move through lines of communication, at each intersection the BGP provides direction as to which turns to take. Once again, the database and logical systems supporting this function are critical to the movement of information, making them vital points within the cyber domain.

---

[56] A complete discussion of information routing within the cyber domain is beyond the purposes of this dissertation. Richard Clark provides a very clear, non-technical description of this process in *Cyber War*. Although simplified, in a four-page span he traces the movement of a single webpage request from his computer to the host server. The metaphors used in the discussion above come from his description. See Clarke and Knake, *Cyber War: The Next Threat To National Security And What To Do About It*, 74-78.

In conclusion, vital points do exist in the domain as convergences of lines of communication, but this definition is too narrow. From the discussion above, we understand that in addition to vital points at the convergence of lines of communication, virtual vital points exist in the other layers of cyberspace. The intent here is not to review each potential vital point, simply to recognize that the element of domain power transfers to the domain but is insufficient as a means of identifying all vital points in the domain.

Does this element of domain power travel to the cyber domain? Yes, but it is insufficiently inclusive.

What does this mean for cyber theory development? Cyber theory must explain what constitutes a vital point within each layer of the domain. It must also relate each vital point to efforts at gaining and exercising control over the domain.

16. *The capability to project power across domain boundaries affects an adversary's will and ability to resist in other domains.*

Because airpower can project power across domain boundaries, our airpower theorists emphasize its ability to directly target an adversary's critical infrastructure and affect an adversary's will and ability to resist. In a related claim, they point out that an aircraft's ability to bypass contested surface domains allows it to provide direct support for the DIME without the requirement to control an over-flown domain.

Cyber domain power exhibits some of the same key characteristics. For instance, a cyber attack against an enemy's critical infrastructure, such as an electrical grid, can paralyze it, leaving it unable to respond to attacks and directly affecting the enemy's will and ability to resist.[57] Another example is the alteration of targeting information within a

[57] There is some evidence that the US electrical grid has already been penetrated and mapped in preparation targeting during for future conflicts. An adversary would presumably find the use of

military database. Done covertly, this may prevent an enemy from effectively responding to an attack, thus demoralizing it and directly affecting its will to continue resisting.

The ability of cyberpower to create cross-domain effects has the potential to alter force structure for military operations within other domains. Despite this implication of cyber development, we have not yet seen organized institutional resistance to fully developing cyberpower as that which occurred during the development of airpower. Future efforts to create separate cyberpower organizations may trigger a reflexive response from established interest groups, a response cyber advocates must prepare to overcome.

Clearly, cross-domain power from cyberspace is capable of bypassing contested surface domains. It is also clearly capable of directly attacking an enemy's will and ability to resist. This element of domain power travels well into cyberspace.

Does this element of domain power travel to the cyber domain? Yes.

What does this mean for cyber theory development? Cyber theory needs to explain the domain's ability to bypass contested domains and directly target systems critical to an adversary's will and ability to resist. It should describe the capabilities required to perform these missions and the amount of domain control necessary to facilitate operations. Cyber theory must also fully tie in the use of cyberpower with operations across the DIME and within other domains. The failure to describe cyberpower's role in creating overall national power risks misuse of national resources through development of more costly forces in other domains.

17. *Rapidly changing, and highly dynamic technology makes creation of enduring domain power problematic*.

---

cyber attacks an effective means of countering American military superiority in the other domains. Clark, "China's Cyberassault on America."

Drawn from Seversky's airpower theory and developed in Chapter 6, this element focuses on the ability of a nation to gain and maintain enduring power within a domain. In Element 13 above, we discussed the dominant character of domain power and technology's role in determining the relative strengths of offensive and defensive forces. Building on that understanding, this element captures the proliferation of advanced technology and its influence upon national domain power.

The more technologically dependent a domain is, the more significantly changes in domain-centric technology affect a nation's overall domain power. No domain is more technologically dependent than the cyber domain, as without technology, it ceases to exist. The technology upon which the domain depends is constantly advancing, eclipsing older technologies, or making them vulnerable to new and innovative attacks.

The relative ease with which cyber technology proliferates makes it very difficult for a nation to create and maintain domain power without continuous reinvestment in its equipment, networks, and personnel. A nation on the cutting edge of technology may find that for political, legal, or financial reasons it is unable to adopt new technology, causing it to fall behind as other nations advance. The sensitivity of cyberpower to marginal qualitative upgrades creates conditions in which a nation may gain and lose cyber domain power with small changes in the capabilities of its cyber systems.

This is not simply a military aspect of domain power. Commercial cyber technology development and upgrades to the commercial networks upon which most information travels provide increased power to other elements of the DIME. An example of this is investment in ultra-low-latency transatlantic cables between currency traders in

New York City and London.[58] Electronic trading of international currencies using automated computer algorithms makes the reduction of milliseconds in latency a competitive advantage for investors and a nation's economy. Across the DIME, robust and innovative cyber systems provide actors with the ability to quickly identify changes in the international environment and to react before their opponents, creating a strategic advantage and increasing national power and influence.[59]

The technology-dependent nature of the cyber domain makes the balance of domain power especially sensitive to technology changes. Advances in technology alter offensive and defensive capabilities, empower intrusion and intrusion detection software, and change hardware processing speeds. Clearly, this element travels into the cyber domain. The implication of this determination is that once a nation commits itself to creating cyberpower, it must adopt long-term strategies to continuously update and upgrade its means of exercising this power across all four layers of the domain. The failure to predict technology changes or adopt the proper technology will result in a rapid decline of domain power.

Does this element of domain power travel to the cyber domain? Yes.

What does this mean for cyber theory development? Cyber theory must include a description of the domain, as well as its dependence on technology. It should also describe the effect of technology changes across all four layers of the domain. This aspect

---

[58] HiIbernia Atlantic, "Hibernia Atlantic to Construct the Lowest Latency TransAtlantic Submarine Fiber Optic Cable Network from New York to London " *Disaster Recovery Journal* (2010), http://www.drj.com/industry/press-releases/hibernia-atlantic-to-construct-the-lowest-latency-transatlantic-submarine-fiber-optic-cable-network-from-new-york-to-london.html.

[59] Operating inside of a competitor's decision cycle is a concept borrowed from military aviation and operational planning. First popularized by USAF Colonel John Boyd, the observe, orient, decide, and act (OODA) loop concept stresses making decisions faster than an adversary in order to take advantage of its position and inability to respond to rapidly changing conditions.

of cyber theory should focus on the requirement to continuously react and adapt to new technology as a means of gaining competitive advantage.

18. *International trade is critical to creating domain power*.

Mahan's maritime theory touches upon the use of international trade to create domain power using what we would call *soft power* today. Mahan is not alone in alluding to the effect of international trade, but simply the theorist who most directly ties development of trade to the development of domain power. His point is that by participating in international trade through the domain, a nation creates a domestic incentive to develop domain capacity and protect domain access and use.

This is certainly as true with the cyber domain as it is for the maritime domain, and perhaps even more so. By itself, the cyber domain has no value. The cyber domain's ability to rapidly transfer information gives it value. The only motivation a nation has for investing in and building cyber domain systems comes from the desire to engage in information exchange.

We have already identified that commercial development is the key to creating cyber domain systems; commercial and private individuals own and operate the majority of all cyber infrastructure. Without a commercial incentive to develop a nation's domestic cyber infrastructure or to create robust connections to the global network, a nation has little hope of creating and maintaining enduring cyber domain power. International trade creates this incentive.

By encouraging citizens to participate in international trade via the cyber domain, a nation increases its domestic use of the domain, resulting in increased domestic demand for robust and redundant cyber infrastructure. This demand provides the necessary

financial incentive for investment in cyber infrastructure and for creation of domestic human capital.

Beyond incentives to create domestic cyberpower, international trade presents opportunities to create domain power in other ways. The exportation of cyber technology establishes a customer's dependency on continued support for upgrades and service of infrastructure and programming. This provides an opportunity continuously to access and map global cyber networks for exploitation in the future. It also offers the chance to establish international standards of operation and network protocol that provide the supplying nation backdoor access to an adversary's systems if necessary.

A nation's participation in international and domestic trade via the cyber domain is a clear incentive to development of its cyber domain power. Commercial incentives are necessary for investment of cyber infrastructure and to provide opportunities for creating the human capital and industrial base necessary to become a cyberpower. This element travels into the cyber domain. Expansion to include domestic trade in future analytical efforts will capture the overall effect of trade on creating domain power.

One implication of this conclusion is that any government policy discouraging participation in trade through the domain weakens national cyberpower potential by reducing commercial incentives to develop the domain. Because they reduce commerce within the domain, policies such as taxing cyber commerce may have far-reaching effects on a nation's cyberpower development.

Does this element of domain power travel to the cyber domain? Yes, this element should also capture the incentive that domestic trade provides to developing domestic infrastructure and human capital.

What does this mean for cyber theory development? Cyber theory should explain the role of international and domestic trade in creating incentives to develop cyber-centric infrastructure, human capital, and industry. It must connect these three sources of domain power with the creation and use of commercial and military cyberpower during peace and war, describing how they add to a nation's overall domain power and national security.

The preceding review of the eighteen common elements of domain power created in Chapter 6 has demonstrated and assessed their utility as guides for development of cyberpower theory. The majority of these elements proved valid as elements of domain power capable of transferring into the cyber domain.

Elements 9 and 14 proved unable to transfer into the cyber domain. The focus of Element 9 is gaining domain control by eliminating an adversary's ability to enter it, a nearly impossible task when undertaken in cyberspace. The cyber domain's lack of defined access points and its adaptive nature make total denial of domain access unlikely. Instead, control over an enemy's movements within the domain, and its isolation from the global information grid, are objectives more appropriate to pursue. Expressing this element of power for application to the cyber domain would more closely follow the Corbettian model than the majority view identified in Chapter 6. Incorporating Corbett's temporary and localized aspects of domain control, a cyber-focused expression of this element is: *Cyber domain control is gained by isolating an enemy from the global information grid and managing its access where isolation is impossible*.

Element 14's focuses is on the use of domain-centric power to first gain control over the domain and then turn to exercising control. The speed of operations in cyberspace and the requirement for many cyber operations to act as first-strike or

preemptive operations mean that at best cyber forces will split their time between gaining and exercising control over the domain. Expressed more appropriately for cyberspace, the element would read: *The exercise of domain control is the primary function of cyber domain forces, supporting cross-domain operations while restricting the enemy's use of the domain when possible.* The following pages present a tabular summary of our results from the comparisons above.

Table 8: Transfer of Common Elements into the Cyber Domain

Results of Analysis: Common Elements of Domain Power		
	Common Element of Domain Power	**Transfer Into the Cyber Domain?/Assessment**
1	The use of domain power to exercise domain control ensures freedom of action within the domain while denying the adversary freedom of action. Cross-domain power can exercise cross-domain control.	Yes/Control over the cyber domain is exercised by controlling chokepoints where lines of communication intersect.
2	The objective of exercising domain power in a commons is to affect an enemy's will and means to resist.	Yes/Targeting of cyber-enabled critical infrastructure can degrade an adversary's means to resist.
3	Governments must emphasize strategic development of domain power through incentives, coordination of military/civilian development and treaties as part of its long-term national strategy.	Yes/Government involvement in creating domain security is more important to cyber development than industry incentives.
4	Domain power development is a subset of overall national power across the DIME.	Yes/Cyberpower's ability to enhance power across other domains and the DIME requires coordinated development with all other aspects of national power.
5	Simultaneous military and commercial domain development are necessary to become an enduring domain power.	Yes/Cyber domain development is commercially led. Governments must emphasize security and military development that keeps pace with changes in cyber domain technology.
6	Creation of domain power must occur before a crisis or conflict begins.	Yes/Creation of offensive and defensive cyber operations requires extensive pre-mapping of cyber networks and pre-planning to assess effects
7	Control over chokepoints where lines of communication converge or terminate is the most efficient means of exercising domain control and leads to enduring domain control.	Yes/Chokepoints provide an opportunity to restrict the flow of large volumes of information worldwide through control over physical infrastructure.
8	The exercise of domain power is a multistep process: first gaining command of the domain and then exercising command of the domain (to included projection of power across domain boundaries).	Yes/Control over cyber chokepoints denies an adversary effective use of the domain.
9	Gaining domain control means eliminating the enemy's ability to enter the domain or use its lines of communication.	No/It is impossible to effectively eliminate an adversary's access to cyberspace.

10	A nation's geography affects its domain power potential, vulnerability to attack from the domain, influence over lines of communication, and incentive to develop domain power.	Yes/Cyber geography consists of interconnections, not physical locations. A limited number of connections carry the majority of the world's cyber traffic.
11	A nation's population affects domain power through the creation of domestic reserves of both personnel and knowledge available in times of need.	Yes/A large populations provide a deep pool from which to draw and the political and commercial basis from which to develop cyberpower.
12	Domain power development requires the creation of domain-specific governmental institutions and cross-domain coordinating bodies.	Yes/Separation from other domains allows full development of domain-centric capabilities.
13	The state of domain technology determines the dominant character of domain forces.	Yes/Current technology favors offensive use of cyberpower.
14	The pursuit of domain control is the primary function of domain-centric forces.	No/Cyberpower is foremost an enabler across the DIME, and gaining control over the cyber domain may not be possible.
15	Vital points exist as convergences of lines of communication.	Yes/Vital points exist at physical convergences of lines of communication. They also exist at other layer of the domain, such the BGP and DNS.
16	The capability to project power across domain boundaries affects an adversary's will and ability to resist in other domains.	Yes/Cyberpower can bypass contested domains and directly target critical infrastructure.
17	Rapidly changing and highly dynamic technology makes creation of enduring domain power problematic.	Yes/Highly mobile, rapidly changing technology requires continuous reinvestment.
18	International trade is critical to creating domain power.	Yes/Trade creates commercial incentive for domain development.

Domains and Domain Theorists

We began this project to determine a basis for building a theory of cyber domain power. The eighteen elements developed from extant theory and assessed above indicate that extant military domain theory can serve as the basis from which to begin. The following sections briefly discuss how well the body of theory from each domain and each of the five theorists matches up with what we have learned about the requirements for future cyber theory.

Domains

Neither maritime nor aerial domain theory provides a perfect match for cyberspace; neither can serve as a standalone template for creating cyber domain theory. By combining the two, however, we capture key aspects of both domains that do provide guidance for development of cyber domain theory.

Maritime Domain

Pulling from maritime theory, cyber domain theory benefits by capturing the concepts of lines of communication, chokepoints within a global common, and the importance of balanced military-commercial development of the domain. Although air domain theorists also touch upon these concepts, the maritime theorists tie them to development of national power more clearly.

For cyber theorists, these concepts provide a conceptual model to explain how information travels through the common and why control over key geography – chokepoints – facilitates the exercise of domain control. Using this model, the rationale for developing domestic commercial infrastructure and redundancy of domestic networks

becomes an easier sell to policy makers. Similarly, strategists can use the model for identification of capabilities, force structure, and resources required to defend and attack vital chokepoints within the commons. This focus provides direction to military and civilian leaders working to decide how and where to expend national resources to control the cyber domain. Based on the analysis here, control of chokepoints within the physical and virtual commons is the best way to spend those resources.

Aerial Domain

From aerial domain theory, the developers of cyber domain theory should draw forth discussions of bypassing contested territory to strike directly at an enemy's means and will to resist. Air theorists are also more skilled at articulating the requirement for government involvement with industry in order to shape and develop critical aspects of the domain. Finally, air domain theorists provide a template for arguing the requirement to develop separate organizations, outside of the current/traditional domain structure, to provide oversight for a new domain.

