INFORMATION, UNDERSTANDING, AND INFLUENCE:

AN AGENCY THEORY STRATEGY FOR AIR BASE COMMUNICATIONS AND CYBERSPACE SUPPORT

BY

MAJOR MICHAEL T. MCDANIEL

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

MAY 2014

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information, Understanding, And Influence: An Agency Theory Strategy For Air Base Communications And Cyberspace Support	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **School Of Advaned Air And Space Studies,,Air University,,Maxwell Air Force Base,,AL**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This thesis seeks to answer the question: how should the Air Force posture itself to best provide responsive communications and cyberspace support to its air bases in a challenged environment? Airpower, from its early development through the sophisticated operations of today, demands reliable and responsive communications and cyberspace support capabilities. Today, the Air Force provides much of those capabilities through a centralized organizational structure operating the Air Force Network (AFNET).

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**106**	

APPROVAL

The undersigned certify that this thesis meets master's-level standards of research, argumentation, and expression.

_____

MICHAEL V. SMITH, Col, USAF (PhD) (Date)

_____

STEPHEN E. WRIGHT, PhD (Date)

DISCLAIMER

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

ABOUT THE AUTHOR

Major Michael T. McDaniel is a cyberspace operations officer in the United States Air Force. He holds a Bachelor of Science Degree in Electrical Engineering from Louisiana State University, a Master of Science in Telecommunications Management from the University of Maryland, University College, and a Master of Military Operational Art and Science from the Air Command Staff College. He received his commission through the Air Force Reserve Officer Training Corps program at Louisiana State University in 2000 and entered the Air Force as a communications and information officer in January of 2001. Major McDaniel has served in both deployable and base communications squadrons in addition to assignments with the White House Communications Agency, Defense Information Systems Agency, and the Air Staff. Following his assignment to the School of Advanced Air and Space Studies, Major McDaniel will assume command of the 92nd Information Operations Squadron at Joint Base San Antonio-Lackland, Texas.

ACKNOWLEDGEMENTS

This thesis would not have been possible without the encouragement, support, guidance, and advice of many remarkable people. First, the extraordinary group of officers in SAASS class XXIII made this year an incredible experience and one that I will treasure for a long, long time.

The dedication and commitment to the progress and success of its students is what sets the SAASS faculty apart. From the high standards, to the always-honest (and sometimes blunt) feedback, to the constant encouragement, the faculty helped the students get the absolute most out of this year. In particular, my thesis advisor, Colonel Michael V. "Coyote" Smith, was absolutely crucial to this effort. He always asked the right questions to help me ask the right questions and provided encouragement when it was needed the most. In addition, my reader, Dr. Stephen "Wilbur" Wright, taught me new ways to frame and approach tough problems. His careful edits also made this paper much better than it would have otherwise been.

Many of my fellow cyberspace operations officers, serving across the Air Force, influenced my thinking in years past and over the course of writing this thesis. From mentors to colleagues, I am indebted deeply to the many who took time out of their busy schedules to answer questions and review portions of this work. Mr. Warren Nearey, historian at the Air Force Network Integration Center, also provided critical assistance in building much of the history chapter in the thesis. While the collective efforts of these individuals made this thesis stronger, any shortcomings, mistakes, or errors are mine and mine alone.

Finally and most importantly, I want to thank my amazing wife and our two incredible sons, who put up with the many, many hours of me being there, without really "being there." I am truly blessed to have you in my life and I thank God for that blessing everyday. You deserve more than my humble thank you and I love you more than you will ever know.

ABSTRACT

This thesis seeks to answer the question: how should the Air Force posture itself to best provide responsive communications and cyberspace support to its air bases in a challenged environment? Airpower, from its early development through the sophisticated operations of today, demands reliable and responsive communications and cyberspace support capabilities. Today, the Air Force provides much of those capabilities through a centralized organizational structure operating the Air Force Network (AFNET).

This thesis examines the history of communications in support of airpower, from its humble beginnings in the US Army Air Corps to its role in modern day cyberspace operations. It focuses on the service's organizational approaches, the role of communications in support of air operations, and its ability to integrate new technology and capabilities into the force.

The thesis then uses agency theory to explain the influences that shape the past and present communications and cyberspace support organizations. Next, it introduces a strategy based on this analysis to bring information, understanding, and influence from supported air bases into the AFNET organizational structure. The thesis then tests and demonstrates the strategy under normal and stressed operational conditions to evaluate its performance.

The analysis concludes that airpower communications and cyberspace support requires an effective balance between security and capability. The current AFNET organizational structure provides a strong and necessary emphasis on security, but it could also benefit from realignment in order to enhance responsiveness to airpower operations. The proposed strategy answers the research question and aims to help achieve the balance the Air Force needs.

CONTENTS

Illustrations

Figure

Chapter 1

Introduction

> *The U.S. military's ability to use cyberspace for rapid communication and information sharing in support of operations is a critical enabler of DoD missions.*
>
> *2011 Department of Defense Strategy for Operating in Cyberspace*

Today the United States Air Force stands at a crossroads in deciding how to posture effectively and equip its force with the sustainable communications and cyberspace support necessary for 21st century warfare. Military operations are more dependent on information and communications technology capabilities than ever before. At the same time, threats to the systems that provide these capabilities have never been more numerous and continue to proliferate.

In the past decade, the Air Force has made two significant changes in the way it provides communications and cyberspace support to its air bases. First, over the past decade, it has consolidated information and communications technology services in an effort to reduce costs and enhance network security through centralized control, management, and administration.[1] This effort is largely complete, culminating in the consolidation of 27 legacy networks across the service into a global Air Force Network (AFNET).[2] Now a separate cost saving effort is currently underway to consolidate many of these same services at the Department

---

[1] For a synopsis on the benefits and history of the creation of the AFNET see, Michael J. Basla, "Toward a Single AFNet: Three Reasons Why the Air Force Must Migrate," *High Frontier*, May 2011, 3–4.

[2] Shelly Petruska, "Historical Milestone Reached for Air Force Cyberspace," *Air Force Network Integration Center*, April 1, 2014, http://www.afspc.af.mil/news1/story.asp?id=123405483; Max Cacas, "The Best Laid Plans Fly Awry," *SIGNAL Magazine*, accessed January 8, 2014, http://www.afcea.org/content/?q=node/11125.

of Defense (DoD) level through the Joint Information Environment (JIE) program.[3] Second, the Air Force incorporated its air base communications and cyberspace support structure into a new cyberspace operations enterprise, leading to the stand-up of the 24th Air Force under the Air Force Space Command.[4]

While both efforts appear successful in saving money and enhancing security, growing pains have emerged with implications for future communications and cyberspace support to Air Force missions. Cyber threats to Air Force communications and cyberspace support capabilities in the employment of missions in air, space, and cyberspace make this issue critical. Further consolidation and efficiency efforts at the DoD level with the JIE appear to further cloud the future of communications and cyberspace support to Air Force bases. This drives the need for the service to re-examine its current cyberspace support model, before an additional layer of consolidation and bureaucracy removes it further from the operational missions it supports. At the present crossroads the Air Force can either continue along the current path or re-examine the results of events that led to today's structure, reconsider potential pitfalls, and readjust as necessary to meet future changes in the DoD information enterprise.