Cyberpower's ability to bypass contested territory mimics airpower in its seductiveness to strategists. Conceptually, a cyber silver bullet may exist to overcome an enemy's means and will to resist. More realistically, however, cyberpower provides promise as an enabler to levers of power across the DIME and the other domains. Strategists must integrate cyberpower into operations at the national level, much as military strategists have learned to integrate airpower with land and maritime operations today.

Like airpower, cyberpower depends on commercial development of the domain. We have already discovered that unlike airpower development, commercial development

drives cyberpower. This twist on the concept does not relieve governments of the responsibility to create cyberpower; it changes their focus. Instead of incentivizing cyberpower as they did with airpower, governments must balance it, carefully regulating and managing its development along both commercial and military lines. With cyber, the danger is developing an imbalance of power, not a failure to develop power. Overdependence on commercial development creates systemic vulnerabilities that only equally robust military and security development of the domain offset.

Cyberpower, like airpower, began as a means to enhance and support operations within other domains. Operational experience and improved technology have now grown cyber capabilities to a point where further development of the domain may suffer because of limited vision and funding provided through traditional defense and civil organizations. How successfully integrated the domain's commercial and military sectors are depends on the oversight put into place at the federal level.

Theorists

None of our five reviewed theorists appears to be an ideal choice to serve as the basis for development of cyber domain theory. As we discovered during the review of each theorist, they wrote to address specialized domains and often with an agenda in mind.[60] When assessed as a group, combinations of elements from each theorist's work provide guidance that will assist cyber theorists in the future. Considering all five simultaneously, we arrived at the eighteen elements of domain power above. What

[60] Mahan's argument that the US needed a large navy, Corbett's call to correct an imbalance of battleships and cruisers, and our air theorists' universal call for an independent force are some macro examples of the agendas present in their writings.

follows is a brief review of key areas from which cyber theorists can benefit when looking for inspiration and guidance.

Mahan: From Mahan's writings, theorists will benefit most by concentrating on his discussion of the six factors that determine a nation's seapower: geographical position, physical conformation, extent of territory, number of population, character of the people, and character of the government. A similar discussion of the factors that determine a nation's domain power potential must be included in a complete theory of cyberpower. Mahan's major shortcoming is his concentration of gaining complete control over the domain, which prevents him from fully expanding on exercising control over the maritime domain. As we learned above during the discussion of common domain power elements, the concept of total domain control does not apply well to the cyber domain.

Corbett: Where Mahan failed, Corbett succeeded. His theory provides a good starting point from which to begin discussing the use of domain power for exercising domain control. His focus on exercising, not gaining, and maintaining, domain power is more appropriate to the cyber domain than that of our other four theorists. Additionally, his use of temporary and localized control over a domain to achieve specific operational objectives provides guidance for inclusion of a similar discussion within cyberpower theory.

Douhet: Douhet's focus on using domain power to strike directly at the adversary's means and will to resist is a good starting point for discussing the use of cyberpower in support of overall national efforts. Douhet's emphasis on striking hard and fast before an enemy can mobilize defenses travels well into the cyber domain. His focus on targeting an enemy's population to reduce the will to continue resistance, however, is

not compatible with cyber theory development. Historical experience as well as international law and custom prevent the sort of total war he envisioned.

Mitchell: Future theorists will benefit from drawing upon Mitchell's discussions of the role government plays in creating domain power through support of commercial industry. His discussion of the means by which commercial infrastructure and human capital development provide a basis for creating military power is equally applicable to the cyber domain. Additionally, like Douhet and Seversky, he can also serve as a model for discussions of national-level oversight and the need to create separate bureaucratic organizations to oversee development of new domains.

Seversky: The key take-away from Seversky is obviously the element of domain power directly inspired by his work, the effect of new technology on the distribution of power within a domain. His assessment that new technology can rapidly change the balance of power is apropos for discussing cyberpower development. A nation must continuously upgrade and adapt technology to stay ahead of adversaries. As discussed earlier, new technologies are constantly eclipsing the old within the domain, making offensive and defensive cyber operations reliant on using up-to-date information and capabilities.

Taken together, these guiding concepts provide a solid foundation from which to begin building cyber theory. No one template is available for use in this process. Fortunately, the historical experience of creating domain power in the maritime and air commons as a whole provides solid guidance for cyberpower theory. The lack of historical cyber precedence upon which to fall back means that assistance from cross-

domain theory must be sought and heeded if the domain is to move out of the pre-theory stage. The following table summarizes the findings of this section:

Table 9: Guiding Concepts from Domains and Theorists

Guiding Concepts from Domains and Theorists	
Domain or Theorist	**Conceptual Take-away for Transfer into Cyber Theory**
Maritime Domain Theory	❖ Lines of communication direct the flow of traffic within the global common. ❖ Control of chokepoints along lines of communication allows the exercising of control over the domain. ❖ Balanced military-commercial development of the domain is necessary.
Air Domain Theory	❖ Bypass contested territory to strike directly at an enemy's means and will to resist. ❖ Government involvement with commercial industry is required to shape domain power development. ❖ Separate domain-centric oversight across military, commercial, and civil functions is required.
Mahan	❖ Six factors determine a nation's domain power potential: geographical position, physical conformation, extent of territory, number of population, character of the people, and character of the government.
Corbett	❖ Exercising control over the domain is as important as gaining control. ❖ Local and temporary control of the domain to achieve specific purposes is a more efficient and realistic use of domain power.
Douhet	❖ The objective of exercising domain power is to strike at the enemy's means and will to resist.
Mitchell	❖ Separate domain-centric organizations and bureaucracy are required to coordinate domain development. ❖ The government must manage domain and human capital development across military, commercial, and civil lines.
Seversky	❖ Changes in technology rapidly change the distribution of power within the domain. ❖ Nations must commit to continuous development of the domain to maintain cyberpower.

In Chapter 6, we discovered that a nation's potential to develop domain power is a function of its government, geography, and population. While it is possible for a nation to display leadership in an individual component of this formula, the creation of enduring power in a domain requires all three. The following pages discuss how each of the three components of domain power applies to cyberspace.

Government

As the coordinating element, responsible for determining how a nation takes advantage of its geography and manages the development of its raw human capital, government plays a central role in determining a nation's domain power potential. Without good governance, a rich nation can squander its resources or choose the wrong focus for development of national power – in both cases leaving that nation weak in critical areas and vulnerable to less well-endowed adversaries. As Mahan pointed out, the development of domain power requires a long-term strategic approach by governments to balance military and commercial development of the domain. Nations can create martial power by decree, but without a follow-up long-term strategy, this power will dwindle and fade away. Only through recognition of the domain as a national security priority and implementation of a consistent domain development strategy can a nation become an enduring domain power.

Industrial policy: A nation's industrial policy is its coordinated strategic effort to develop domestic industry in a particular field. It is the summation of government efforts to encourage business development through financial incentives and government-industry cooperation. Industrial policy also includes the actions taken by the government to protect domestic industry from foreign competition and to position domestic industry to create an export market.

The fact that commercial innovation leads cyber domain development within the United States frees the federal government from requirements to focus on stimulation of industry. Instead, it must focus on creating a domestic and international environment friendly to American commercial leadership. The government can do this through treaty

negotiation, intellectual property rights enforcement, and development of international law to establish attribution and criminal use precedents relating to cyberspace.

A long-term national focus on creating cyberpower requires a long-term strategic use of industrial policy to ensure domestic cyber infrastructure and industry flourish. Shortsighted efforts to capitalize from the use of the domain, such as sales taxes or government access fees, reduce incentives for commercial development of the domain. Unique to the cyber domain, from commercial use flows national domain power; policy makers' failure to embrace this unnecessarily restricts a nation's domain power potential.

Regulation: The government's use of regulation to shape the cyber industry is integral to balancing commercial development against security interests. There are several areas where government regulation can create a more secure cyber domain and increase national security. For instance, government regulation can improve security of key infrastructure locations supporting our transoceanic cable beachheads. A failure to secure these beachheads risks an adversary's control over significant portions of a nation's domestic and international traffic within the domain.

A second area that government cyber regulation must address is security requirements for critical civil infrastructure, such as the control systems for water supplies and the monitoring of the smart electrical grid. Without regulation, commercial industry will not invest in securing these critical components of national security; it is not in their best financial interest to do so.[61]

[61] In most countries, critical infrastructure "assets are in private hands, so the challenge now is to develop a strong enough private-public partnership to secure these systems, and to convince people to make that initial investment. Anticipation is often seen as a waste of money." See Grauman, "Cyber-Security: The Vexed Question of Global Rules," 9.

A final example of where government regulation can directly influence commercial development and improve national security is the requirement for private networks to perform deep packet inspection of Internet traffic transiting their systems. Both former White House officials and current FBI director Robert Mueller have proposed this.[62] Deep packet inspection is "the online equivalent of screening a passengers' luggage, to filter out malicious data and flag suspicious activity."[63] The use of deep packet inspections can ward off denial-of-service attacks on systems and identify malicious activity. Deep packet inspection provides a technical means for exercising domain control.

The use of deep packet inspection would provide increased cyber domain security within the US, increasing its domain power. Its use is unlikely to become widespread, however, without government interventions. The costs involved in creating deep packet inspection systems, as well as public relations fears over misuse of information are high, making it improbable that commercial industry will voluntarily undertake this task.

Dedicated bureaucracy: The establishment of US Cyber Command is an indicator that the American government recognizes the value of centralized coordination to cyberpower development within the military. The difficulty of extending this same level of coordination across civil agencies and the whole of government is likely to prove more difficult.

Every agency and institution in the government has an interest in cyber development. The various cyber-related policy concerns that arise often pit legal,

---

[62] Brito and Watkins, "The Cybersecurity-Industrial Complex: The Feds Erect a Bureaucracy to Combat a Questionable Threat," 30.

[63] Ibid. For a more detailed description of deep packet inspection, see Michael Kassner, "Deep Packet Inspection: What you Should Know," ZDNet, http://www.zdnet.co.uk/news/it-strategy/2008/07/31/deep-packet-inspection-what-you-should-know-39454822/.

commercial, economic, military, and intelligence interest groups against each other. As a result, it is difficult for the government to create consistent policy and to articulate and pursue a strategic vision for domain power development.

Overcoming this lack of coordination requires centralized institutions that are capable of speaking with one voice about the domain's development. Without a central clearinghouse for guidance on cyberpower development, each agency and department will operate on its own. Each will use unique internal guidance to develop the domain based on its own interpretations of what best serves national security and their own organizational interests. The US observed the inefficiency of this process playing out in development of the air domain.

If they are properly focused on the US' airpower development experience, policy makers will recognize the utility of creating the required bureaucratic organizations early in the cyber development process. Accompanying this recognition must be actions to create civil oversight within the government to coordinate domestic security, commercial development, and military power requirements across all government agencies.

Geography

Of the three factors in the domain power potential equation, a nation's geography has traditionally been the most difficult to alter. Previously, only through development of some system-changing event, such as the opening of the Panama Canal or discovery of a new passage, did geography change significantly.[64] Within the cyber domain, geography takes on a slightly different connotation. Lines of communication and chokepoints are

[64] The next great alteration of the maritime domain may be the opening of a Northwest passage due to global warming.

still critical aspects of potential domain power, but their man-made nature makes the geography much less permanent. A nation's status as endowed, or under endowed, in cyber geography is often the result of government policy, private investment, and commercial development. Creating and maintaining secure redundant geography and using meshed systems providing multiple paths for information flow create national domain power potential. It also creates vulnerabilities. Securing geographic features is as important as creating them.

Nations must look beyond their borders for cyber geography development. Entire regions rely on a few fiber-optic cables for movement of cyber traffic, potentially restricting even the strongest cyberpower from accessing the region. Treaties, agreements, alliances, and coalitions are all diplomatic efforts a government must undertake to create distant geography, allowing cyberpower to travel freely to wherever a nation's interests lay.

Endowments: Like endowments in the other domains, some endowments within the cyber domain are associated with a nation's location in relation to the domain's major lines of communication. In this case, these lines of communication are international and transoceanic cables. When cables pass through a nation's sovereign territory, they provide access to the domain and the power to significantly affect traffic flowing worldwide. In the discussions of Element 7 above, we noted that inside one building located within Alexandria, Egypt, five cables intersect. These five cables carry 80% of all cyber traffic from Europe to the Middle East. Physical control over this one location provides Egypt with domain power, in the negative sense. It can easily control the facility

and restrict access to cyberspace for much of the world, potentially affecting a nation's ability to exert power in other domains and all across the DIME.[65]

National endowments also include the type of domestic networks a nation has and their redundancy. Obviously, the more interconnections that exist between the various routes across a nation, the more resilient networks are. Nations can also set up separate networks, essentially creating a separate cyber domain that exists alongside of what we commonly consider the global Internet. Air-gapped systems such as military classified networks are a man-made geographic feature that an adversary must overcome to penetrate into a new cyber domain. Nations that create and maintain these networks for critical infrastructure or military operations are theoretically creating protected space for operations "behind the lines" in relative safety from attacks across traditional cyberspace connections.[66] In practice, these systems have proven accessible due to human error or design oversights, but in order to gain entry, an adversary must be willing to invest in finding a way to overcome any defenses well before conflicts begin.

Finally, a nation's position of leadership in the domain can act as an endowment, for instance, the US basing of the Internet Corporation for Assigned Names and Numbers (commonly known as ICANN).[67] Although ICANN is moving toward a multi-stakeholder model for governance, the organization's close ties with the US government

---

[65] The reader will recall that during our discussion of Element 10, we learned of a cut in fiber cables during 2008 that significantly reduced US Air Force remotely piloted vehicle operations due to lack of connectivity between the Middle East and US.

[66] "Cyberspace can be constantly replicated. As an entity, there is only one air, one sea, one space, and one land. In contrast, there can be as many cyber-spaces as one can possibly generate. In reality, there is only one portion of the air, sea, or land that is important: that portion that is being contested." See Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 97.

[67] Created in 1998, ICANN coordinates the global Internet system upon which the domain name system discussed previously relies. Visit their webpage at http://www.icann.org/en/about.

have led to international fears of US control over the Internet at a fundamental level. While direct government influence over ICANN is unclear, its US roots and organizational base mean that American legal, social, and industrial standards form the core of its business practices. As we have seen with other aspects of domain power, a nation's endowments are a function of long-term government policy to create a strong commercial presence in the domain.

Exposure to the domain: Simply put, the more wired together a nation is the more exposure it has to the cyber domain. Much of the population's ability to access the sea and use it for trade determines maritime domain exposure; access to cyberspace determines the development of cyber-related business and social interactions. Increasing reliance on the domain for industrial and personal use creates stronger interest groups associated with domain development and security. These interest groups find it to their advantage to become politically active, helping provide an impetus toward good governance of a nation's cyber infrastructure and business development.[68] Because most Internet infrastructure is in the hands of commercial Internet service providers, a nation's exposure to the domain is itself a function of the commercial environment created by government policy. Without an economic incentive to create the physical infrastructure necessary for increased domain exposure, commercial development will not occur.

[68] Interestingly, David Clark notes that the $100 laptop project. If successful in providing children in the developing world access to cyberspace, it will create millions of military-age young adults who are fully cyberspace-conversant. The peacetime social and economic motivations that generated this project could have long-term implications for international security. See Clark, "Characterizing Cyberspace: Past, Present and Future," 4.

Population

The population factor in our domain power equation is itself a function of several factors, some of which government action influences over time and some of which it cannot. Ultimately, a nation that does not have a population willing and able to engage in cyberspace will not be able to create enduring domain power.

Size: From a domain power standpoint, the more citizens a nation has, the more people it will have available for use as human capital devoted to the creation of cyber domain power. The larger the market for cyber infrastructure and the larger the pool of cyber-faring citizens involved in the domain, the more likely a nation is to develop cyber industries and create robust domestic cyber infrastructure. As industries grow, human capital can be broken off to create military cyberpower. Overall, potential therefore depends on a nation's ability to support a large population and that population's propensity to focus on cyber development.

In the short term, small or sparsely populated nations desiring military cyberpower will be the ones to pursue hiring of mercenaries for creation of offensive domain power; they will let computers do the fighting for them.[69] This is also true for non-state actors who may seek to influence state policy. Over the long run, without continuous investment and development of reliable domestic capabilities to maintain their power, small nations and non-state actors will not create the commercial power necessary to become an enduring domain power. The ability of these small actors to disrupt the

[69] Clark discusses this scenario as one most likely for small nations compensating for their lack of population. See Clark, "Software Power: Cyber Warfare is the Risky New Frontline."

domain or use it for offensive purposes may be significant but is also fleeting. Changes in technology and the geography of the domain will render their advantages obsolete.

Human capital: A nation's human capital development is a function of its education, industry, and culture. A large population without the knowledge, skills, and abilities necessary to support industry and government use of the cyber domain is useless in creating domain power. A well-educated nation with many people employed in domain-associated industries, on the other hand, can create domain power despite a smaller overall population.

Education is the primary variable in creating human capital for cyberpower development. The domain's technology-based nature means that some familiarity with sciences, technology, engineering, and mathematics is necessary for employment in the cyber industry. Technical skills are a prerequisite for creating and maintaining cyber industry and infrastructure. Without a well-educated population and investments in creating cyber-capable workers, a nation will be unable to create its own geography and develop a reserve of military capability for use in times of crisis. Government incentives to create educational tracks for development of cyber professionals are one means of creating human capital that policy makers should consider a policy priority.

Liberal nature: Tied in with education and culture, a nation's willingness to embrace new technology and seek trade and influence beyond its border plays a significant role in determining its cyberpower potential. An inward focus and emphasis on conservative social norms are indicators that a nation or culture will be unable to fully participate in the cyber development process. Because the cyber domain is man-made,

cyberpower development will take on the characteristics dictated by the population from which it springs.

Cultures that eschew technology or are unwilling to open themselves to the free flow of information are at a disadvantage when it comes to developing enduring cyberpower. Unfamiliarity with the domain reduces human capital; the failure to actively seek out and embrace technology limits the potential for domestic cyberpower development in other ways. Lower demand for exposure to the domain results in lower cyber penetration and less redundant cyber geography. This in turn creates fewer personnel eligible to participate in cyber industry and in developing the domain from a regulatory and policy standpoint.

Based on our review of the three factors of domain power above, the United States is in a good position to create and retain enduring cyber domain power. Its domain power potential is high. The federal government is taking steps to play its role as coordinator for domain development. The recent publication of military and civil cyber strategies and creation of bureaucratic elements such as Cyber Command and a Cyber Czar indicate the federal government is positioning itself to include consistent strategic cyberpower guidance as part of its national security plan.

Table 10: US Cyber Domain Power Potential

US domain power potential = High	
Dominant variable ❖ Lesser variable	**US potential**
Government	
❖ Industrial policy	High-business friendly capitalist system
❖ Regulation	Low-poor security for critical infrastructure controls
❖ Dedicated bureaucracy	Low-trending upward
Geography	
❖ Endowments	Medium-competitive industry across physical and virtual aspects of the domain, but highly cyber-reliant critical infrastructure is poorly secured
❖ Exposure to the domain	High-numerous overseas connections and well-developed domestic networks
Population	
❖ Size	High-large population
❖ Human capital	Medium-national emphasis on technical fields necessary to support industry growth is slipping with no plan to refocus efforts on cyber development.
❖ Liberal nature	High-national character is commerce-oriented and outward looking.

From a geography standpoint, the nation's infrastructure is very robust. Internally it has a well-organized system of Internet service providers that create redundancy within the system. A weakness is the nation's lack of strong regulatory guidance on security for critical infrastructure and protection of domestic chokepoints.

Finally, with a large well-educated population and a robust cyber economy, the United States is unlikely to find itself short of personnel to develop and maintain its cyber industry and infrastructure. The population's liberal outlook on technology and freedom of information guarantee long-term involvement in the cyber domain from a commercial and military standpoint.

Tasks of Cyber Theory

Whether cyberpower theory evolves to be prescriptive or descriptive in nature, it will need to perform the tasks suggested by Harold Winton as laid out in Chapter 2.[70] We also know from this review that cyber theory must encompass both military and commercial aspects of domain. It must describe the dual nature of cyberpower and focus on the domain's support of efforts across all elements of the DIME. Ultimately, the more inclusive cyberpower theory is the more utility it has for guiding cyber policy development.

At this stage in the domain's development, it is unlikely that a cyberpower theory formulated during the next few years will be able to clearly address all of Winton's criteria. There is simply not enough historical experience with all aspects of the domain for theorists to draw from. Working to overcome this lack of historical experience using extant theory, however, should generate rough outlines for future theorists to begin filling.

Define the field:[71] As presented earlier, the definition of cyberspace has gone through a number of changes over the years, narrowing down to emphasize the domain's simultaneous physical and virtual nature. A cyber theory must settle this debate, defining the domain and cyberpower, as well as what it constitutes and how it is measured.

---

[70] Descriptive theory works to educate the mind of the decision maker, while prescriptive theory provides concrete guides to action. See Winton, "On the Nature of Military Theory," 27. An example of descriptive military theory is Clausewitz's *On War*. An example of prescriptive military theory is Jomini's *The Art of War*.

[71] John Sheldon outlines these points in his work. His effort serves as the basis for the summary of all five criteria presented here. See Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," 108-09.

Categorize constituent parts: As we have discussed, cyberpower has offensive and defensive uses. It also consists of commercial and military components spread across at least four layers of analysis. Additionally, it is a function of both government and industrial actions. Cyber theory must break out these various components of the domain and identify how they relate to the development of cyberpower. Analysis and description of each component should occur individually and then as a whole to identify how they all fit together. For instance, cyberpower theory must relate the development of physical infrastructure to overall domain power and tie security of critical infrastructure to government regulation.

Explain: Tied in closely with defining the field and categorizing its parts are theoretical explanations of how these parts function together. Describing the use of cyberpower to advance national interests through hard and soft power is important for creating an understanding of when and where cyberpower is appropriate. A cyber theory must address how the power is effectively used and under what circumstances its utility increases and decreases against various nations, societies, and cultures over the long term. Without an explanation tying the strategic use of cyberpower for tasks such as disruption, deception, denial, and destruction to the overall national security strategy, it loses its utility for guiding development of the domain and the creation of policy.

Connect to other fields: Cyber theory must connect the domain and the use of cyber domain power with other fields. Obviously, cyber's penetration into every element of the DIME requires an explanation of how it enables and strengthens efforts in these areas and fits into theories for each of these levers of national power. Cyber theory must also discuss the relationship of cyber theory with overall military and economic theory to

ensure that it ties in with the creation of national power across these broad categories of international competition.

Anticipate: Perhaps the most difficult of Winton's five criteria, a cyber theory must anticipate which aspects of cyberpower are timeless and will continue to remain relevant as technology continues to advance the field. The roles of government, geography, and populations in developing cyberpower are areas where the anticipatory nature of cyber theory will be useful. Additionally, discussions of the cross-domain potential for cyberpower and its use to enhance and enable power in other domains will benefit from identifying enduring characteristics of cyberpower use.

Summary

In this chapter, the application of the eighteen elements of domain power generated in Chapter 6 confirms that extant domain theory can serve as the theoretical basis from which to develop cyber policy and strategies. Furthermore, the chapter identified that no specific military domain theory serves as an ideal model for development of the cyber domain. The domain's dual physical and virtual nature and its combination of lines of communication and the ability to bypass traditional defenses makes it a unique challenge to theorists who will benefit by pulling concepts from both maritime and air theorists as they undertake their task. Having completed the review of cyber theory and established extant military domain theory as a basis for cyber theory development by validating sixteen of the eighteen common elements of domain power, we now move to the concluding chapter.

Chapter 8: Conclusion

The growing dependence of modern nations on interconnected computer systems has created an explosion of interest in cyberspace. Military, civil, and commercial use of computer networks provides access to vast amounts of data worldwide. Professionals from all fields, without even thinking of it, now rely on cyberspace to perform their core tasks every day. It is safe to say that if disconnected from the global information grid, much of what we consider modern society would at least temporarily fall into disarray.

Recognizing the importance of the cyber environment to all aspects of national power, strategists, military practitioners, and policy makers have begun to grapple with the problem of constructing policy to develop and secure cyberpower. Hampering their efforts is an almost universal lack of understanding about the domain. Few outside of the cyber community have more than a user-level understanding of the domain and what it takes to create, defend, and use cyberpower to ensure a nation's interests are protected. Creating a deeper understanding across communities of interest is usually the role of domain power theory. Unfortunately, at this point in cyber domain development, no theory of cyberpower is available to serve as the basis for education or the touchstone for policy guidance.

> The development of cyberpower is a long-term process. It requires investment in human capital and the accumulation of experience operating within the domain. It is neither possible to create cyberpower overnight or wish it into existence. Cyberpower develops over time as part of a consistent, long-term plan.

Research Review

Recognizing cyber theory's requirement as a precursor to creation of good cyber policy, this research set out to determine a suitable basis from which to begin building cyber theory. Starting with the knowledge that new theory builds upon the foundation of older theories, the focus of this work has been on determining what, if any, elements of extant theory will aid in the creation of cyber theory. The animating research questions for the effort were:

Q1: What is the theoretical basis from which to develop cyber policies and strategies?

Q2: Can existing military domain theory inform the development of a starting point for a domain control theory of cyberspace?

The following two research hypotheses served as a starting point for answering the research questions, bringing organization and clarity to the research effort:

H1: Existing military domain theory can inform cyber theory development and provide a starting point for theory expansion.

H2: Cyberspace is a physical domain, with a defined geography and geostrategic attributes similar to established domains.

The first few chapters of this work identify the role of military domain theory as a conceptual framework, defining the cyber domain and identifying the maritime and air domains as the two sources of theory most closely resembling the cyber domain. These two domains share with cyber a reliance on technology and a designation as a global common, and both rapidly transformed every element of the DIME during the early years of their development.

Focusing on maritime and air power theorists from the early days of each domains' development, a review of five theorists identifies key elements from each to

determine consistent themes for use in creating cyber theory. This review, conducted in chapters 4 and 5, identifies eighty elements pulled from all five theories.[1]

To identify common themes among the five theories, deductive analysis applied in Chapter 6 consolidates these eighty elements down into eighteen common elements of domain power.[2] These eighteen elements reflect consistent themes from the maritime and air domains, suggesting key concepts, insights, and methods for creating domain power. Through their identification, this study has created a baseline toolkit for approaching development of domain power theory. These eighteen elements provide points of departure for discussion of gaining domain control, exercising domain control, power creation, power projection, power protection, and integration of domain power with other sources of national influence.

Unexpectedly, the consolidation process also identified distinct trends in these elements, leading to the conclusion that a nation's domain power potential is a function of three independent variables: its government, geography, and population. All three play prominent roles in the maritime and air theory reviewed here, as they are critical aspects of a nation's ability to create and maintain power within a domain.[3] As critical determinants of a nation's domain power potential, each of these independent variables is itself a product of lesser independent variables. A graphic depiction of this model appears below:

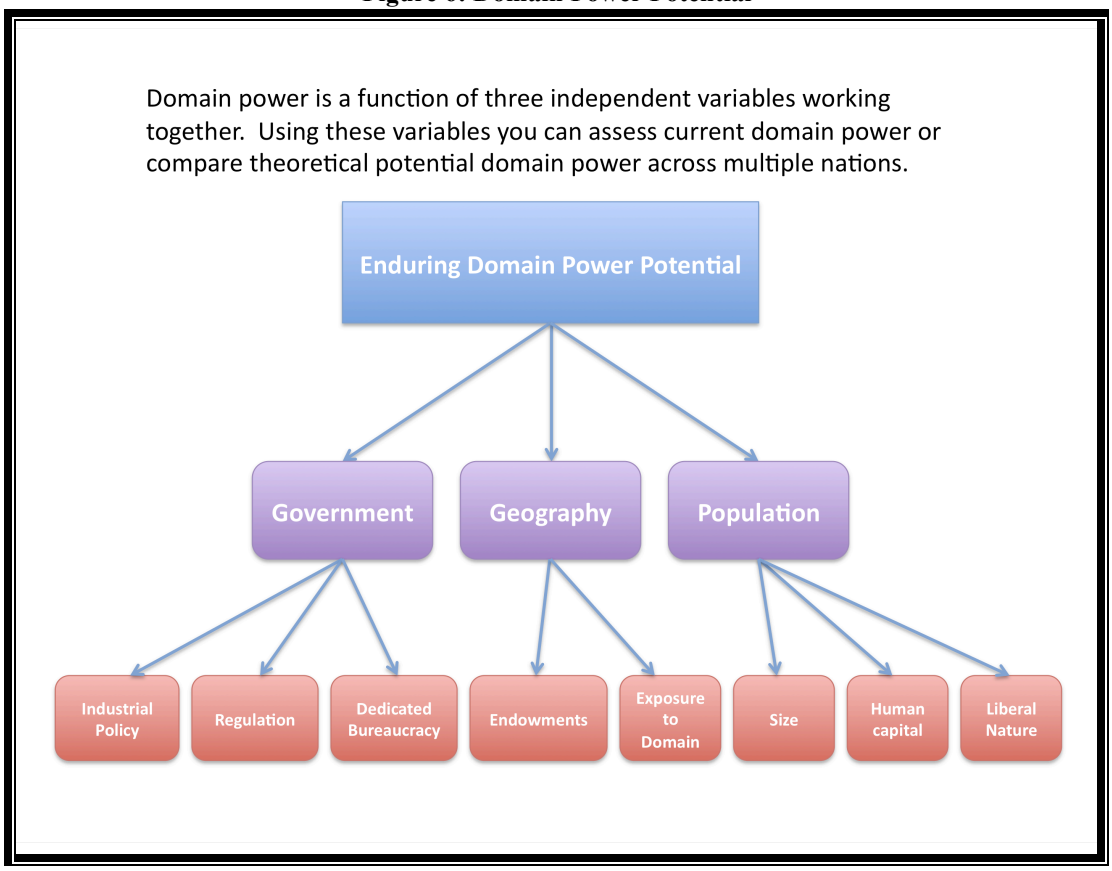
---

[1] The eighty elements appear in two appendices to this study. See Appendix I for the twenty-four maritime elements of domain power and Appendix II for the fifty-six aerial elements of domain power.

[2] The table listing the eighteen common elements of domain power is in Appendix IV to this study and on the left-hand column of Table 8-2: Elements of Domain Power Assessment Results below.

[3] A full discussion of the role played by each independent variable is found in Chapter 6 of this study.