The Air Force faces the difficult task of providing reliable, responsive, and relevant air base communications and cyberspace support on a global scale and in a challenged environment, where cyber threats are real and growing. It must further refine the methods it uses to deliver communications and cyberspace support from a corporately managed enterprise to meet the needs of Airmen at the edge of combat operations. This research aims to address this task and answer the

---

[3] Henry S. Kenyon, "Joint Information Environment Is Under Way," *SIGNAL Magazine*, accessed January 8, 2014, http://www.afcea.org/content/?q=node/11696.
[4] Air Force Fact Sheet, "24th Air Force Fact Sheet." http://newpreview.afnews.af.mil/24af/library/factsheets/factsheet.asp?id=15663

question: how should the Air Force posture itself to best provide responsive communications and cyberspace support to its air bases in a challenged environment?

Definitions

In the communications and cyberspace operations fields, terminology is often vague and at times confusing for a number of reasons. First, because cyberspace is a manmade domain of warfare, even professionals are prone to conceptualize the domain and operations within it in different ways. Second, the Air Force established its cyber operations force largely from the wholesale conversion of personnel in the communications and information technology community.[5] This led many to the conclusion that cyberspace operations and information technology are the same, or at the very least, evolutionary. This is not the case.[6]

For a clear discussion on the issues at hand, the author defines "communications and cyberspace support" as the information technology and communications services and associated infrastructure that the Air Force provides from the corporate and base levels. These services range from simple email, data, and collaboration services to voice communications to networks supporting command and control systems.

---

[5] The Air Force also incorporated personnel from the space, intelligence, and electronic warfare communities into its cyber force. This statement refers to the conversion of communications and information career field into the cyber operations force. These personnel make up the preponderance of the Air Force's cyber operators, but many still perform communications and information systems duties. For background on these decisions see, Joseph R. Golembiewski, "From Signals to Cyber: The Rise, Fall, and Resurrection of the Air Force Communications Officer" (School of Advanced Air and Space Studies, 2010), 80–87.

[6] The commander of the AF Space Command emphasized this point at a recent conference, "Information technology and cyber operations are not the same thing … Certainly IT provides the great tools and platform that we use, but that is not cyber operations. No more so than the F-22 sitting on the ground is doing air superiority." William L. Shelton, "Integrating, Air, Space & Cyberspace Capabilities" (presented at the Air Force Association - Air and Space Technology Exposition, National Harbor, MD, September 17, 2013), http://www.afspc.af.mil/library/speeches/speech.asp?id=742.

In other words, communications and cyberspace support are essential voice and computer services traditionally provided to operational missions through base communications squadrons. For the purposes of this thesis, other base communications squadron services such as radio and airfield systems are not included in the definition and remain outside the scope of this analysis.

Joint doctrine provides an appropriate definition of cyberspace operations and defines it as the employment of "cyberspace capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace."[7] To be clear, communications and cyberspace operations are separate, but related concepts. The success of communications capabilities depends on effective defensive cyberspace operations (DCO) and DoD Information Network (DoDIN) Operations.[8] The Air Force's cyberspace operations enterprise includes units that conduct cyberspace operations, but units that also provide communications and cyberspace support.

Methodology, Evidence, and Analytical Criteria

This thesis proposes a practical strategy in order to answer its central research question. Richard Rumelt, one of the world's most influential thinkers and writers on strategy and management, asserts that a good strategy includes three essential elements he calls the kernel of strategy: "a *diagnosis* of the situation at hand, the creation or identification of a *guiding policy* for dealing with the critical difficulties,

[7] "Joint Publication 3-30: Command and Control of Joint Air Operations" (Office of the Chairman of the Joint Chiefs of Staff, February 10, 2014), IV–3, http://www.dtic.mil/doctrine/new_pubs/jp3_30.pdf.

[8] US Cyber Command recognizes three lines of cyberspace operations: offensive, defensive, and DoD Network Operations. This work is primarily concerned with DCO and DODIN Operations. Offensive cyberspace operations are outside its scope. For a description of each of the three lines see Cheryl Pellerin, "Cyber Command Adapts to Understand Cyber Battlespace," *American Forces Press Service*, March 7, 2013, http://www.defense.gov/news/newsarticle.aspx?id=119470.

and a set of *coherent actions*."[9] This thesis constructs a strategy in similar fashion. Chapter two and the first part of chapter three help to *diagnose* the situation at hand. Chapter three then goes on to identify a *guiding policy* and set of *coherent actions* to form a strategy that places information, understanding, and influence at places where it does not currently exist.

In order to determine how the Air Force can best posture to provide responsive communications and cyberspace support in the future it is important to understand how today's support structure developed into its current form. This thesis begins with a brief history of how the Air Force has provided communications to its force, beginning with the origins of communications supporting early airpower through today's era of cyberspace operations. It takes advantage of archival documents, as well as historical and journalistic literature to examine the organizational development, operational impact, and technological integration that characterized the growth of Air Force communications and now cyberspace operations for eight decades of history.

Chapter three continues to diagnose the current state of Air Force communications and cyberspace support and begins with an explanation of why it is important for the Air Force to provide responsive communications and cyberspace support to operational commanders. It introduces agency theory and its applicability to the understanding of human and organizational behavior. The chapter then uses agency theory to explain tension points in the historical organization of Air Force communications under the Air Force Communications Command. It provides an explanation of the AFNET enterprise organizational model

[9] Rumelt received his doctoral degree from Harvard Business School and is currently the Harry and Elsa Kunin Chair at the UCLA Anderson School of Management. *The Economist* named him one of 25 living persons who have had the biggest impact on management concepts and corporate practice. Richard P. Rumelt, *Good Strategy, Bad Strategy: The Difference and Why It Matters*, 1st ed (New York: Crown Business, 2011), 7.

and its relationship to the missions it supports. Agency theory helps explain potential tension points in the current AFNET model. These tension points identify focus areas and help form a *guiding policy* consisting of three pillars that can drive actions. Finally, the chapter builds on this analysis and proposes a set of *coherent actions* to complete the strategy that enhances responsive communications and cyberspace support to air bases.

Chapter four aims to test and demonstrate the strategy presented in chapter three through two hypothetical case studies. The chapter introduces relevant doctrine, cyberspace security literature, and recent history of conflict in cyberspace in order to construct realistic and viable cases. The first case presents a demanding, but still reasonable, vignette of operations at a notional air base in the US Pacific Command area of responsibility. The second case builds on the original scenario, adding significant stress to the operations of the notional air base and the global AFNET. The author then evaluates the strategy's performance in each case to determine its contribution and responsiveness to the needs of the air base and the AFNET. Finally, chapter five presents a brief conclusion with implications for the future of communications and cyberspace support.

Scope and Limitations

Before addressing such a critical issue, it is important to identify the scope and limitations of this thesis. The aim here is to examine an Air Force issue, specifically, how the Air Force provides communications and cyberspace support to its operational bases. It does not focus on more specific models such as support to the Air Operations Center or remotely piloted aircraft operations.