Figure 6: Domain Power Potential



A qualitative discussion of this formula as it applies to the cyber domain appears in Chapter 7 and confirms the model's utility in framing a nation's domain power potential. Fully exploring the relationship of these independent variables to overall domain power was not the focus of this study. Future quantitative research to confirm this model's predictive power requires a separate effort. As applied here, the model provides a means of comparing individual nations to determine current or theoretical potential domain power. An example of this model's potential use, an assessment of current US cyber domain power, appears in the following table:

Table 11: US Cyber Domain Power Potential

US domain power potential = High	
Dominant variable ❖ Lesser variable	**US potential**
Government	
❖ Industrial policy	High-business friendly capitalist system
❖ Regulation	Low-poor security for critical infrastructure controls
❖ Dedicated bureaucracy	Low-trending upward
Geography	
❖ Endowments	Medium-competitive industry across physical and virtual aspects of the domain, but highly cyber-reliant critical infrastructure is poorly secured
❖ Exposure to the domain	High-numerous overseas connections and well-developed domestic networks
Population	
❖ Size	High-large population
❖ Human capital	Medium-national emphasis on technical fields necessary to support industry growth is slipping with no plan to refocus efforts on cyber development
❖ Liberal nature	High-national character is commerce-oriented and outward-looking.

Chapter 7 also uses the eighteen common elements of domain power as a lens to focus discussion on the development of the cyber domain. Using deductive reasoning, each element undergoes an assessment to determine its suitability to guide development of cyber theory. The discussion accompanying each element's assessment identifies key concepts cyberpower theorists must fully develop and analyze if they hope to link the use of cyberpower with pursuit of national security strategy. The following table presents the results of this assessment. It also identifies which theorist's work directly supports each element.

Table 12: Elements of Domain Power Assessment Results

	Common Element of Domain Power	Supported by:					Transfer to the Cyber Domain
		Mahan	Corbett	Douhet	Mitchell	Seversky	
1	The use of domain power to exercise domain control ensures freedom of action within the domain while denying the adversary freedom of action. Cross-domain power can exercise cross-domain control.	Y	Y		Y	Y	Y
2	The objective of exercising domain power in a commons is to affect an enemy's will and means to resist.		Y	Y	Y	Y	Y
3	Governments must emphasize strategic development of domain power through incentives, coordination of military/civilian development, and treaties as part of its long-term national strategy.	Y		Y	Y	Y	Y
4	Domain power development is a subset of overall national power across the DIME.		Y	Y	Y	Y	Y
5	Simultaneous military and commercial domain development are necessary to become an enduring domain power.	Y		Y	Y	Y	Y
6	Creation of domain power must occur before a crisis or conflict begins.	Y	Y	Y	Y	Y	Y
7	Control over chokepoints where lines of communication converge or terminates is the most efficient means of exercising domain control and leads to enduring domain control.	Y	Y	Y	Y	Y	Y
8	The exercise of domain power is a multi-step process: first gaining command of the domain and then exercising command of the domain (to included projection of power across domain boundaries).		Y		Y	Y	Y
9	Gaining domain control means eliminating the enemy's ability to enter the domain or use its lines of communication.	Y	Y	Y	Y	Y	N
10	A nation's geography affects its domain power potential, vulnerability to attack from the domain, influence over lines of communication, and incentive to develop domain power.	Y	Y		Y		Y
11	A nation's population affects domain power through the creation of domestic reserves of both personnel and knowledge available in times of need.	Y			Y		Y
12	Domain power development requires the creation of domain-specific governmental institutions and cross-domain coordinating bodies.			Y	Y	Y	Y
13	The state of domain technology determines the dominant character of domain forces.	Y	Y	Y	Y	Y	Y
14	The pursuit of domain control is the primary function of domain-centric forces.	Y		Y	Y	Y	N
15	Vital points exist as convergences of lines of communication.	Y	Y	Y	Y	Y	Y
16	The capability to project power across domain boundaries affects an adversary's will and ability to resist in other domains.			Y	Y	Y	Y
17	Rapidly changing and highly dynamic technology makes creation of enduring domain power problematic.					Y	Y
18	International trade is critical to creating domain power.	Y					Y

Keeping in mind the domain awareness gained through assessment of the eighteen elements, this study also identifies key concepts from each domain and each theorist to guide follow-on efforts at cyber theory development. Of note is the cyber domain's reliance on physical lines of communication – like the maritime domain – and its ability to bypass fielded forces to strike directly at an enemy's means and will to resist – like the aerial domain. These fundamental similarities create strong links for future cyber theory to both maritime and air theory. The following table presents the results of this assessment:

Table 13: Guiding Concepts from Domains and Theorists

Guiding Concepts from Domains and Theorists	
Domain or Theorist	**Conceptual Take-away for Transfer into Cyber Theory**
Maritime Domain Theory	❖ Lines of communication direct the flow of traffic within the global common. ❖ Control of chokepoints along lines of communication allows the exercising of control over the domain. ❖ Balanced military-commercial development of the domain is necessary.
Air Domain Theory	❖ Bypass contested territory to strike directly at an enemy's means and will to resist. ❖ Government involvement with commercial industry is required to shape domain power development. ❖ Separate domain-centric oversight across military, commercial, and civil functions is required.
Mahan	❖ Six factors determine a nation's domain power potential: geographical position, physical conformation, extent of territory, number of population, character of the people, and character of the government.
Corbett	❖ Exercising control over the domain is as important as gaining control. ❖ Local and temporary control of the domain to achieve specific purposes is a more efficient and realistic use of domain power.
Douhet	❖ The objective of exercising domain power is to strike at the enemy's means and will to resist.
Mitchell	❖ Separate domain-centric organizations and bureaucracy are required to coordinate domain development. ❖ The government must manage domain and human capital development across military, commercial, and civil lines.
Seversky	❖ Changes in technology rapidly change the distribution of power within the domain. ❖ Nations must commit to continuous development of the domain to maintain cyberpower.

Conclusions

Generating the eighteen elements of domain power and applying them to the cyber domain demonstrated a remarkable level of similarity between the cyber domain and extant domains. Sixteen of the eighteen elements of domain power are conceptually compatible with the cyber domain, directly transferring into future cyber theory. Furthermore, the process of analyzing the two outliers identified domain characteristics that provide guidance to cyber theory development. Understanding how these elements of domain power apply to the cyber domain not only aids the theory development process, but also encourages the development of sound policy to create cyberpower.

Following are several conclusions drawn from this research. The first two directly answer this study's research questions, while the remainder represent major insights into requirements for future development of cyber theory. Presentation of each includes a brief discussion of the conclusion and its implications for cyber theory development.

Conclusion I: The theoretical basis from which to develop cyber policies and strategies is a theory of cyberpower development across military, civil, and commercial uses of the domain. A fully developed cyberpower theory along these lines will provide a common framework for reference by all participants in the policy development debate, allowing them to assess the tradeoffs of policy actions, prioritize resource expenditure, and create long-term strategic guidance for development and use of cyberpower.

Conclusion II: Extant military domain theory can inform the development of a domain control theory of cyberspace, specifically military theory for creating maritime and air domain power. As demonstrated with this study, domain power themes gleaned from these two domains provides guidelines for creation of cyberpower theory. While no

single domain provides a stand-alone model for cyber theory development, the use of concepts and insights from across both domains and all five theorists provides many of the required pieces.

Conclusion III:[4] It is impossible to gain total control over the cyber domain.

What this means: The vast number of entry points into the domain and the ability to set up self-contained computer networks makes complete denial of an adversary's use of the domain impossible and efforts along this line of operations resource-intensive. Cyber control is therefore unlikely to result in complete dominance of the domain. Rather than investigating complete control over the domain, theorists and strategic planners should focus on gaining temporary and local control to attack an enemy's capabilities or enable other elements of national power.

> "The US government cannot sustain its cyber dominance with its current uncoordinated approach; cyber is a multidimensional domain that requires a national strategy and strong government leadership"[5]

Conclusion IV:[6] Control of chokepoints is the most efficient means of exercising cyber domain control.

What this means: Cyber theorists, military planners, and policy makers should focus on control of chokepoints, using them to monitor and regulate the flow of information through the global information grid. Identification and protection of physical and virtual chokepoints must be a continuous part of a nation's cyber preparation and overall cyber strategy. Protection of critical chokepoints extends beyond domestic routing all the way into theaters of operation. The fact that this infrastructure is commercially and

[4] Review discussion of elements 1, 9, and 8 in Chapter 7 for further insight.
[5] "Cyber 2020 Asserting Global Leadership in the Cyber Domain," (McLean, VA: Booz Allen Hamilton, 2010), 14.
[6] Review discussion of elements 1 and 7 in Chapter 7 for further insight.

privately owned means that strategists and planners must develop operational models to secure access to the domain across all regions of national interest.

Conclusion V:[7] Cyber theory must educate as well as describe and predict.

What this means: One of the most important functions of new domain theory is to build a common conceptual framework for use when discussing the domain. The reviewed airpower theorists each found it necessary to educate the nation's population while simultaneously presenting propositions on airpower. By doing so, they created a fundamental level of knowledge about the domain necessary for their ideas to resonate and win political support. The cyber domain suffers from a similar lack of popular understanding. Without an understanding of how the domain functions, what constitutes its geography, or the layers of which it consists, policy makers, strategists, and others have no means of evaluating cyber development options. As part of theory development, cyber theorists must identify, include, and explain fundamental concepts such as lines of communication; chokepoints; the roles of government, population, and geography; and operational uses, such as direct attack of an enemy's will and means to resist.

Conclusion VI:[8] Military and commercial domain power must be balanced.

What this means: Military-commercial partnerships are required to ensure development of new technology and systems include provisions for overall national security. Commercial leadership of the cyber development process means that commercial domain power increases more quickly than government-led security and military elements can react. Without coordination between commercial industry and

[7] All five theories educate the reader about its respective domain. Airpower theories, because they focused on an entirely new domain, found it necessary to provide fundamental discussions of domain operations.
[8] Review discussion of elements 3, 4, and 5 in Chapter 7 for further insight.

government agencies, a nation runs the risk of creating an imbalance in cyberpower between national security requirements and industry profitability. Increased commercial reliance on the domain creates robust infrastructure, increasing cyberpower. It also creates vulnerabilities to disruption in cyber traffic. Without simultaneous development of military and security forces to protect domain power and provide the latest in offensive cyber capabilities, a nation risks finding itself unable to use domain power during times of crisis.

Conclusion VII:[9] Creation of cyber-specific institutions is necessary for full development of civil, military, and commercial domain development.

What this means: Following the DOD's lead in creating Cyber Command, development of similarly empowered oversight for civil and commercial sectors of the domain must take place. Because cyber touches all aspects of the DIME, many different government institutions exercise authority over or have a vital interest in the domain's development. Coordinating across various agencies is difficult without a centralized arbitrator to determine the costs and benefits of individual policies. Similar to the development of airpower, bureaucratic interests play a disproportionate role in determining pursuit of polices and their implementation.

Conclusion VII:[10] Government policy plays the pivotal role in determining a nation's cyberpower.

What this means: Government policy determines the effectiveness of efforts to develop domain power. In addition to directly authorizing creation of military cyberpower, government actions create the environment for development of commercial

[9] Review discussion of elements 12 and 16 in Chapter 7 for further insight.
[10] Review discussion of elements 3, 10, 11, 12, and 18 in Chapter 7 for further insight.

cyberpower and human capital. Policies that discourage commercial use of the domain reduce the incentive to create domestic infrastructure, resulting in weak cyber geography and inhibiting creation of cyber-centric human capital. The next section expands upon the vital role government plays in the domain's development.

Near-term Government Focus

This study's seventh conclusion places government policy at the center of domain power development. The domain's commercially led development and manmade nature require specific government oversight to maximize its domain power. By reviewing these points here, outside of the recommendations section below, the author hopes to leave the reader with the understanding that government actions in the near term are vital to setting and maintaining positive cyber development in the absence of unifying cyber theory.

The domain's relative youth and lack of historical reference mean that for practical purposes, a comprehensive and widely accepted theory of cyberpower is a distant target, requiring work across many different fronts to advance the cause. Development of the domain, however, marches on. Closer targets will have long-lasting effects on the United States' domain power potential and require government action in the short term.

To begin with, creating a commercial environment friendly to developing and retaining a domestic cyber industry is critical. The review conducted here identified the role cyber domain industry plays in creating a nation's long-term influence through the use of soft power to set standards and create international norms. Cyber industry development not only requires business encouragement, but also requires careful regulation to make sure it takes into account legitimate national security interests. One

example of necessary legislation repeatedly identified in this study is the creation of security standards for critical infrastructure control systems.

Equally important is the creation of a national plan for developing human capital. The US needs a plan for training cyber professionals for placement in industry and government positions. Allan Paller of the SANS Institute suggests a plan that begins in middle school with basic programming instruction and continues all the way through hands-on graduate level degrees.[11] If these programs are modeled upon teaching programs such as medical school or flight school, such experience-based programs would graduate skilled practitioners who are ready for employment and familiar with cyberpower application from the first day on the job. Federal government initiatives to emphasize cyber education programs like the one suggested by Paller are an example of near-term actions to take without awaiting full development of comprehensive cyber theory.

Table 14: Near-term Government Focuses Items

Areas of near-term government focus with long-term consequences	
1	Creating a commercial environment friendly to developing and retaining domestic cyber industry
2	Creation of a national plan for developing cyber oriented human capital
3	Creation of international cyber standards, norms, laws, and a framework for legal cooperation
4	Developing internationally recognized standards for monitoring and policing cyber operations within states borders
5	Creation of international agreements on information sharing, criminal prosecution, or freedom of movement through the domain
6	Creating domestic policy establishing security standards for critical infrastructure control systems

Another near-term area for action is the creation of international cyber standards, norms, laws, and a framework for legal cooperation. By working to negotiate treaties or creating multilateral agreements, the US could seek to increase good order and good governance of the cyber domain. Creating the

[11] Paller discussed this strategy as part of an interview to promote the National Initiative on Cybersecurity Education (NICE) in 2011. See Brittany Ballenstedt, "Expert Flags Flaw in Cyber Workforce Plan," in *Wired Workplace*, ed. nextgov (2011).

tools to reduce international cyber crime and cyber espionage is in America's security interest. In a secure and stable cyber environment, America's cyber-enabled industries can capitalize on the nation's domain power to extend and deepen their cyber presence. This in turn strengthens the nation's commercial cyberpower. By taking the lead in these areas, the US can shape international norms and law to its advantage.

Efforts to bring order to the domain must focus on nations with weak cyber legislation. These nations either wittingly or unwittingly provide sanctuary within which cyber criminals and cyber protagonists hide and operate.[12] Developing internationally recognized standards for monitoring and policing cyber operations and holding states responsible for enforcement of these standards are good starting points for this effort. Another approach is to broker international agreements to share information on cyber attacks and detected threats within a global forum. Coordinated web-wide responses to identified threats will minimize the damage caused by cyber criminals or individuals/groups intent on launching denial of service attacks or releasing viruses into the domain.

It will not be easy to create international agreements on information sharing, criminal prosecution, or freedom of movement through the domain. American dominance of the domain makes the development of coalitions important to this process. A multinational approach to these efforts will provide higher levels of legitimacy to any agreement that a US effort can attain.[13] With the understanding that reaching consensus within a coalition takes time and patience, the US must provide a consistent example for others to follow. Identifying and supporting basic US interests such as freedom of

[12] Grauman uses the term *weak link countries* to describe nations with poor cyber enforcement. See Grauman, "Cyber-Security: The Vexed Question of Global Rules," 19.
[13] Segal, "Cyberspace Governance: The Next Step, Policy Innovation Memorandum No. 2," 3.

movement within the cyber domain and freedom of access to information can support long-term National Security Strategy goals.[14] Consistently applied over time, US leadership combined with its commercial cyberpower will produce a foundation for international agreements that are compatible with long-term US cyberpower strategy.

As one of the most cyber-dependent nations in the world, the US is also one of the most cyber-vulnerable. The final area for near-term government action is the creation of domestic policy establishing security standards for critical infrastructure control systems. Key infrastructure and sources of national power such as utilities, air traffic control, and the financial markets should be required to meet basic levels of security and redundancy. Commercial industry will not rise to meet sufficiently high security standards on its own; this will require government direction and implementation. The challenge for future researchers is to identify appropriate levels of security and the means for their implementation without unduly burdening commercial industry.

Government's role in creating and securing a nation's cyber geography and in developing its cyber human capital is a critical and underappreciated aspect of the cyber domain development process. Cyberpower is not something that can be created overnight, nor is it something that can be wished into existence when needed. Instead, cyberpower results from a consistent, long-term strategy for its development. Because commercial use of the domain drives cyberpower development, national governments must participate in creating an environment that encourages commercial industry.

---

[14] This can take many forms, one of which is US government support for US-based corporations as they try to compete fairly and maintain access in foreign markets. An example of a US corporation working to support corporate interests in line with US national security interests in the domain is Google's recent tensions with China. Using its considerable influence in the domain, Google threatened to pull out of China in the face of censorship. See Brimley, "Promoting Security in Common Domains," 126.

Future Cyber Research

The author's recommendations for further research are broken into two sections. This section covers recommendations for research based on observed gaps in cyber literature and a lack of commonly shared terminology within the field of study. Filling these gaps is a necessary precursor to creating a theory of cyber domain power. The follow-on to this section will present recommendations for further domain power research based upon the original work performed here.

Define the domain

Coming to a shared understanding of the domain and its terminology is a necessary step toward development of a comprehensive cyber theory. To begin with, there is no widely agreed upon definition of the domain. In Chapter 3, this research reviewed the historical development of the cyber domain concept, eventually settling on a definition focused on the domain's physical and virtual nature. This definition is consistent with military approaches to defining the domain but has yet to gain widespread acceptance across academic and government institutions. Adoption of a consistent definition across academic, military, and civil organizations will provide a firm basis for cross-community development of common terminology and discussions about creation and use of cyberpower.

Develop and define universal terminology

Second, during the course of this research, the author identified widespread inconsistent applications of terminology to the domain. For example, many cyber professionals use the word *attack* to describe almost any event outside of normal cyber

operations. Overuse of the word *attack* clouds discussions about proper responses to different levels of aggression and responsibility for protection of infrastructure. Various camps within the cyber community apply different standards to the definition of attack.

> "The number of times a computer network is probed is not evidence of a breach, an attack, or even a problem."[15]

For instance, cyber security experts and those concerned with protection of consumer and industrial information consider any probe of networks or attempts at cyber theft and espionage to be attacks.[16] Following this line of reasoning, the system is constantly under attack from state and non-state actors. Military planners, on the other hand, fall back on much more restrictive definitions, searching for a threshold that requires (or allows) a response.[17] Deciding what constitutes an attack is important, as overuse of the term tends to militarize thinking about domain security, limiting policy options and creating an expectation of government control over what is essentially a commercially driven domain.[18]

---

[15] Brito and Watkins, "The Cybersecurity-Industrial Complex: The Feds Erect a Bureaucracy to Combat a Questionable Threat," 31.

[16] Grauman identifies three distinct categories for cyber activity of his type: cyber espionage, cyber crime, and cyber war. See Grauman, "Cyber-Security: The Vexed Question of Global Rules," 6. This author takes the position that espionage and crime in cyberspace are not attacks, and labeling them as attacks is an expansion of the term to include operations that are not similarly categorized in the traditional physical domains.

[17] For discussions of this, see Charles Jr. Dunlap, Major General, USAF Retired, "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly* 5, no. 1 (2011): 83-85, See also Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal* (2011), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html#ixzz1O2urKzzR.

[18] "The overuse of the terms *cyber-war* and *warfare* tends to push the cyber-security problem into the government and defense spheres, thereby potentially ignoring the effect of the cyber-threat on the private sector and creating an imbalance in government funding. I try to void the use of the words *cyber-war* or *warfare* as they can lead o the militarization of cyber-space." Tim Scully, CEO of STRATSEC and Head of Cyber-Security at BAE Systems Australia, quoted in Grauman, "Cyber-Security: The Vexed Question of Global Rules," 7.

Once an agreed-upon definition for cyber attack is created, the discussion must move to setting levels of attribution required before responding to an attack and what form of response is appropriate.[19] Debates over the acceptable use of non-cyber force in response to cyber attacks must be resolved before full development of more nuanced security concepts such as deterrence, denial, and punishment in cyberspace can take place.

Define and assign responsibilities for domain oversight

As the research done for this dissertation points out, the role of government in creating and maintaining domain power is crucial. Closely tied in with defining cyber attacks and appropriate responses is the allocation of responsibility to protect cyber networks and their supporting infrastructure. Currently, responsibilities are ill-defined and spread between agencies. The military defends its own .mil networks, and the Department of Homeland Security has responsibility for the civil .gov network. This is problematic for many reasons, not the least of which is that the other "dot" domain names remain unassigned. Who is responsible for protection of the commercial networks that drive development of a nation's cyber domain power? General Hayden, former director of the Central Intelligence Agency and the National Security Agency, has mused that the private sector may find itself responsible for providing its own security.[20] If this is indeed true, research into the legal responsibilities and authorities for action taken domestically

[19] For instance, is an attack using airpower an acceptable response to a cyber attack?
[20] Take from General Hayden's participation in a web broadcast discussion at the Aspen Security Forum in 2011. See Allan Holmes, "ASF 2011: Cyber Security," in *Aspen Security Forum* (USA The Aspen Institute, 2011). Available at: http://www.aspeninstitute.org/video/asf-2011-cyber-security.

and internationally is required.[21] Once responsibilities and legal authorities are in place, policies to properly assign responsibility and empower agencies and organizations to secure and defend cyber infrastructure and cyber systems become possible.

As definition of terms takes place, responsibilities for domain protection are allocated, and the uses of domain power are refined, cyber theorists will increasingly have the tools necessary to describe the use of cyberpower in support of other domains, across all elements of national power. Ultimately, cyber theory must connect the use of cyberpower to combined force efforts in support of overall policy objectives. Cyberpower's cross-domain capabilities provide opportunities to create asymmetrical advantages in other domains, making it an ideal platform for enabling a joint force.[23] Without theory to guide its development or inform strategic planning, realization of a nation's full cyberpower potential is impossible.

> Context matters for attribution purposes. If something occurs with a nation's computer systems while the Chinese are attacking Taiwan, then there is little need to wait for development of detailed attribution evidence.[22]

Further Research Based on This Study

The research done for this dissertation opens two areas for further research, neither of which is necessarily cyber-focused. First is further validation and work on identifying elements of domain power. The work done here was limited to a review of five theorists, across two domains. This study identified remarkable consistency between theories and across domains, yet it is necessarily limited by its sampling of only a small

[21] For more on this, see Clark, "Software Power: Cyber Warfare is the Risky New Frontline."
[22] Summarized from points raised by Daniel Kuehl during a presentation the author attended in 2011. Kuehl, "CYBERSPACE: Its Place in National Security."
[23] For a description of cross-domain synergy, see U.S. Department of Defense, "Joint Operational Access Concept," 16.

subset of overall military domain theory. Future research similar to the effort undertaken here but expanded to include other theorists across other domains will further refine and improve the list of common elements of domain power. Furthermore, work that applies these elements to other fields of competition will improve our understanding of how theory ties in with development of power. A good test for the power of the eighteen common elements developed in Chapter 6 will be to perform an analysis of the space domain similar to the analysis of the cyber domain performed in Chapter 7 of this study. Comparing the results of these two efforts would provide insight for further refinement of the elements of domain power. A space-oriented test would also have the secondary benefit of providing insight into development of spacepower theory, a field that is also far from settled.

Second, the identification of three factors to measure a nation's domain power potential (government, geography, population) creates an opportunity for further research. Having developed the relationship of these three factors into a rough theoretical model, creation of an empirical formula for quantitative analysis awaits future effort. Work to establish empirical measures for each of the independent variables and sub-variables will provide a means to test the formula's utility. Should testing conducted by means of historical data prove the formula's usefulness, its application to contemporary nations across varying domains will provide a theoretical measure of domain power potential.

The formula's use is not limited to assessing potential power; contemporary comparisons across several nations are also possible by assigning numerical values to each independent variable and comparing total scores. For example, in the sample

assessment of US domain power above, the US received four high ratings, two medium ratings, and two low ratings. Using a scale where high = 3, medium = 2, and low = 1, the US overall score would be 18. Compared across several nations, this provides a means to measure relative domain power.

A Basis for Theory Development

Coming to the end of this study, in an effort to determine if this effort aids the theory development process, we return to Harold Winton's five requirements for military theory. Using each of the five criteria lain out by Winton, the following section identifies where and how this study supports further development of cyber theory to satisfy Winton's requirements.

Define the field of study: The definition of cyberspace adopted here specifically states that the domain has both physical and virtual components. This study confirmed this definition, identifying physical infrastructure as the source of lines of communication and the use of virtual routing instructions to move information within the domain. Furthermore, this study defined the cyber common as the physical and virtual connections between users on the domain's edges.[24] Both of these findings support creation of a universal definition of cyberspace, aiding efforts in defining the field from a physical and conceptual standpoint. Moreover, the review of domain power elements suggests that cyberpower is the ability to exercise domain control by restricting an adversary's freedom of movement within the cyber common while retaining freedom of movement for oneself.

[24] See Chapter 6 for a discussion of the cyber domain and identification of the cyber common.

Categorize the field of study into its constituent parts: This study identifies and applies the domain's four layers to assess their use in the exercise of domain power. Furthermore, during discussions of the eighteen common elements of domain power in Chapter 7, it identifies distinct roles for both commercial and military development of the domain and breaks down planning and operational requirements into both offensive and defensive parts. Taken together, these constituent parts begin to provide an overall understanding of the domain and how each part interacts to form the whole of cyberpower.

Provide an explanation for the elements in these categories: This study did not specifically focus on explaining how cyberpower achieves its desired effects (disruption, denial, deception, etc.). As mentioned in the sections above, explaining each element in detail is an area for future research.

Connect the field of study to other relevant fields: This study clearly identified cyberpower's connection to all elements of the DIME and its use to enable operations in other domains. However, it did not go into detail describing the ways and means by which cyberpower enables the DIME or operations within other domains. Having identified these connections, this study places cyber theory into a subset of overall national security studies. Identifying and exploring cyber theory connections to military, economic, and diplomatic theory require further study.

Anticipate key trends and changes to facilitate policy development: Two trends identified within this study, the use of chokepoints to control the domain and the required development of commercial infrastructure, facilitate policy development and are potential features of future cyber theory.

Contents of a Future Cyber Theory

Based on the discussion above, it is safe to say that this study advances efforts to create cyber domain theory. However, it does not create a cyber domain theory. A fully developed cyberpower theory will include both an analysis of the role played by domain theory and a history of cyberpower development.[25] The analysis of cyber theory's role must discuss the use of cyberpower as an instrument of national power during both peacetime and war, across the entirety of the DIME. Cyber theory will also discuss the integration and use of cyberpower in conjunction with land, sea, air, and space power in pursuit of national security objectives.

Based upon the common elements of domain power identified in Chapter 6, a cyberpower theory should discuss the development of cyber domain capabilities during four types of operations:[26]

1. Control operations: operations that allow your nation to use the medium when and where desired
2. Denial operations: operations designed to prevent use of the medium by adversaries
3. Power projection: operations to project power within the domain to affect adversary cyber operations and also have effects outside of the cyber domain
4. Power protection: operations to protect and ensure use of the cyber domain from interference originating from both within the domain and across domain borders

Once developed, cyberpower theory will focus on the unique aspects of cyber operations, both internally to the domain and across domain boundaries, from the strategic down to the tactical level. It will link cyber operations to national security objectives through physical effects, cognitive perception, and moral interpretations

[25] Winton discusses the requirements for a complete airpower theory in Winton, "A Black Hole in the Wild Blue Yonder: The Need for a Comprehensive Theory of Air Power," 42. This discussion serves as the inspiration for the next few paragraphs.
[26] This four-category formulation is also identified by Winton: ibid.

consistent with national objectives, culture, and societal limitations. A cyber theory will also address the effect of cyberpower operations within the domain on governmental, commercial, and private use of the medium. Theory must also clearly delineate the cyber domain within the information environment and discuss its role in the collection, processing, and dissemination of information during peacetime and war. Most importantly, as reflected in the theories analyzed above, a cyber theory must discuss the peacetime requirement to develop cyberpower for use across the spectrum of war, from peacetime operations through low-level hostilities and all the way up to operations during traditional open warfare. The preceding chapters provide insight into the ways a cyber theory will meet these requirements, making this study a source for future cyber theory development.

Closing

> "Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon. Do not get me wrong. There are genuine experts, and most of us know about patches, insider threats, worms, Trojans, WikiLeaks, and Stuxnet. But few of us (myself included) have created the broad structural framework within which to comfortably and confidently place these varied phenomena. And that matters. I have sat in very small group meetings in Washington, been briefed on an operational need and an operational solution, and been unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of any decision we might make."[27] – General Michael Hayden 2011

The rapid expansion of cyberspace over the last few decades has changed how nations, cultures, and economies interact. Cyberspace increasingly permeates the tools governments, corporations, and individuals use every day. Growing awareness of this permeation and the domain's importance has increasingly led to calls for action, both to

[27] Michael V. Hayden, General, USAF, Retired, "The Future of Things "Cyber"," *Strategic Studies Quarterly* 5, no. 1 (2011): 3.

secure the domain and harness it in pursuit of national security goals. Unfortunately, without a guiding theory for cyberpower development, these calls for action either go unanswered or result in measures addressing immediate concerns without sufficient consideration of long-term cyber strategy.

Establishing a baseline for cyberpower theory and beginning the process of building it are necessary first steps. This study has identified that extant theories of maritime and aerial domain power can serve as the baseline from which to begin. For example, knowledge that control over chokepoints within the cyber domain is similar to the use of chokepoints during the exercise of maritime power provides a point of reference for creating shared conceptual models. Drawing additional examples from the discussions in Chapter 7, theorists will identify relevant domain theory applications and transfer them directly into the cyber domain. As we identified during this study, borrowing from extant theory is the same process applied by theorists creating maritime and air power theories – a tested and successful technique. What we have done here is create the starting point from which a long intellectual journey begins. However, this starting point is the foundation – hopefully a sturdy one – on which to build and refine cyber theory.