Further limitations include the ever-changing nature of communications and cyberspace support in the Department of Defense. For example, while the stakeholders have developed many of the

organizational concepts, the department is still determining how to implement the JIE initiative. Therefore, this strategy may not account for the complete impact of new departmental changes associated with this effort and, in fact, the *coherent actions* proposed as part of this strategy will soon be obsolete. However, it is the author's hope that the tension points and *guiding policy* identified here for the AFNET communications and cyberspace support model will have transfer value to JIE implementation and future centralized cyberspace support models.

In addition to these limitations, the author acknowledges the limitations associated with the use of agency theory in explaining organizational behavior.[10] While these are certainly worthy concerns, it is also important to consider the advantages that agency theory brings to this analysis by revealing the position of natural and rational forces in organizational interactions. This is the purpose of using the theory here.

Conclusion

The Air Force has made significant strides in consolidating resources and posturing itself to operate effectively in the cyberspace domain. It must now re-examine the impact these changes have had on its ability to provide communications and cyberspace support to operational air, space, and cyberspace missions. With the modern military's dependence on information and communications technologies and the DoD's further consolidation of communications services, the importance and urgency is significant.

[10] For a critique on the applicability of Agency theory to management applications see, Sumantra Ghoshal, "Bad Management Theories Are Destroying Good Management Practices," *Academy of Management Learning & Education* 4, no. 1 (March 1, 2005): 75–91.

In the search for answers, it is first critical to examine how the Air Force arrived at its current model. Chapter two will provide the history of Air Force communications along with the logic for the present model.

Chapter 2

History

A Short History of Air Force Communications and Cyberspace Operations

The general whose communications have broken down has generally lost the battle.

General of the Air Force Harold H. Arnold

In many ways, the growth of communications in the Air Force has followed the growth of the service itself. As America advanced airpower for military purposes in the 20th century, its military developed and adapted the communications necessary to support new forms of warfare. New technologies gave way to new capabilities that the Air Force utilized as it evolved. This rapid growth inspired Airmen and others to view information networks as a new domain of warfare.

In developing of a strategy for responsive communications and cyberspace support to air bases, this thesis begins by *diagnosing* the situation hand. This chapter initiates that diagnosis by examining the rich history of communications supporting the US Air Force. It covers its growth and development of Air Force communications from the early days of the interwar period through the employment of information and communications technologies in today's advanced cyberspace domain.

The chapter begins with the story of early Airmen and their recognition of the need for a robust communications system. Next, it highlights the development of communications in WWII and through the new US Air Force's early years. It illustrates the rise and fall of centrally managed communications in the service. Finally, this chapter details the rapid growth of information and communications technology into a new domain of warfare and the Air Force's efforts to evolve with it.

Several themes emerge from this history that challenge communications and cyber operations personnel today. The first is the central management of information and communications technology capabilities and services. The second is the dependence of military operations on these capabilities and their integration into operational missions. The third theme is the acquisition, integration, and employment of new technologies and the ability of communications Airmen to apply them in support of airpower.

Influential American Airmen of the interwar period recognized the importance of effective communications in advancing airpower. Today's Airmen still recognize this importance. However, the Air Force faces the challenge of continuing to advance information and communications technologies in support of air, space, and cyberspace power through an increasingly complex and contested cyberspace domain.

Early Years

The airplane itself began its military career as a communications requirement from the U.S. Army Signal Corps for a heavier-than-air machine in late 1907.[1] As early Airmen advanced American airpower and began to uncover its potential through World War I and the interwar years, radio technology lagged behind the need for effective communications to support air operations. The use of short wave frequencies in the 1920s and the Very High Frequency band in the 1930s went a long way towards making communication between aircraft and ground stations worthwhile.[2] The United States established the first radio stations in a small air-to-ground communications network in 1923 and soon a network of 30 such stations existed across the country.[3]

---

[1] Christopher H. Sterling, ed., *Military Communications: From Ancient Times to the 21st Century* (Santa Barbara, Calif: ABC-CLIO, 2008), 10.
[2] Sterling, *Military Communications*, 11.
[3] Sterling, *Military Communications*, 32.

While not all early Airmen were proponents of radio communications in aviation, one influential Airman who recognized the importance of an established and coordinated communications network to enhance flying operations was Lieutenant Colonel Henry "Hap" Arnold.[4] On July 19, 1934, Arnold led an ambitious flight of 10 Martin B-10's from Bolling Field in Washington, D.C. to Fairbanks, Alaska and back again.[5]

Arnold knew he would need a well-coordinated effort to support the mission with navigational and weather information, so he tapped Captain Harold McClelland to organize this portion of the mission.[6] McClelland organized the ground communications stations needed to support the flight and assigned radiomen to aircrews. McClelland himself piloted one of the B-10s. The flight was an amazing success and earned Arnold and his team the distinguished Mackay trophy.[7]

Airmen like Arnold and McClelland knew that communications would be important in the advancement of airpower, but there were several barriers to a service-wide system of air communications. Civilian aviation made significant advances during the 1930s under the oversight of the Department of Commerce and commercial airlines. Together they created a robust communications network to create "highways in the sky" or air passageways to make air travel safer through improved navigation and communications.[8] A subsequent military training flight led by Arnold was less successful than the Alaska mission and further convinced him of the need for an integrated airways communications system.[9]

---

[4] Louis Shores, *Highways in the Sky* (New York: Barnes & Noble, 1947), 3.
[5] Morrison, Larry R., *From Flares to Satellites: A Brief History of Air Force Communications* (Scott AFB, IL: Air Force Communications Agency, 1997), 6–7.
[6] Shores, *Highways in the Sky*, 4–5.
[7] Shores, *Highways in the Sky*, 5.
[8] Shores, *Highways in the Sky*, 5.
[9] Morrison, Larry R., *From Flares to Satellites*, 7.

In addition, the means of a makeshift airways network was already in place throughout the United States in the 1930s, but it suffered from lack of coordination. The servicemen who operated the network worked for the post commander, so often times the needs of the post took precedence over transient air missions.[10]

Arnold and McClelland were convinced of the need for a robust, centrally managed, and coordinated system, comparable to the civilian system to support military aviation at home and abroad in the future. This desperate need took the first step towards realization on November 15, 1938 when the Headquarters Army Air Corps, at the direction of the War Department, formally established the Army Airways Communications System, better known as the AACS.[11]

The Army Air Corps placed the AACS under the direction and control of its Chief via the Directorate of Communications in the Training and Operations Division. Major Wallace Smith, the Air Corps Communications Officer served as the first AACS Control Officer. The Air Corps assigned the organization the mission of managing the its fixed radio communications facilities across the United States.

These facilities provided three basic services in support of air operations: 1) Interstation and air-to-ground communications along designated airways, 2) dissemination of weather data throughout the system, and 3) air traffic control services through the use of radio and other navigational aids.[12]

The AACS started out slowly, but evolved and grew at a rate to keep pace with the expansion of America's airways in the years leading up to World War II. The system initially divided the country into three

---

[10] Shores, *Highways in the Sky*, 5, 8.
[11] Betty A. Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, ed. Thomas S Snyder, Revised Edition (Scott AFB, IL: Air Force Communications Command, 1986), 5.
[12] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 5.

regions, each supported by a communications squadron with an officer serving as both the Regional Control Officer and squadron commander.[13] The AACS soon expanded to support routes in Puerto Rico, Panama, Alaska, and Hawaii and by 1940 had detachments in all of these locations as well as the Philippines.[14] Upon America's entry into World War II, the AACS had grown into a centrally directed worldwide organization supporting Army Air Forces across the globe.