Appendix I

Appendix I

Maritime Domain Elements of Analysis

	Mahan	Corbett
1	Domain power depends on the creation and maintenance of both strong military and commercial use of the domain.	Domain power is a subset of integrated national power; political considerations to strengthen all elements of the DIME during times of both peace and war guide its use.
2	International trade via a domain is critical to a nation's development of domain power.	Command of a common lies in control of the lines of communication within it, either temporarily or permanently.
3	Lines of communication develop between commercial partners and become sources of strength and vulnerability within the domain.	Lines of communications are the vital pathways by which nations sustain their life and pursue national power (whole of DIME) in a global common.
4	Defense of commercial lines of communication requires and encourages the development of strong military capabilities.	Offensive operations wrest control from an adversary; they are the purview of the stronger force but are complicated by an adversary's option to deny engagement, thus keeping command in doubt.
5	During conflict, exercising domain power guarantees one's access to lines of communication in the domain while denying access to one's foe.	Defensive operations deny an adversary its intended purpose and are inherently the stronger form of action, often the option of the weaker force.
6	Destruction of enemy capability to challenge one's access to the domain is critical and achieved through decisive action against enemy forces.	Isolation allows a nation controlling the common to dictate a conflict's degree of escalation to match its political goals.
7	A nation must not divide its forces; concentration of force in the domain is necessary to destroy the enemy when the opportunity appears.	Being uncommanded is the natural state of global common – weaker forces often retain the ability to disrupt and locally challenge stronger forces for short durations.
8	Geographical position affects a nation's domain power potential.	Control of geopolitically strategic points where lines of communication converge, such as geographic chokepoints, are critical to gaining and exercising command of the domain.
9	Physical conformation (including natural conditions and climate) determines a nation's ability to access a domain and its incentive to develop domain power.	Denying an adversary the use of a domain can occur through either prevention of entry or harassment while transiting lines of communication.
10	Extent of territory determines a nation's ability to gain and maintain exposure to the domain.	To control a common, a nation must be capable of both gaining and exercising command of the domain – exercising command is the more critical of the two.
11	The number of population engaged in domain pursuits determines potential and the size of reserves.	Forces exercising control of a common must be capable of rapidly massing to engage in decisive action when and where control is threatened.
12	The character of the people as well as their cultural and societal predispositions affects domain development.	
13	The character of the government (and national institutions) determines how effectively domain power is developed and used.	

Appendix II

Appendix II

Air Domain Elements of Analysis

	Douhet	Mitchell	Seversky
1	Governments must encourage the development of commercial infrastructure and industry to develop national economic and military power.	Use of domain power should focus on defeating an adversary's will and capability to engage in conflict.	Gaining command of a domain and projecting power across domain boundaries require different forces.
2	Commercial and military interests in the global common overlap, requiring national-level organization for military and civil development in a coordinated and efficient manner.	Power in a technology-dependent domain depends on military and commercial development of personnel, infrastructure, technology, and industry.	Gaining control of the domain requires denial of the enemy's ability to enter the domain or complete destruction of his domain forces.
3	The ability to bypass fielded forces makes an enemy's will and capability to resist the strategic objective.	Development of personnel to exploit a domain is as important as the technology to enter the domain.	Enduring control of the domain is only possible through attrition and eventual destruction of the enemy's domain-centric forces.
4	Command of a domain from which effects are projected provides protection and allows one to directly target an adversary's means, and will to resist	The willingness of a government to use incentives for stimulation of commercial industry and infrastructure determines domain power.	Domain control consists of two phases: gaining control of the domain followed by projection of power from the domain.
5	In the absence of geography, chokepoints develop at access points to the domain.	Commercial development of technology is faster and more efficient than government development.	Cross-domain power projection allows control or blockade of lines of communication in other domains.
6	Efficiently targeting an adversary's domain power requires targeting domain access points, not units currently within the domain or along lines of communication.	Central guidance ensures that military and civil development occurs in a coordinated manner (Department of Defense, national civil administration).	New domain theory must simultaneously educate and advocate for domain power development.
7	The elimination of geography as a factor in movement and increased speeds of travel reduce the warning and reaction time nations have to respond to attacks.	Military and civil organization for exploitation of a domain must focus solely on that domain (separate service).	Commercial technology development is superior to government development.
8	Increased mobility makes defense of a global common resource-prohibitive.	Geography determines domain power potential through access to resource, creation of incentives, development of national character, and force structure requirements.	Transportability of technology means late adaptors can jump ahead of those with locked production of equipment.
9	The relative strength of domain power at the onset of conflict is a significant determinant of which nation will gain command of the domain; once	Absent geography, chokepoints occur at points of entry into a domain.	Speed and flexibility reduce the importance of geography.

Appendix II

	reduced, it cannot be rebuilt quickly.		
10	Forces in a global common are primarily offensive in nature.	Recreation of domain power during a conflict is not possible due to destruction of industrial means and long lead times.	Efficient use of national resources means development of forces with the longest range and greatest striking power possible.
11	Given the offensive nature of forces, they should consist of combat power to deny enemy use of the domain and reconnaissance.	Speed, flexibility, and the vastness of a common complicate development of robust defenses, making highly mobile forces offensive in nature.	Government involvement to set commercial standards is necessary to coordinate commercial/government use of the domain.
12	Forces designed for combat in a global common must exist as a fully trained "capability in being" before conflict erupts.	Defense of vital points in common is necessary to ensure access/use of the domain (points of domain access and vital national infrastructure).	National strategic forces are those with the greatest range and power.
13	Bypassing fielded forces allows direct targeting of all means of resistance, including a population's will to endure bombardment.	The lack of warning before an attack means that forces in the domain must constantly be prepared to defend vital points.	In technology-driven competition, marginal quality advantages are relatively superior to quantity.
14	The lack of predictable targets and set lines of communication makes defense of global common is resource-prohibitive.	The ability to influence across domain boundaries decreases the importance of traditional defenses such as distance and reaction time.	Forces and personnel must be specialized to fit not only a nation's general strategy but also the tactical problems of a specific campaign.
15	Resources expended on creating defensive capabilities divert resources from the development of combat power and the ability to gain command of the domain.	Control of a common can be temporary or permanent in nature, depending on operational objectives: Control is necessary for effective projection of power to another domain.	Destruction of an enemy's means to resist is more effective than directly targeting his morale and population directly.
16	Destruction of the enemy's capability to use a domain is necessary to gain command – a good offense is the best defense.	One type of force is incapable of fully exploiting a domain: Both specialized counterforce and attack units are required.	The principle of unity of command applies to all domains.
17	Efficacy of national power development across all domains requires coordination across national interests	Gaining domain control requires elimination of the enemy's ability to enter the domain.	Creation of a separate domain-centric force is necessary for proper domain power development.
18	Full development of domain power requires an independent organization within the military command structure to provide equal footing between all domains.	As long as a common is uncontrolled, any point within the domain or along its seams is vulnerable to attack.	The projection of power across domain boundaries alleviates the need to develop dominant domain-centric forces in all domains.
19		Control of the domain allows the controlling force to influence use of other domains across domain	Blockade of internal lines of communication is possible because overlying domains mean overlying boundaries.

		boundaries as desired.	

Appendix III

Appendix III	
1	**The use of domain power to exercise domain control ensures freedom of action within the domain while denying the adversary freedom of action. Cross-domain power can exercise cross-domain control.**
	Mahan
5	During conflict, exercising domain power guarantees one's access to lines of communication in the domain while denying access to one's foe.
	Corbett
2	Command of a common lies in control of the lines of communication within it, either temporarily or permanently.
3	Lines of communications are the vital pathways by which nations sustain their life and pursue national power (whole of DIME) in a global common.
6	Isolation allows a nation controlling the common to dictate a conflict's degree of escalation to match its political goals.
	Douhet
	Mitchell
9	Absent geography, chokepoints occur at points of entry into a domain.
17	Gaining domain control requires elimination of the enemy's ability to enter the domain.
18	As long as a common is uncontrolled, any point within the domain or along its seams is vulnerable to attack.
19	Control of the domain allows the controlling force to influence use of other domains across domain boundaries as desired.
	Seversky
18	The projection of power across domain boundaries alleviates the need to develop dominant domain-centric forces in all domains.

2	**The objective of exercising domain power in a common is to affect an enemy's will and means to resist.**
	Mahan
	Corbett
3	Lines of communications are the vital pathways by which nations sustain their life and pursue national power (whole of DIME) in a global common.
6	Isolation allows a nation controlling the common to dictate a conflict's degree of escalation to match its political goals.
	Douhet
13	Bypassing fielded forces allows direct targeting of all means of resistance, including a population's will to endure bombardment.
	Mitchell
1	Use of domain power should focus on defeating an adversary's will and capability to engage in conflict.
	Seversky

Appendix III

15	Destruction of an enemy's means to resist is more effective than directly targeting his morale and population directly.

Appendix III

3	**Governments must emphasize strategic development of domain power through incentives, coordination of military/civilian development and treaties as part of its long-term national strategy.**
	Mahan
13	The character of the government (and national institutions) determines how effectively domain power is developed and used.
	Corbett
	Douhet
2	Commercial and military interests in the global common overlap, requiring national-level organization for military and civil development in a coordinated and efficient manner.
9	The relative strength of domain power at the onset of conflict is a significant determinant of which nation will gain command of the domain; once reduced, it cannot be rebuilt quickly.
12	Forces designed for combat in a global common must exist as a fully trained "capability in being" before conflict erupts.
17	Efficacy of national power development across all domains requires coordination across national interests.
	Mitchell
2	Power in a technology-dependent domain depends on military and commercial development of personnel, infrastructure, technology, and industry.
4	The willingness of a government to use incentives for stimulation of commercial industry and infrastructure determines domain power.
6	Central guidance ensures that military and civil development occurs in a coordinated manner (Department of Defense, national civil administration).
10	Recreation of domain power during a conflict is not possible due to destruction of industrial means and long lead times.
	Seversky
11	Government involvement to set commercial standards is necessary to coordinate commercial/government use of the domain.

Appendix III

4	Domain power development is a subset of overall national power across the DIME.
	Mahan
	Corbett
1	Domain power is a subset of integrated national power; political considerations to strengthen all elements of the DIME during times of both peace and war guide its use.
	Douhet
2	Commercial and military interests in the global common overlap, requiring national-level organization for military and civil development in a coordinated and efficient manner.
17	Efficacy of national power development across all domains requires coordination across national interests
	Mitchell
6	Central guidance ensures that military and civil development occurs in a coordinated manner (Department of Defense, national civil administration).
	Seversky
10	Efficient use of national resources means development of forces with the longest range and greatest striking power possible.

Appendix III

5	**Simultaneous military and commercial domain development are necessary to become an enduring domain power.**
	Mahan
1	Domain power depends on the creation and maintenance of both strong military and commercial use of the domain.
2	International trade via a domain is critical to a nation's development of domain power.
3	Lines of communication develop between commercial partners and become sources of strength and vulnerability within the domain.
4	Defense of commercial lines of communication requires and encourages the development of strong military capabilities.
	Corbett
	Douhet
1	Governments must encourage the development of commercial infrastructure and industry to develop national economic and military power.
	Mitchell
2	Power in a technology-dependent domain depends on military and commercial development of personnel, infrastructure, technology, and industry.
4	The willingness of a government to use incentives for stimulation of commercial industry and infrastructure determines domain power.
5	Commercial development of technology is faster and more efficient than government development.
	Seversky
7	Commercial technology development is superior to government development.
11	Government involvement to set commercial standards is necessary to coordinate commercial/government use of the domain.

Appendix III

6	Creation of domain power must occur before a crisis or conflict begins.
	Mahan
13	The character of the government (and national institutions) determines how effectively domain power is developed and used.
	Corbett
1	Domain power is a subset of integrated national power; political considerations to strengthen all elements of the DIME during times of both peace and war guide its use.
	Douhet
4	Command of a domain from which effects are projected provides protection and allows one to directly target an adversary's means, and will to resist
10	Forces in a global common are primarily offensive in nature.
	Mitchell
1	Use of domain power should focus on defeating an adversary's will and capability to engage in conflict.
10	Recreation of domain power during a conflict is not possible due to destruction of industrial means and long lead times.
13	The lack of warning before an attack means that forces in the domain must constantly be prepared to defend vital points.
	Seversky
8	Transportability of technology means late adaptors can jump ahead of those with locked production of equipment.
14	Forces and personnel must be specialized to fit not only a nation's general strategy but also the tactical problems of a specific campaign.
15	Destruction of an enemy's means to resist is more effective than directly targeting his morale and population directly.

Appendix III

7	**Control over chokepoints where lines of communication converge or terminates is the most efficient means of exercising domain control and leads to enduring domain control.**
	Mahan
3	Lines of communication develop between commercial partners and become sources of strength and vulnerability within the domain.
4	Defense of commercial lines of communication requires and encourages the development of strong military capabilities.
8	Geographical position affects a nation's domain power potential.
9	Physical conformation (including natural conditions and climate) determines a nation's ability to access a domain and its incentive to develop domain power.
	Corbett
2	Command of a common lies in control of the lines of communication within it, either temporarily or permanently.
3	Lines of communications are the vital pathways by which nations sustain their life and pursue national power (whole of DIME) in a global common.
8	Control of geopolitically strategic points where lines of communication converge, such as geographic chokepoints, are critical to gaining and exercising command of the domain.
	Douhet
5	In the absence of geography, chokepoints develop at access points to the domain.
6	Efficiently targeting an adversary's domain power requires targeting domain access points, not units currently within the domain or along lines of communication.
	Mitchell
9	Absent geography, chokepoints occur at points of entry into a domain.
12	Defense of vital points in common is necessary to ensure access/use of the domain (points of domain access and vital national infrastructure).
	Seversky
2	Gaining control of the domain requires denial of the enemy's ability to enter the domain or complete destruction of his domain forces.

Appendix III

8	**The exercise of domain power is a multi-step process: first gaining command of the domain and then exercising command of the domain (to included projection of power across domain boundaries).**
	Mahan
	Corbett
10	To control a common, a nation must be capable of both gaining and exercising command of the domain – exercising command is the more critical of the two.
	Douhet
	Mitchell
14	The ability to influence across domain boundaries decreases the importance of traditional defenses such as distance and reaction time.
15	Control of a common can be temporary or permanent in nature, depending on operational objectives: Control is necessary for effective projection of power to another domain.
16	One type of force is incapable of fully exploiting a domain: Both specialized counterforce and attack units are required.
18	As long as a common is uncontrolled, any point within the domain or along its seams is vulnerable to attack.
19	Control of the domain allows the controlling force to influence use of other domains across domain boundaries as desired.
	Seversky
1	Gaining command of a domain and projecting power across domain boundaries require different forces.
4	Domain control consists of two phases: gaining control of the domain followed by projection of power from the domain.

Appendix III

9	**Gaining domain control means eliminating the enemy's ability to enter the domain or use its lines of communication.**
	Mahan
6	Destruction of enemy capability to challenge one's access to the domain is critical and achieved through decisive action against enemy forces.
	Corbett
6	Isolation allows a nation controlling the common to dictate a conflict's degree of escalation to match its political goals.
9	Denying an adversary the use of a domain can occur through either prevention of entry or harassment while transiting lines of communication.
	Douhet
9	The relative strength of domain power at the onset of conflict is a significant determinant of which nation will gain command of the domain; once reduced, it cannot be rebuilt quickly.
11	Given the offensive nature of forces, they should consist of combat power to deny enemy use of the domain and reconnaissance.
	Mitchell
9	Absent geography, chokepoints occur at points of entry into a domain.
10	Recreation of domain power during a conflict is not possible due to destruction of industrial means and long lead times.
17	Gaining domain control requires elimination of the enemy's ability to enter the domain.
18	As long as a common is uncontrolled, any point within the domain or along its seams is vulnerable to attack.
	Seversky
1	Gaining command of a domain and projecting power across domain boundaries require different forces.
2	Gaining control of the domain requires denial of the enemy's ability to enter the domain or complete destruction of his domain forces.
3	Enduring control of the domain is only possible through attrition and eventual destruction of the enemy's domain-centric forces.