World War II

From the initial Japanese attack on Pearl Harbor in 1941 to the Allied operations in Western Europe in 1944 to the final surrender of the Japanese empire in 1945, the Airmen of the AACS served with honor and distinction. On December 7, 1941, AACS Airmen braved the attack on American soil while executing duties in the control tower of Hickam Airfield.[15]

While most ground communications personnel served in relatively secure settings throughout the war, extraordinary commitment to the mission, even at great personal risk, was not uncommon. Sergeant Ranier Payton was one such individual who exemplified this commitment and bravery. A ground based radio operator at Guadalcanal, Sergeant Payton responded to an urgent call for volunteer radio crewmen from a nearby bomber squadron in August of 1943. Ranier volunteered for the mission despite having no aircrew experience and unfortunately became the first AACS casualty of the war when the B-17 in which he flew was gunned down by an enemy night fighter.[16]

---

[13] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 5.
[14] Shores, *Highways in the Sky*, 25–29; Linda G. Miller and Cora J. Holt, *Window to the Future: Air Force Communications Command Chronology 1938-1988* (Scott AFB, IL: Air Force Communications Command, 1989), 15.
[15] Sterling, *Military Communications*, 33.
[16] Miller and Holt, *Window to the Future*, 24.

AACS Airmen supported operations in the European theater with comparable commitment and dedication. After the initial D-Day invasion in Normandy, AACS men soon followed to support allied air operations at airfields belonging to the enemy only hours before their arrival.[17] The mobile nature of operations on the European continent required support personnel to be very mobile, establishing new airfields as ground forces advanced.

As Lieutenant General George S. Patton's 3rd Army raced toward the Rhine, communications men from the AACS steadfastly followed. In one case, an AACS detachment inadvertently moved past Patton's advance patrols and established a communications presence at an unsecured German airfield. The Airmen awoke the next morning to the sound of German tanks and supply trucks in the area. Luckily, the detachment escaped unharmed, but their endeavor is an example of the spirit and dedication to the mission these Airmen exuded.[18]

At the war's end in August of 1945, the AACS played a critical role in communicating General MacArthur's surrender instructions to the Japanese. After normal War Department signal channels failed to prompt a response from Japanese forces, MacArthur turned to the AACS for assistance. AACS radio operators suspected Japanese forces monitored a frequency used for transmitting un-coded weather information and used it to transmit MacArthur's message. It worked, as the Japanese responded within two hours. This was the first direct military communication between the Allies and the Japanese since the war began.[19]

AACS Airmen were among the first American military personnel to land at Atsugi Airfield in preparation of the deployment of MacArthur's

---

[17] Miller and Holt, *Window to the Future*, 28.
[18] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 19–20.
[19] Sterling, *Military Communications*, 33; Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 38.

occupation force. Uneasy AACS Airmen had their fears calmed when they learned the overwhelming number of troops lined along the airfield were a guard arranged in honor of their arrival and not a hostile force poised for a sneak attack.[20] The war had indeed ended.

Like the mission and the execution of airpower itself throughout the war, the communications support structure evolved as well. As America entered the war, the AACS quietly avoided a reorganization that would have surely spelled the disbanding of its central control structure. The logic behind the Allied multi-theater command structure should have placed the mission and assets of the AACS under each theater level command. However, since the Army Air Forces viewed communications largely as a secondary priority, the incumbent organization structure survived and by most measures performed satisfactorily.[21]

During World War II, the AACS had grown from a small outfit of regional squadrons and detachments to a wing to a full-fledged command by the spring of 1944.[22] By the end of the war, the AACS consisted of 8 wings, 21 groups, 55 squadrons, over 700 detachments, with more than 49,000 troops, and 819 stations across the world.[23]

The AACS also took advantage of significant improvements in technology to enhance its support to air operations. In Feb of 1945, the AACS installed the first ground controlled approach radar, an AN/MPN-1, in Etain, France.[24] This dramatically enhanced safety for night landings and landings during bad weather conditions.[25] In addition, the AACS was able to utilize improvements in radio and wired

---

[20] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 39.
[21] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 42.
[22] Miller and Holt, *Window to the Future*, 25.
[23] Sterling, *Military Communications*, 33.
[24] Miller and Holt, *Window to the Future*, 29.
[25] Morrison, Larry R., *From Flares to Satellites*, 10–11.

communications, including the use of a Western Electric time division multiplexed microwave relay system across Europe.[26]

Post-War Years and the U.S. Air Force

The U.S. Army Air Forces and its communications support saw significant changes at the end of World War II. Organizational changes helped the new service prepare for operations in Berlin and Korea. In addition, communicators were able to bring new technologies to bear in support of early US Air Force airpower.

The end of the war meant rapid demobilization for the US military and the AACS was no exception in that effort. The command slimmed down from its wartime strength to 4 wings, 11 groups, and 25 squadrons.[27] Because a significant portion of AACS support was tied to airlift operations, the organization was re-designated the Air Communications Service and transferred to the Air Transport Command on March 13, 1946. It was re-designated again as Airways and Air Communications Service six months later and regained its battle tested AACS brand name.[28]

Not long before the Air Force officially gained its independence, a debate sparked that would be a recurring theme throughout the history of Air Force communications: whether communications should be managed centrally. In March of 1947, Lieutenant General John K. Cannon, Commander of the Air Training Command endorsed a letter from Major General James Hodges, Air Training Command's Flying Division, to General Carl Spaatz, the Commanding General of the Army Air Forces advocating the alignment of communications resources and operations under individual base commanders. Hodges argued that in

---

[26] Morrison, Larry R., *From Flares to Satellites,* 11.
[27] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History,* 47.
[28] Miller and Holt, *Window to the Future,* 34–35.

order to be effective air base commanders needed to control all facets of the base's operations. He went on to articulate "direction, standardization, and overall control should come from Headquarters, Army Air Forces, not from a small vertical lateral command."[29]

AACS commander at the time, Major General McClelland, crafted a rebuttal for General Spaatz's consideration. McClelland's argument emphasized the dual-hatted nature of organizing to support individual missions with a central single manager to ensure consistency and effective integration of communications systems across the service.

Perhaps nothing at the time was more convincing than the performance of the AACS during WWII and McClelland went on to argue against dissolving a system "that has proven itself capable of meeting wartime requirements, just to make the base commander 'king of all he surveys.'"[30] This logic led Spaatz to accept McClelland's position and continue to manage and control the AACS organization centrally.[31] However, similar debates would re-emerge throughout the command's history.

As the Air Force gained its independence in September of 1947, the AACS remained an independent command, but in June of 1948 the Air Force incorporated it as a subordinate command under the Military Air Transport Service (MATS). This was a part of a service-wide consolidation of strategic airlift resources into a single transportation organization.[32] AACS would remain a subordinate command under the MATS until the early 1960s.

The AACS and its centralized organization structure proved more than capable of supporting the early operations of a young air service.

---

[29] Hodges as quoted in Miller and Holt. Miller and Holt, *Window to the Future*, 35.
[30] Miller and Holt, *Window to the Future*, 35.
[31] Miller and Holt, *Window to the Future*, 35.
[32] Miller and Holt, *Window to the Future*, 35.

The Air Force would need the AACS and its subordinate units to play critical roles in both the Berlin Airlift and the Korean War.

The 1946 AACS Squadron, the primary unit supporting the Berlin Airlift with air traffic control and communications services, had to adapt and grow as rapidly as the airlift itself. Vastly understaffed at the beginning of the airlift, the unit quickly augmented its low numbers with reserve and civilian personnel, utilizing on-the-job training to prepare them for the complexities of the mission. Maintenance personnel installed additional radio communications and navigation equipment to support air routes and the enormous volume of air traffic. In total, AACS controllers and maintenance personnel controlled and supported 276,926 airlift flights during the infamous operation to supply West Berlin during the Soviet blockade.[33]

Within one week of President Truman's authorization of American involvement in the Korean War, AACS detachments were operating at airfields at Pusan, Pohang, and Taegu.[34] AACS units continued to support MacArthur's initial offensive and advances in 1950. However in late 1950, China's entry into in the conflict and subsequent counteroffensive forced communications personnel to remain mobile.

As communist forces pushed back American troops, AACS Airmen played key roles keeping airfields active for the withdrawal. For two days and nights, an AACS detachment armed with rifles helped defend a doomed Pohang Airfield from foxholes as forces evacuated the area. The Airmen then trucked radar and other equipment 12 miles through hostile territory to a waiting landing ship. The detachment of 45 men escaped without casualty.[35]

---

[33] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 51–57.
[34] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 60.
[35] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 63.

As the young air service oriented itself to a large role in American defense during the early Cold War, its views on communications also matured. Operational experiences in Berlin and Korea as well as rapidly developing technology compelled the service to re-examine how it approached communications. It did just that in the early 1960s.

A Major Air Command for Air Force Communications

During its first decade as an independent service, Air Force leaders observed that the importance of communications in command and control required a single manager for Air Force communications. By the early 1960s, most Air Force leaders agreed with this view, which paved the way for a service-wide command, devoted to the communications needs of the larger force.[36] This command would go on to serve the Air Force well in the operations in Vietnam and help the service leverage breakthrough communications technology for air power.

The Air Force took several steps in re-organizing its communications beginning in the late 1950s and early 1960s. It first centralized communications procurement under the Air Force Logistics Command. Next, it established a division for the development, integration, and procurement of C2 systems under Air Force Systems Command.[37] These actions paved the way for the reorganization of communications into a single major command to support the Air Force.

On July 1, 1961, the Air Force relieved AACS from its previous command, the Military Air Transport Service, re-designated it as the Air Force Communications Service (AFCS), and established it as the Air Force's 16th major air command.[38] The new command inherited the responsibilities of air traffic control and long-haul message services from

---

[36] Sterling, *Military Communications*, 3.
[37] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 79.
[38] Miller and Holt, *Window to the Future*, 59.

its predecessor, the AACS, but its mission also stretched to meet the growing demands of global Air Force communications.[39]

The expanded mission of the new AFCS organization consisted of four areas. First, the new command coordinated most on-base communications services, including base cable plants and maintenance networks.[40] Second, it managed an expanded set of long-line communications such as radio, teletype, and telephone networks as well as special networks for aircraft and missile early warning systems.[41] Third, it expanded air traffic control services, including point-to-point and ground-to-air stations, airfield control towers, navigational aids, precision approach radar control services, and flight service evaluations.[42] Finally, the new command also managed contingency mission support through rapidly deployable mobile units. These units could deploy at moment's notice to provide essential communications and air traffic control support to emerging Air Force operations.[43]

The AFCS initially continued to employ a regional organizational support model with subordinate units organized into nine geographically based units. Seven communications regions covered the continental United States and Alaska, while two communications areas supported the Europe-African-Middle Eastern and Pacific major overseas theaters.[44] Over its first two years, the new command used this structure to gradually assume the telecommunications and air traffic control services

---

[39] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 79–80.
[40] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 80.
[41] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 80.
[42] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 80.
[43] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 80.
[44] Miller and Holt, *Window to the Future*, 59.

of all Air Force major commands except Strategic Air Command (SAC) and Air Defense Command (ADC).[45] The decision to centralize SAC and ADC communications support met resistance due to the enormous importance of each command's mission and the issue would go unresolved until the 1970s.[46]

Although it would take several decades to fully implement, the regional organizational structure eventually gave way to a functional structure designed around the operational commands themselves. In 1963, at the request of Tactical Air Command (TAC), AFCS stood up the TAC Communications Region at Langley AFB, Virginia.[47] It would be the mid-1980s before AFCS fully adopted the command-based organization structure.[48]

The success of AFCS as a major command as well as the effectiveness of the TAC Communications Region helped lead to the incorporation of SAC communications into the AFCS structure. In 1976, AFCS created the Strategic Communications Area to support SAC. SAC communications and its more than 5,000 communications professionals transitioned to the AFCS. The AFCS area commander served not only as the operational communications commander for the units supporting SAC, the position also served as the Communications Deputy to the SAC Commander in Chief.[49]

In 1974, the Air Force, following congressional guidance, sought to reduce its management headquarters and support function management through consolidation.[50] On November 21 of the same year,

---

[45] Miller and Holt, *Window to the Future*, 59.
[46] Miller and Holt, *Window to the Future*, 59, 81.
[47] Miller and Holt, *Window to the Future*, 63.
[48] Miller and Holt, *Window to the Future*, 109.
[49] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 145.
[50] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 149.

Headquarters Air Force announced it would disestablish the AFCS as a major command and realign it under the Military Airlift Command (MAC) in an effort to reduce costs.[51] The realignment not only returned the communications command back to its air transport origins, but it also required the organization to move from its headquarters at Richards-Gebaur AFB, Missouri to Scott AFB, Illinois.[52]

The move drew scrutiny from AFCS civilian employees as well as Missouri political leaders, resulting in a lawsuit that forced the Air Force to study the environmental impact of the move.[53] When the Air Force filed the final environmental report in 1977, it directed the AFCS to move to Scott AFB. However, the Air Force opted to keep AFCS as a major command, but mandated it share staff resources with the MAC.[54]

The unique staff sharing experiment between the MAC and AFCS was the first of its kind and called for the sharing of non-technical support functions such as comptroller, staff judge advocate, personnel, and administration.[55] The arrangement soon proved troublesome and nearly all staff functions returned to the communications command.[56] As a firmly established major air command now at Scott AFB, the Air Force re-designated AFCS as the Air Force Communications Command (AFCC) on November 15, 1979 (the 41st anniversary of the AACS).