Appendix III

10	**A nation's geography affects its domain power potential, vulnerability to attack from the domain, influence over lines of communication, and incentive to develop domain power.**
	Mahan
8	Geographical position affects a nation's domain power potential.
9	Physical conformation (including natural conditions and climate) determines a nation's ability to access a domain and its incentive to develop domain power.
10	Extent of territory determines a nation's ability to gain and maintain exposure to the domain.
	Corbett
8	Control of geopolitically strategic points where lines of communication converge, such as geographic chokepoints, are critical to gaining and exercising command of the domain.
	Douhet
	Mitchell
8	Geography determines domain power potential through access to resource, creation of incentives, development of national character, and force structure requirements.
	Seversky

11	**A nation's population affects domain power through the creation of domestic reserves of both personnel and knowledge available in times of need.**
	Mahan
11	The number of population engaged in domain pursuits determines potential and the size of reserves.
12	The character of the people as well as their cultural and societal predispositions affects domain development.
	Corbett
	Douhet
	Mitchell
2	Power in a technology-dependent domain depends on military and commercial development of personnel, infrastructure, technology, and industry.
3	Development of personnel to exploit a domain is as important as the technology to enter the domain.
	Seversky

Appendix III

Note: This is a domain-specific element. Discussion of the domain theories and contributing elements appears in Chapter 6.

12	**Domain power development requires the creation of domain-specific governmental institutions and cross-domain coordinating bodies.**
	Mahan
	Corbett
	Douhet
17	Efficacy of national power development across all domains requires coordination across national interests
18	Full development of domain power requires an independent organization within the military command structure to provide equal footing between all domains.
	Mitchell
6	Central guidance ensures that military and civil development occurs in a coordinated manner (Department of Defense, national civil administration).
7	Military and civil organization for exploitation of a domain must focus solely on that domain (separate service).
	Seversky
14	Forces and personnel must be specialized to fit not only a nation's general strategy but also the tactical problems of a specific campaign.
17	Creation of a separate domain-centric force is necessary for proper domain power development.

Appendix III

Note: This is an element of disagreement. Discussion of these contributing elements appears in Chapter 6.

13	**The state of domain technology determines the dominant character of domain forces.**
	Mahan
	Corbett
4	Offensive operations wrest control from an adversary; they are the purview of the stronger force but are complicated by an adversary's option to deny engagement, thus keeping command in doubt.
5	Defensive operations deny an adversary its intended purpose and are inherently the stronger form of action, often the option of the weaker force.
	Douhet
3	The ability to bypass fielded forces makes an enemy's will and capability to resist the strategic objective.
8	Increased mobility makes defense of a global common resource-prohibitive.
10	Forces in a global common are primarily offensive in nature.
15	Resources expended on creating defensive capabilities divert resources from the development of combat power and the ability to gain command of the domain.
16	Destruction of the enemy's capability to use a domain is necessary to gain command – a good offense is the best defense.
	Mitchell
11	Speed, flexibility, and the vastness of a common complicate development of robust defenses, making highly mobile forces offensive in nature.
14	The ability to influence across domain boundaries decreases the importance of traditional defenses such as distance and reaction time.
18	As long as a common is uncontrolled, any point within the domain or along its seams is vulnerable to attack.
	Seversky
9	Speed and flexibility reduce the importance of geography.
10	Efficient use of national resources means development of forces with the longest range and greatest striking power possible.

Appendix III

Note: This is an element of disagreement. Discussion of these contributing elements appears in Chapter 6.

14	**The pursuit of domain control is the primary function of domain-centric forces.**
	Mahan
	Corbett
	Douhet
13	Bypassing fielded forces allows direct targeting of all means of resistance, including a population's will to endure bombardment.
14	The lack of predictable targets and set lines of communication makes defense of global common is resource-prohibitive.
	Mitchell
1	Use of domain power should focus on defeating an adversary's will and capability to engage in conflict.
	Seversky

Appendix III

Note: This is an element of disagreement. Discussion of these contributing elements appears in Chapter 6.

15	Vital points exist as convergences of lines of communication.
	Mahan
6	Destruction of enemy capability to challenge one's access to the domain is critical and achieved through decisive action against enemy forces.
7	A nation must not divide its forces; concentration of force in the domain is necessary to destroy the enemy when the opportunity appears.
	Corbett
2	Command of a common lies in control of the lines of communication within it, either temporarily or permanently.
7	Being uncommanded are the natural states of global common – weaker forces retaining the ability to locally disrupt and challenge stronger forces for short durations.
9	Denying an adversary the use of a domain can occur through either prevention of entry or harassment while transiting lines of communication.
	Douhet
4	Command of a domain from which effects are projected provides protection and allows one to directly target an adversary's means, and will to resist
8	Increased mobility makes defense of a global common resource-prohibitive.
10	Forces in a global common are primarily offensive in nature.
11	Given the offensive nature of forces, they should consist of combat power to deny enemy use of the domain and reconnaissance.
15	Resources expended on creating defensive capabilities divert resources from the development of combat power and the ability to gain command of the domain.
	Mitchell
12	Defense of vital points in common is necessary to ensure access/use of the domain (points of domain access and vital national infrastructure).
15	Control of a common can be temporary or permanent in nature, depending on operational objectives: Control is necessary for effective projection of power to another domain.
17	Gaining domain control requires elimination of the enemy's ability to enter the domain.
18	As long as a common is uncontrolled, any point within the domain or along its seams is vulnerable to attack.
19	Control of the domain allows the controlling force to influence use of other domains across domain boundaries as desired.
	Seversky
2	Gaining control of the domain requires denial of the enemy's ability to enter the domain or complete destruction of his domain forces.
3	Enduring control of the domain is only possible through attrition and eventual destruction of the enemy's domain-centric forces.
4	Domain control consists of two phases: gaining control of the domain followed by projection of power from the domain.

Appendix III

Note: This is an element of disagreement. Discussion of these contributing elements appears in Chapter 6.

16	**The capability to project power across domain boundaries affects an adversary's will and ability to resist in other domains.**
	Mahan
	Corbett
	Douhet
3	The ability to bypass fielded forces makes an enemy's will and capability to resist the strategic objective.
4	Command of a domain from which effects are projected provides protection and allows one to directly target an adversary's means, and will to resist
13	Bypassing fielded forces allows direct targeting of all means of resistance, including a population's will to endure bombardment.
	Mitchell
1	Use of domain power should focus on defeating an adversary's will and capability to engage in conflict.
14	The ability to influence across domain boundaries decreases the importance of traditional defenses such as distance and reaction time.
18	As long as a common is uncontrolled, any point within the domain or along its seams is vulnerable to attack.
19	Control of the domain allows the controlling force to influence use of other domains across domain boundaries as desired.
	Seversky
1	Gaining command of a domain and projecting power across domain boundaries require different forces.
4	Domain control consists of two phases: gaining control of the domain followed by projection of power from the domain.
18	The projection of power across domain boundaries alleviates the need to develop dominant domain-centric forces in all domains.
19	Blockade of internal lines of communication is possible because overlying domains mean overlying boundaries.

Note: This is a unique element. Discussion of these contributing elements appears in Chapter 6.

17	**Rapidly changing, and highly dynamic technology makes creation of enduring domain power problematic.**
	Mahan
	Corbett
	Douhet
	Mitchell
	Seversky
8	Transportability of technology means late adaptors can jump ahead of those with locked production of equipment.
13	In technology-driven competition, marginal quality advantages are relatively superior to quantity.

Appendix III

Note: This is a unique element. Discussion of these contributing elements appears in Chapter 6.

18	International trade is critical to creating domain power.
	Mahan
2	International trade via a domain is critical to a nation's development of domain power.
3	Lines of communication develop between commercial partners and become sources of strength and vulnerability within the domain.
	Corbett
	Douhet
	Mitchell
	Seversky

Appendix IV

Appendix IV

	Common Elements of Domain Power
1	The use of domain power to exercise domain control ensures freedom of action within the domain while denying the adversary freedom of action. Cross-domain power can exercise cross-domain control.
2	The objective of exercising domain power in a common is to affect an enemy's will and means to resist.
3	Governments must emphasize strategic development of domain power through incentives, coordination of military/civilian development and treaties as part of its long-term national strategy.
4	Domain power development is a subset of overall national power across the DIME.
5	Simultaneous military and commercial domain development are necessary to become an enduring domain power.
6	Creation of domain power must occur before a crisis or conflict begins.
7	Control over chokepoints where lines of communication converge or terminates is the most efficient means of exercising domain control and leads to enduring domain control.
8	The exercise of domain power is a multi-step process: first gaining command of the domain and then exercising command of the domain (to included projection of power across domain boundaries).
9	Gaining domain control means eliminating the enemy's ability to enter the domain or use its lines of communication.
10	A nation's geography affects its domain power potential, vulnerability to attack from the domain, influence over lines of communication, and incentive to develop domain power.
11	A nation's population affects domain power through the creation of domestic reserves of both personnel and knowledge available in times of need.
12	Domain power development requires the creation of domain-specific governmental institutions and cross-domain coordinating bodies.
13	The state of domain technology determines the dominant character of domain forces.
14	The pursuit of domain control is the primary function of domain-centric forces.
15	Vital points exist as convergences of lines of communication.
16	The capability to project power across domain boundaries affects an adversary's will and ability to resist in other domains.
17	Rapidly changing, and highly dynamic technology makes creation of enduring domain power problematic.
18	International trade is critical to creating domain power.

Bibliography

Bibliography

Adee, Sally. "The Hunt for the Kill Switch." *ieee Spectrum* (2008), http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0.

Alberts, David S., John J. Garstka, Richard E. Hayes, and David A. Signori. *Understanding Information Age Warfare*, CCRP publication series. Washington, DC: DOD, 2001.

Baker, Meredith Attwell. "Hands Off Tomorrow's Internet." *The Washington Post* (2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/12/20/AR2010122003901.html?wpisrc=nl_opinions.

Baldor, Lolita. "Government-backed Hacker Teams do Most China-based Data Theft." *USA Today* (2011), http://www.usatoday.com/tech/news/story/2011-12-12/chinese-hackers/51830840/1.

Ballenstedt, Brittany. Expert Flags Flaw in Cyber Workforce Plan. In Wired Workplace, edited by nextgov, Web blog regarding cyber issues at the government level, 2011, http://wiredworkplace.nextgov.com/2011/08/expert_flags_flaw_in_cyber_workforce_plan-print.php.

Barrett, Major General Mark, Dick Bedford, Elizabeth Skinner, and Eva Vergles. "Assured Access to the Global Commons." edited by Supreme Allied Command Transformation. Norfolk, VA: North Atlantic Treaty Organization, 2011.

Billo, Charles, and Welton Chang. "Cyber Warfare and Analysis of the Means and Motivations of Selected Nation States." edited by Technology Institute for Security, and Society, 142. Hanover, NH: Dartmouth College, 2004.

Bradford, James C. *Admirals of the New Steel Navy: Makers of the American Naval Tradition, 1880-1930*, Makers of the American Naval Tradition. Annapolis, MD: Naval Institute Press, 1990.

Brimley, S. "Promoting Security in Common Domains." *Washington Quarterly* 33, no. 3 (2010): 119-32.

Brito, Jerry, and Tate Watkins. "The Cybersecurity-Industrial Complex: The Feds Erect a Bureaucracy to Combat a Questionable Threat." *Reason* 43, no. 4 (2011): 7.

Burlingame, Roger. *General Billy Mitchell, Champion of Air Defense*, They Made America. New York, NY: McGraw-Hill, 1952.

Bush Administration. "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." edited by Executive Office of the President, 6. Washington, DC, 2003.

Cartwright, James E. General, USMC. "AFA's 2007 Air Warfare Symposium Transcripts." AFA, http://www.afa.org/events/AWS/2007/post_Orlando/scripts/cartwright.asp.

Caton, Jeffrey. The Future of National Security in Cyberspace: Are We Leading the Target? In Dime Blog, 2010, http://www.carlisle.army.mil/DIME/blog/article.cfm?blog=dime&article=135.

Clark, David D. "Characterizing Cyberspace: Past, Present and Future." 18. Cambridge, MA: MIT CSAIL, 2010.

Bibliography

Clark, Richard. "China's Cyberassault on America." *The Wall Street Journal* (2011), http://online.wsj.com/article/SB10001424052702304259304576373391101828876.html?mod=wsj_share_facebook.

———. "Software Power: Cyber Warfare is the Risky New Frontline." Harvard Kennedy School, http://belfercenter.ksg.harvard.edu/power/2011/02/07/software-power-cyber-warfare-is-the-risky-new-frontline/.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat To National Security And What To Do About It*. 1st ed. New York, NY: ECCO, 2010.

Clausewitz, Carl von. *On War*. Translated by Peter Paret and Michael Howard. Edited by Peter Paret and Michael Howard. Princeton, NJ: Princeton University Press, 1976.

Clodfelter, Mark A., Lt Col. "Molding Airpower Convictions: Development and Legacy of William Mitchell's Strategic Thought." In *The Paths of Heaven: The Evolution of Airpower Theory*, edited by Col. Phillip S. Meilinger and School of Advanced Airpower Studies (US), 79-114. Maxwell AFB, AL: Air University Press, 1997.

Committee on Detering Cyberattacks. "Letter Report from the Committee on Deterring Cyberattacks: Informing Strategies and Develping Options for U.S. Policy." edited by National Research Council, 35. Washington, DC: National Academy of Sciences, 2010.

"Convention on International Civil Aviation." 1944.

Cooke, James J. *Billy Mitchell*, (The Art of War). Boulder, CO: Lynne Rienner, 2002.

Corbett, Sir Julian Stafford. *Some Principles of Maritime Strategy*, Classics of Sea Power. Annapolis, MD: Naval Institute Press, 1988.

"Cyber 2020 Asserting Global Leadership in the Cyber Domain." 24. McLean, VA: Booz Allen Hamilton, 2010.

De Seversky, Alexander P. *Victory Through Air Power*. New York, NY: Simon and Schuster, 1942.

De Seversky, Alexander Procofieff. *Air Power: Key to Survival*. New York, NY: Simon and Schuster, 1950.

"Defending the Networks: The NATO Policy on Cyber Defence." edited by NATO Public Diplomacy Division. Brussels, BE: North AtlanticTreaty Organization, 2011.

Defense, U.S. Department of. "U.S. Cyber Command Fact Sheet." edited by U.S. Strategic Command, 1: U.S. Department of Defense Office of Public Affairs, 2010.

Denmark, Abraham M., and James Mulvenon, eds. *Contested Commons: The Future of American Power in a Multipolar World*: Center for a New American Security, 2010.

Dictionary, Merriam-Webster. "Domain, n." Merriam-Webster, Incorporated, http://www.merriam-webster.com/dictionary/domain.

———. "Freedom of navigation." Merriam-Webster, Incorporated, http://www.merriam-webster.com/dictionary/freedom%20of%20navigation.

Dolman, Everett C. *Astropolitik: Classical Geopolitics in the Space Age*, Cass series--strategy and history. Portland, OR: Frank Cass, 2002.

Douhet, Giulio. *The Command of the Air*, World Affairs: national and international viewpoints. North Stratford NH: Ayer Company Publishers, Inc, 1942. Reprint, 1999.

Bibliography

Dunlap, Charles Jr., Major General, USAF Retired. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly* 5, no. 1 (2011): 81-99.

England, Gordon. "The Definition of Cyberspace." Washington, DC: Department of Defense, 2008.