A final significant organizational change during this period came in the early 1980s with the merger of information systems and communications. As small computing technology proliferated in government and business, boundaries between communications and

---

[51] Miller and Holt, *Window to the Future*, 79.
[52] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 149.
[53] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 149.
[54] Miller and Holt, *Window to the Future*, 82–84.
[55] Miller and Holt, *Window to the Future*, 85.
[56] Miller and Holt, *Window to the Future*, 86.

data automation quickly blurred. Recognizing these changes, the Air Force responded by merging its existing data automation organizations, which operated major systems like mainframe computers, into the AFCC.[57]

As the organizational structure continued to evolve during this era, Air Force communications units provided a tremendous amount of support to major air operations of 1960s, and 1970s. From the Cuban Missile Crisis to the Vietnam War, Air Force communications professionals continued a firmly established tradition of supporting contingency air operations with dedication.

From October 8 to November 4, 1962, the AFCS's 3rd Mobile Communications Group provided support to the forces participating in the Cuban Missile Crisis buildup. Within a week of notice, the group had navigation, communications, and weather teletype machines deployed to locations throughout Florida in preparation for potential operations.[58] Fortunately, the buildup succeeded and the United States avoided catastrophe. However, this experience identified the need for a new structure for mobile communications support, leading to the creation of the 4th and 5th Mobile Communications Groups (of which the 5th Combat Communications Group still remains today).[59]

AFCS played a major role in America's involvement in Vietnam in the 1960s and 1970s. In May 1962, the AFCS established the 1964th Communications Squadron as its first fixed unit in Southeast Asia, marking the beginning of a sustained presence for the organization.[60] The large increase in American involvement led to the creation of the 1974th Communications Group at Korat AB, Thailand to support Air

[57] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 192.
[58] Miller and Holt, *Window to the Future*, 62.
[59] Miller and Holt, *Window to the Future*, 65.
[60] Miller and Holt, *Window to the Future*, 61.

Forces throughout Southeast Asia beginning in 1965.[61] In 1968, global air operations reached an all-time high with 19,539,435 operations worldwide, fueled primarily by missions supporting military operations in South Vietnam. Air traffic controllers at Bien Hoa, DaNang, and Tan Son Nhut Air Bases routinely exceeded traffic at America's busiest airports.[62]

The war in Vietnam produced many casualties and communications personnel were not immune. Staff Sergeant David Fasnacht, a telecommunications system controller with the 1st Mobile Communications Group, became the first AFCS casualty. On July 15, 1967, after landing at DaNang AB, the C-130 he was travelling on came under attack and was hit by a mortar.[63] The AFCS would go on to lose 11 Airmen in the Vietnam conflict.[64]

Communications played a major role throughout operations in Vietnam. At the war's end in 1973, Airmen from the 1st Mobile Communications Group established communications in Hanoi to support medical evacuation flights for America's liberated prisoners of war (POW). Meanwhile, communications Airmen at Clark AB, Philippines readied hundreds of phone lines to connect the POWs to loved ones for the first time.[65] In the spring of 1975, AFCS Airmen with a radio-equipped jeep provided communications for the Defense Attaché Office during the evacuation of Saigon. Two Airmen volunteered to stay and support the US Marines securing the embassy and when they were airlifted out by helicopter in the early morning of May 1st, they became the last Air Force personnel evacuated from South Vietnam.[66]

---

[61] Boyce et al., *The Air Force Communications Command: 1938-1986, An Illustrated History*, 124.
[62] Miller and Holt, *Window to the Future*, 69.
[63] Miller and Holt, *Window to the Future*, 69.
[64] Miller and Holt, *Window to the Future*, 75.
[65] Miller and Holt, *Window to the Future*, 78.
[66] Miller and Holt, *Window to the Future*, 80.

In addition to the significant military operations of Vietnam, this period also ushered in a wave of communications technology to support air power. High-speed data communications, standardized voice networks, and improvements in infrastructure paved the way for significant advances in capability for the Air Force and the Department of Defense.

High-speed data communications can trace its origins to several points in history, but one significant milestone would be the establishment of the Air Force Data Communications system. The system was developed to replace the Combat Logistics Network and became the Air Force's first fully electronic and automatic high speed data network. The system went operational in 1963 and would go on to grow into the Department of Defense Automated Digital Information Network (AUTODIN).[67]

The AUTODIN utilized automated switching technology to maximize the use of available bandwidth and deliver messages with a high rate of reliability.[68] The system was in such demand that its users saturated the network in its first year of operations and the Secretary of Defense quickly approved its expansion.[69] The Defense Communications Agency (DCA) eventually assumed AUTODIN management and operational responsibility as the system grew to 450 installations across the Department of Defense.[70] The system would serve the military well, lasting for over 30 years before the Defense Message System eventually replaced it in the late 1990s and early 2000s.[71]

The Air Force implemented a similar program for voice communications. In 1963, the Department of Defense activated the

[67] Miller and Holt, *Window to the Future*, 63.
[68] Sterling, *Military Communications*, 47.
[69] Morrison, Larry R., *From Flares to Satellites*, 22.
[70] Sterling, *Military Communications*, 47.
[71] Sterling, *Military Communications*, 120–121.

Automatic Voice Network, or AUTOVON, a system derived from the US Army's Switched Circuit Automatic Network system. The network superseded the Wide Area Telephone Service system and replaced commercial toll calls between installations. Important to military purposes, the system enabled the prioritization of individual phone lines (for example those belonging to commanders and alert facilities) with call precedence preemption to increase the reliability of priority voice communications.[72] The AUTOVON system eventually grew into today's Defense Switched Network, or DSN.[73]

Air Force communications Airmen managed a wide variety of infrastructure to support systems like the AUTODIN and AUTOVON. One advantage of a centralized command like the AFCS was the ability to procure, manage, and standardize the operations of systems across the Air Force. This would be needed to manage a diverse set of infrastructure, which included everything from the maintenance of underwater cable with the use of AFCS cable barge, the *Colonel Basil O. Lenoir,* to wideband and satellite communications.[74]

In Vietnam, the Tactical Air Control System drove the need for a robust network to support long-haul communications between air bases. Air Force communicators leveraged tropospheric-scatter and microwave technologies in addition to underwater cables (ironically, Airmen maintained these cables). The network began as a small effort named "Backporch," but eventually grew into a resilient communications backbone that connected Army, Navy, and Air Force locations as part of the Integrated Communications System – Southeast Asia.[75] The system

[72] Morrison, Larry R., *From Flares to Satellites*, 22–23.
[73] Sterling, *Military Communications*, 122.
[74] Miller and Holt, *Window to the Future*, 67.
[75] Morrison, Larry R., *From Flares to Satellites*, 31–33.

grew to support 80 locations throughout the theater, ensuring delivery of voice and data communications.[76]

Satellites added speed and range to Air Force's mobile communications capabilities. The first satellite terminal, the AN/MSC-46 became operational in 1967 at Clark AB, Philippines under the Initial Defense Communications Satellite Program. In November 1968, the 3rd Mobile Communications Group proved the feasibility of a mobile satellite communications terminal to support tactical deployments with the testing of the AN/TSC-54.[77] Satellite communications still play a vital role in the Air Force's ability to project power across the globe.

As an independent major air command, the structure charged with delivering the service's communications went through a series of organizational changes as it supported major combat operations and integrated new technology to support air power. However, the debate to manage centrally Air Force communications continued.

"That Darned Comm Command"

The 1990s saw several changes in the communications community as it adapted as an organization, continued to support contingency operations, and merged new information and communications technologies to support the Air Force. The proliferation of information networks added tremendous capability to the Air Force arsenal and its ability to command and control forces. However, with the new capacity also came new liabilities.

In July 1989, then Secretary of Defense Richard B. Cheney directed the military services to analyze operations and acquisition processes in an effort to find more cost-effective management methods;

[76] Morrison, Larry R., *From Flares to Satellites*, 33.
[77] Morrison, Larry R., *From Flares to Satellites*, 26.

he set a target of saving $39 billion in fiscal years 1991-1995.[78] AFCC identified significant changes in technology and management that would allow the command to shed 2,350 manpower positions. The Air Staff quickly accepted the changes. However, the functional review morphed into a new debate over the future of Air Force communications and the AFCC.[79]

In addition to the functional review, a similar discussion on communications support in the Pacific Air Forces (PACAF) command took place in the late 1980s. This prompted the PACAF commander at the time, General Merrill McPeak, to send a formal request to assign all communications units in the PACAF theater to his command. McPeak referred to the existing structure as a "stovepipe" and thus saw no advantages in the functional command with dual-hat responsibilities. He offered PACAF as a test case to see how a new operational command structure would work for the Air Force.[80]

It was in this context that Air Force Chief of Staff General Larry Welch created a separate Defense Management Review panel to look at alternative structures for AFCC.[81] On June 18, 1990, General Welch announced a "complete restructure of Air Force communications and computers" effective October 1, 1990.[82] The announcement cited the need to strengthen the unity of command for operational commanders as

[78] Shelley L. Davis et al., *The Air Force Communications Command: 1938-1991, An Illustrated History*, ed. Thomas S Snyder, Third Edition (Scott AFB, IL: Air Force Communications Command, 1991), 259.
[79] Davis et al., *The Air Force Communications Command: 1938-1991, An Illustrated History*, 260.
[80] Davis et al., *The Air Force Communications Command: 1938-1991, An Illustrated History*, 260.
[81] Davis et al., *The Air Force Communications Command: 1938-1991, An Illustrated History*, 260.
[82] Davis et al., *The Air Force Communications Command: 1938-1991, An Illustrated History*, 260–261.

a primary reason for the changes, harking back to similar issues raised by Major General Hodges in 1947.[83]

As part of the reorganization, the AFCC transferred its operations and maintenance units to the commands they supported to create an operational command structure.[84] This meant that each operational command owned and operated its communications units just as it did any other unit. The former AFCC communications division now reported to the major command commander, while base communications squadrons reported directly to their respective wing commanders. The move sliced the command from approximately 55,000 authorized personnel to 9,000.[85]

In a 1993 interview following his retirement, Lieutenant General (retired) Robert Ludwig, AFCC commander at the time of the reorganization, reiterated the reasoning cited in the announcement. "We thought that our dual-hat relationship was a structure which would allow the operational commanders to have operational control over their communicators," General Ludwig explained, "but, … in the view of the operational commanders, that didn't cut the mustard."[86] He went on to note, "they [operational commanders] didn't like AFCC making independent assessments of how they would organize their comm units," and, "resource allocation decisions within their comm units."[87] General

---

[83] Davis et al., *The Air Force Communications Command: 1938-1991, An Illustrated History*, 261.
[84] Robert T. Cossaboom et al., "History of the Air Force Communications Command: 1 January - 31 December 1991," July 1, 1992, 1, (AR) 7101, HAF-HO.
[85] Davis et al., *The Air Force Communications Command: 1938-1991, An Illustrated History*, 275.
[86] Lieutenant General (retired) Robert H. Ludwig, interview by Robert T. Cossaboom, April 30, 1993.
[87] Lieutenant General (retired) Robert H. Ludwig, interview. Ironically, it is worth noting that General Ludwig expressed sentiments similar to those of operational Air Force commanders arguing for the dissolution of AFCC with the Defense Information Systems Agency's (DISA) ability to provide C4 services to the Air Force. When asked about Defense Management Review Decision 918, a directive that gave DISA the authority to

Ludwig observed that the AFCC structure placed a communications squadron commander in a tough position and some of the frustration this created led to the command's dissolution:

> Their [communications squadron commanders'] wing commander would ask them to do something, set up a small computer personnel support center, and AFCC would never resource the unit to have a small computer personnel support center, so the squadron commander would have to readjust within his own resources. He would obviously enter into a lot of pissing and moaning, discussion, and the word goes back, "that darned comm command." And that was "the" single largest factor, which lead [sic] to the disestablishment of AFCC. OPCON [operational control] was not the same thing as ownership and the operational commands felt they needed ownership.[88]

On February 4, 1991, Chief of Staff, General Merrill McPeak, as part of a larger headquarters restructuring, further directed the AFCC to transition from a major command to a forward operating agency, reporting directly to the Deputy Chief of Staff, Command, Control, Communications, and Computers.[89] The change took effect July 1, 1991.[90] With the move, "that darned comm command" was no longer a command.

---

operate and manage the DoD's wide area information network infrastructure, he called it one of "the most ill-conceived and potentially disastrous things that could ever happen in my 34-35 years in the military information systems business. I say that because what it does is it removes and breaks the link between the provider of information technology service and the consumer, or the requirer of it. It puts DISA, who is not responsible for the outcome, in the sole position of organizing and training and equipping the information technology activities of the services, and they're not accountable in any way, shape, or form to the operational commanders who have to use it." This is essentially the same argument that operational commanders used against a centralized AFCC.

[88] Lieutenant General (retired) Robert H. Ludwig, interview.

[89] Cossaboom et al., "History of the Air Force Communications Command: 1 January - 31 December 1991," 4–5.

[90] Sterling, *Military Communications,* 5.

The Road to Cyberspace

The 1990s saw the rapid expansion of unclassified and classified data networks, which communications units integrated quickly into the operations of each air base. Under the operational command structure, each major command established and operated capabilities to serve best the individual budgets and needs of their respective organizations. The Defense Information Systems Agency, through the governance it provided in connecting to the Secret Internet Protocol Router Network (SIPRNET, or classified network) and the Non-secure Internet Protocol Router Network (NIPRNET, unclassified network), underwrote, at least in some part, interoperability during this growth period.[91] However, this governance only went so far and the disjointed growth of information and communications technology systems and capabilities across the Air Force persisted.