Franzese, Patrick W., Lt Col, USAF. "Sovereignty in Cyberspace: Can it Exist?" *Air Force Law Review* 64, (2009): 1-42.

Fulghum, David A., Paul McLeary, and Bill Sweetman. "Cyber Strategy More of a Wish Than a Plan." *Aviation Week & Space Technology* (2011), http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/awst/2011/08/01/AW_08_01_2011_p28-352024.xml&headline=Cyber%20Strategy%20More%20Of%20A%20Wish%20Than%20A%20Plan&next=20.

Gibson, William. "Burning Chrome." *Omni*, 1 July 1982, 72-77.

———. *Neuromancer*, Ace Science Fiction. New York: Ace Books, 1984.

Glaser, Barney G. *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory*. Mill Valley, Calif.: Sociology Press, 1978.

Gorman, Siobhan, and Julian E. Barnes. "Cyber Combat: Act of War." *The Wall Street Journal* (2011), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html#ixzz1O2urKzzR.

Grauman, Brigid. "Cyber-Security: The Vexed Question of Global Rules." 108. Brussels, BE: Security & Defense Agenda, 2012.

Gross, Michael Joseph. "A Declaration of Cyber-War." *Vanity Fair* (2011), http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

Handel, Michael I. *Masters of War: Classical Strategic Thought*. 3rd rev. and expanded ed. London ; Portland, OR: F. Cass, 2001.

Hattendorf, John B. "The Uses of Maritime History in and for the Navy." *Naval War College Review* Spring, no. 56 (2003): 13-39.

Hayden, Michael V., General, USAF, Retired. "The Future of Things "Cyber"." *Strategic Studies Quarterly* 5, no. 1 (2011): 5.

HiIbernia Atlantic. "Hibernia Atlantic to Construct the Lowest Latency TransAtlantic Submarine Fiber Optic Cable Network from New York to London " *Disaster Recovery Journal* (2010), http://www.drj.com/industry/press-releases/hibernia-atlantic-to-construct-the-lowest-latency-transatlantic-submarine-fiber-optic-cable-network-from-new-york-to-london.html.

"History: NWC History." U.S. Naval War College, http://www.usnwc.edu/About/History.aspx.

Holmes, Allan. "ASF 2011: Cyber Security." In *Aspen Security Forum*, 73:39. USA The Aspen Institute, 2011.

Hurley, Alfred F. *Billy Mitchell, Crusader for Air Power*. Bloomington, IN: Indiana University Press, 1975.

Kaplan, Abraham. *The Conduct of Inquiry; Methodology for Behavioral Science*, Chandler publications in anthropology and sociology. San Francisco, CA: Chandler Pub. Co., 1964.

Bibliography

Kassner, Michael. "Deep Packet Inspection: What you Should Know." ZDNet, http://www.zdnet.co.uk/news/it-strategy/2008/07/31/deep-packet-inspection-what-you-should-know-39454822/.

Kelley, Olen L., Colonel. "Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative." Masters Thesis, U.S. Army War College, 2008.

Klein, John J. "Corbett in Orbit: A Maritime Model for Strategic Space Theory." *Naval War College Review* 57, no. 1 (2004): 59-74.

Kramer, Franklin D. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 3-23. Washington, DC: Potomac Books, 2009.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. *Cyberpower and National Security*. 1st ed. Washington, DC: Potomac Books, 2009.

Kuehl, Daniel T. "CYBERSPACE: Its Place in National Security." In *Cyber Power: The Quest for Common Ground*. Maxwell AFB, AL: Verbal presentation to conference panel 27 October, 2011.

———. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 25-42. Washington, DC: Potomac Books, 2009.

Lakatos, Imre. "Falsification and the Methodology of Scientific Research Programmess." In *Criticism and the Growth of Knowledge*, edited by Imre Lakatos and Alan Musgrave, 91-124. Cambridge Eng.: Cambridge University Press, 1970.

Leiner, Barry M., Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff. "A Brief History of the Internet." http://www.isoc.org/internet/history/brief.shtml.

Lewis, James Andrew. "Neither Mahan nor Mitchell: National Security Space and Spacepower, 1945-2000." In *Toward a Theory of Spacepower: Selected Essays*, edited by Charles D. Lutes, Peter L. Hays, Vincent A. Manzo, Lisa M. Yambrick and M. Elaine Bunn, 277-99. Washington, DC: National Defense University Press, 2011.

Livezey, William Edmund. *Mahan on Sea Power*. Norman, OK: University of Oklahoma Press, 1947.

Mahan, A. T. *From Sail to Steam; Recollections of Naval Life*. New York, NY: Harper & brothers, 1907.

Mahan, Alfred Thayer. *The Influence of Sea Power Upon History, 1660-1783*. New York, NY: Dover Publications, 1987.

Martel, William C. *Victory in War: Foundations of Modern Strategy*. Rev. and expanded ed. New York, NY: Cambridge University Press, 2011.

McKee, Kandice. "A Review of Frequently Used Cyber Analogies." Smithfield, VA: National Security Cyberspace Institute, 2011.

Meilinger, Col Phillip S., USAF, Retired. *Airmen and Air Theory: A Review of Sources*. Maxwell Air Force Base, AL: Air University Press, 2001.

———. *Airwar: Theory and Practice*, Cass series – studies in air power. Portland, OR: Frank Cass, 2003.

———, ed. *The Paths of Heaven: The Evolution of Airpower Theory*. Maxwell AFB, AL: Air University Press, 1997.

Bibliography

Mesic, Richard, Myron Hura, Martin C. Libicki, Anthony M. Packard, and Lynn M. Scott. "Air Force Cyber Command (Provisional) Decision Support." edited by Rand Corporation. Santa Monica, CA: RAND Corporation, 2010.

Mill, John Stuart. "A System of Logic, Ratiocinative and Inductive: Being a Connected View of the Principles of Evidence, and Methods of Scientific Investigation." London, UK: John W. Parker, 1843.

Miller, James N., Dr. "Statement of Dr. James N. Miller Principal Deputy Under Secretary of Defense for Policy." In *Hearing on the Department of Defense in Cyberspace and U.S. Cyber Command,*, edited by U.S. Congress (House of Representatives) Committee on Armed Services Subcommittee on Emerging Threats and Capabiliites. Washington, DC, 2011.

Miller, Robert A., and Daniel T. Kuehl. "Cyberspace and the "First Battle" in 21st-century War." *Defense Horizons* 68, (2009): 6.

Mitchell, William. *Our Air Force, the Keystone of National Defense*. New York, NY: E.P. Dutton & Company, 1921.

———. *Winged Defense: The Development and Possibilities of Modern Air Power, Economic and Military*. New York, NY: Dover, 1988.

Montalbano, Elizabeth. "DOD Website Sells Public On Cybersecurity Strategy." *Informationweek - Online*,no. 19383371 (2011), http://www.informationweek.com/news/government/security/231002588#.

Nakashima, Ellen. "An army of tech-savvy warriors has been fighting its battles in cyberspace." *The Washington Post*, 24 September 2010, A18.

———. "Pentagon is debating cyber-attacks." *The Washington Post*, 6 November 2010, A.1 and A.7.

Nathan Gardels. "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly." *New Perspectives Quarterly* 27, no. 2 (2010): 15-17.

"National Security Strategy of the United States 2010." edited by White House, 2010.

Nye, Joseph S. "Facing up to cyber security challenges." *Policy and Power* (2011), http://belfercenter.ksg.harvard.edu/power/2011/06/13/facing-up-to-cyber-security-challenges/.

Organization for Economic Co-operation and Development. "Global Commons Definition." (2011), http://unstats.un.org/unsd/environmentgl/gesform.asp?getitem=573.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Edited by National Research Council. Washington, DC: National Academies Press, 2009.

Pfaltzgraff, Robert L. Jr. "International Relations Theory and Spacepower." In *Toward a Theory of Spacepower: Selected Essays*, edited by Charles D. Lutes, Peter L. Hays, Vincent A. Manzo, Lisa M. Yambrick and M. Elaine Bunn, 37-56. Washington, DC: National Defense University Press, 2011.

Posen, Barry R. "Command of the Commons: The Military Foundation of U.S. Hegemony." *International Security* 28, no. 1 (2003): 5-46.

Potter, E. B., and Chester W. Nimitz, eds. *Sea Power; A Naval History*. Englewood Cliffs, NJ: Prentice-Hall, 1960.

Bibliography

Puleston, W. D. *Mahan; The Life and Work of Captain Alfred Thayer Mahan*. New Haven, CT: Yale University Press, 1939.

Ripp, Mason L. "General William Mitchell." Air University, 1965.

Rosenau, James N. *The Scientific Study of Foreign Policy*. Rev. and enl. ed. London: New York: F. Pinter; Nichols., 1980.

Schurman, D. M. *Julian S. Corbett, 1854-1922: Historian of British Maritime Policy from Drake to Jellicoe*, Royal Historical Society Studies in History Series. London, UK: Royal Historical Society, 1981.

Schwartz, Peter. "The Role of Architecture in Internet Defense." In *America's Cyber Future: Security and Posperity in the Information Age*, edited by Kristin M. Lord and Travis Sharp, 219-28. Washington, DC: Center for New American Security, 2011.

Seager, Robert. *Alfred Thayer Mahan: The Man and His Letters*. Annapolis, MD: Naval Institute Press, 1977.

Sechrist, Michael. *Cyberspace in Deep Water: Protecting the Arteries of the Internet by Creating an International Public-Private Partnership*. Cambridge, MA: John F. Kennedy School of Government, 2010.

Segal, Adam. "Cyberspace Governance: The Next Step, Policy Innovation Memorandum No. 2." 4: Council on Foreign Relations, 2011.

Sheldon, John B. "Deciphering Cyberpower: Strategic Purpose in Peace and War." *Strategic Studies Quarterly* 5, no. 2 (2011): 95-112.

Shiplett, Myra Howze, Wendy Russell, Anne M. Khademian, and Lenora Peters Gant. "A Well-educated Workforce: Vital Component of National and Economic Security." In *Economic Security: Neglected Dimenson of National Security?*, edited by Sheila R. Ronis, 83-97. Washington, DC: National Defense University Press, 2011.

Sigaud, Louis A. *Air Power and Unification: Douhet's Principles of Warfare and Their Application to the United States*. 1st ed. Harrisburg, PA: Military Service Pub. Co., 1949.

———. *Douhet and Aerial Warfare*. New York, NY: G. P. Putnam's Sons, 1941.

Singer, J. David. "The Level-of-Analysis Problem in International Relations." *World Politics* 14, no. 1 (1961): 77-92.

Singer, P.W., and Noah Shachtman. "The Wrong War." (2011), http://www.nextgov.com/nextgov/ng_20110815_3244.php.

Smith, Steve. "Review: Rosenau's Contribution." *Review of International Studies* 9, no. 2 (1983): 137-46.

Starr, Stuart H. "Toward a Prelimary Theory of Cyberpower." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 43-88. Washington, DC: Potomac Books, 2009.

STRATFOR. "A Report on China's Internet Traffic 'Hijacking'." *STRATFOR Global Intelligence* (2010).

Sturdevant, Rick W., Dr. "Cyberspace: An Etymological and Historical Odyssey." *High Frontier* 5, no. 3 (2009): 47-49.

Sumida, Jon. "Old Thoughts, New Problems: Mahan and the Consideration of Spacepower." In *Toward a Theory of Spacepower: Selected Essays*, edited by

Bibliography

Charles D. Lutes, Peter L. Hayes, Mincent A. Manzo, Lisa M. Yambrick and M. Elain Bunn, 4-18. Washington: National Defense University Press, 2011.

"Theory." In *Shorter Oxford English Dictionary*, 3233. Oxford, UK: Oxford University Press, 2007.

Thompson, J. J. *Tendencies of Recent Investigations in the Field of Physics*. London, UK: British Broadcasting Corp, 1930.

U.S. China Economic and Security Review Commission. "2010 Report to Congress of the U.S.-China Econiomic and Security Review Commission." edited by U.S. Congress. Washington DC: U.S. Government Printing Office, 2010.

U.S. Congress (House of Representatives), Committee on Armed Services, Subcommittee on Emerging Threats and Capabiliites. "Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates." edited by Government Accountability Office. Washington, DC: United States Government Accountability Office, 2011.

U.S. Cyber Command Public Affairs. "U.S. Cyber Command Fact Sheet." http://www.stratcom.mil/factsheets/cyber_command/.

U.S. Department of Defense, Department of the Navy. "The Commander's Handbook on the Law of Naval Operations." edited by US Naval War College President, International Law Department, 184. Washington, DC: Government Printing Office, 2007.

U.S. Department of Defense, Joint Chiefs of Staff. "Department of Defense Dictionary of Military Associated Terms Joint Publication 1-02." Wahington DC: Government Printing Office, 2010, as amended throught 15 October 2011.

———. "Doctrine for Joint Operations." Washington, DC.: Government Printing Office, 2001.

———. "Joint Operational Access Concept." 66. Washington, DC: Government Printing Office, 2012.

———. *Joint Operations*. Vol. 3-0, Joint Operations. Washington, DC: U.S Government Printing Office, 2011.

———. *Joint Operations*. 17 September 2006, Incorporating Change 2, 22 March 2010 ed. Vol. 3-0, Joint Operations. Washington, DC: U.S. Government Printing Office, 2010.

———. "The National Military Strategy for Cyberspace Operations." edited by Chairman Joint Chiefs of Staff. Washington, DC, 2006.

U.S. Department of Defense, Office of the Secretary of Defense. "Department of Defense Strategy for Operating in Cyberspace." 19. Washington, DC, 2011.

U.S. National Security Council. "The Comprehensive National Cybersecurity Initiative." Washington, DC, 2009.

U.S. National Security Telecommunications Advisory Committee. "Cybersecurity Collaboration Report." Washington, DC: Executive Office of the President, 2009.

U.S. President. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." 30. Washington, DC, 2011.

———. "National Security Strategy." Washington, DC, 2010.

———. *The National Strategy to Secure Cyberspace*. Washington, DC: Dept. of Homeland Security, 2003.

Bibliography

———. "Presidential Decision Directive 63: Protecting America's Critical Infrastructures." Washington, DC: White House, 1998.

U.S. President, Proclamation. "National Cybersecurity Awareness Month." 1. Washington, DC: Office of the Press Secretary, 2010.

United Nations. "United Nations Covention on the Law of the Sea." edited by Division for Ocean Affairs and the Law of the Sea, 202. New York, NY, 1982.

United Nations Statistics Division. "Global Commons Definition." (2011), http://unstats.un.org/unsd/environmentgl/gesform.asp?getitem=573.

Van Evera, Stephen. *Guide to Methods for Students of Political Science*. Ithaca: Cornell University Press, 1997.

White House. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." 76. Washington, DC, 2009.

Winton, Harold R. "A Black Hole in the Wild Blue Yonder: The Need for a Comprehensive Theory of Air Power." *Air Power History* Winter, no. 39 (1992): 32-42.

———. "An Imperfect Jewel: Military Theory and the Military Profession." In *Society for Military History Annual Meeting*. Bethesda, MD, 2004.

———. "On the Nature of Military Theory." In *Toward a Theory of Spacepower: Selected Essays*, edited by Charles D. Lutes, Peter L. Hayes, Mincent A. Manzo, Lisa M. Yambrick and M. Elain Bunn, 19-35. Washington, DC: National Defense University Press, 2011.

Wylie, J. C. *Military Strategy: A General Theory of Power Control*. New Brunswick, N.J.,: Rutgers University Press, 1967.