With the hasty growth of information technology, Congress grew concerned about the possibility of wasteful spending throughout the government. In response, Congress passed the Information Technology Management Reform Act (ITMRA), commonly referred to as the Clinger-Cohen Act, in 1996. The act gave the Air Force full and independent acquisition authority and created the Chief Information Officer position (CIO).[92] The Air Force used the new position to help govern the evolving command, control, communications, and computers functional area.[93]

Increasing dependence on networked information coupled with emerging security threats caused Air Force communications leaders to take notice in the late 1990s. One prominent leader who responded to this concern was Air Combat Command Director of Communications and Information, Brigadier General Dale Meyerrose. General Meyerrose

---

[91] Morrison, Larry R., *From Flares to Satellites,* 70.
[92] Morrison, Larry R., *From Flares to Satellites,* 71.
[93] Morrison, Larry R., *From Flares to Satellites,* 72.

established the first Network Operations and Security Center, or NOSC, to monitor and direct network operations within the command and respond to security incidents.[94] Other major commands soon followed suit. The NOSC enabled the command and control of diverse and complex information networks at the MAJCOM level. However, the Air Force still lacked the ability to control effectively these networks across the service.

Recognizing this fragmented nature of the service's networks and the need to exercise more efficient control over them, Vice Chief of Staff of the Air Force General Robert H. Foglesong, appointed Air Combat Command as the Air Force lead for developing network command and control operations in July 2003.[95] The Air Force approved the Air Force Network Operations (AFNETOPS) concept in 2005. This concept designated the 8th, Air Force commander as the AFNETOPS commander, empowering the position with the authority to direct actions in the operation of the aggregated Air Force network, or AFNET.[96]

The concept also introduced the integrated NOSC, or INOSC, into the structure. Not only would the INOSC allow the AFNETOPS commander to focus on the command and control, operations, and security of the AFNET, it also allowed the Air Force to begin standardizing and centralizing information services such as email and data storage.[97] This effort would eventually allow the Air Force to lock in projected budgetary savings primarily through personnel, operations, and maintenance cuts in base communications squadrons in addition to

---

[94] Maryann Lawlor, "Command Takes Network Control," *SIGNAL Magazine*, October 2006, http://www.afcea.org/content/?q=node/1206.
[95] "Program Action Directive 07-10: The Implementation of the Chief of Staff of the Air Force Direction to Establish the Air Force Network Operations Organization Structure" (Headquarters United States Air Force, November 13, 2007), 1.
[96] Lawlor, "Command Takes Network Control."
[97] Ben Hinton, "Harnessing the Power of Cyberspace," *Intercom*, April 2006, 6.

the personnel cuts directed as part of Program Budget Decision 720.[98] The Air Force consolidated ten major command NOSCs into two INOSCs under the command of the AFNETOPS commander in 2006.[99]

Air Force leaders at the highest levels began to visualize C2 as well as communications and information in a different way. The networks that the service established for communications purposes now formed a part of new domain of warfare to defend and contest. On December 7, 2005, Secretary Michael Wynne and Air Force Chief of Staff T. Michael Moseley announced that the Air Force's mission was to "… fly and fight in air, space, and cyberspace."[100] The addition of cyberspace to the air and space domains was an acknowledgement of the new domain and signaled a change in the Air Force's approach was on the horizon.

The following September, Secretary Wynne and General Moseley issued an order requesting options for an operational cyberspace command, directing relevant MAJCOMs to "construct a plan to organize and to train in preparation for presentation of forces necessary to support Combatant Commanders, and the specified supported agencies in Cyberspace."[101] A subsequent order in November tasked General Robert Elder, in his role as the commander, 8th Air Force and Air Force Cyber Command, to "provide combat ready forces trained and equipped to conduct sustained offensive and defensive operations through the electromagnetic spectrum and fully integrate these with air and space

[98] Todd Stratton, "Cyberspace Support as a Strategic Vulnerability of USAF Operational Wings" (Air War College, 2014), 5.
[99] Lawlor, "Command Takes Network Control."
[100] Michael W. Wynne and T. Michael Moseley, "Letter to the Airmen of the United States Air Force," December 7, 2005, http://www.24af.af.mil/shared/media/document/AFD-111003-050.pdf.
[101] Michael W. Wynne and T. Michael Moseley, "Establishment of an Operational Command for Cyberspace," September 6, 2006, http://www.24af.af.mil/shared/media/document/AFD-111003-051.pdf.

operations."[102] The Air Force was poised to operationalize its cyberspace capabilities, including network operations, further changing the way in which it delivered communications throughout the service.

In September 2007, the Air Force activated Air Force Cyberspace Command (Provisional) at Barksdale AFB, Louisiana in anticipation of establishing a permanent major command in October 2008.[103] The Air Force continued its march toward building the command with the release of Program Action Directive 07-08 Change 1 in January 2008. It directed the alignment of the 67th Network Warfare Wing, the home of AFNETOPS and its INOSC units, combat communications units, and the establishment of an electronic warfare wing within the new command.[104]

A series of events in 2008 interrupted the path of the new command. After the exit of Secretary Wynne and General Moseley in the summer of 2008, new Air Force Secretary Michael B. Donley and Chief of Staff General Norton A. Schwartz directed a delay in the establishment of the new command in order to decide how best to align forces into the joint community.[105] In September 2008, the Secretary of Defense Task Force on DoD Nuclear Weapons Management recommended 8th Air Force focus on its nuclear mission and that the Air Force remove non-bomber related operations from its purview.[106] It was clear the Air Force needed to refocus on its nuclear enterprise.

In addition to these events, the Deputy Secretary of Defense Gordon England issued a new definition of cyberspace in May 2008 to

---

[102] T. Michael Moseley to Commander, 8th Air Force, "Operational Cyberspace Command 'Go Do' Letter," November 1, 2006, http://www.24af.af.mil/shared/media/document/AFD-111003-055.pdf.
[103] Gregory W. Ball, "A Brief History of the Twenty Fourth Air Force" (24th AF Historian, October 15, 2012), 9, http://www.24af.af.mil/media/document/AFD-131101-082.pdf.
[104] "Program Action Directive 07-08, Change 1: Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER)" (Headquarters United States Air Force, January 24, 2008), 11–14.
[105] Ball, "A Brief History of the Twenty Fourth Air Force," 9.
[106] Ball, "A Brief History of the Twenty Fourth Air Force," 10.

guide the joint community and the services as they worked to posture forces in the domain.[107] The new defense definition of cyberspace focused on information networks, but stopped short of encompassing the entire electromagnetic spectrum as the Air Force originally envisioned. This new definition also helped compel the Air Force to re-evaluate its cyber force structure.[108]

It was in this context in the fall of 2008 that the Air Force announced a new course of action to create a numbered air force for cyberspace operations. Planning soon began for the establishment of the 24th Air Force, aligned under Air Force Space Command.[109] Air Force Space Command activated the 24th Air Force on August 18, 2009 at a ceremony at the home of the new command at Lackland AFB, Texas.[110] The new organization included the 67th Network Warfare Wing, the 688th Information Operations Wing, and the 624th Operations Center and added the 689th Combat Communications Wing two months later to complete the transition.[111] The new command achieved full operational capability the following year on October 1, 2010.[112] The Air Force now had an operational command dedicated to cyberspace.

Conclusion

The history of communications in the Air Force is long one. As air operations grew in complexity, so too did their dependence on effective communications. From the coordination of a flight of B-10s bound for Alaska, to operations in WWII and Vietnam, to the dependence on

[107] Nancy E. Brown, "Difficulties Encountered as We Evolve the Cyber Landscape for the Military," *High Frontier*, May 2009, 6.
[108] John W. Maluda, "On Cyberspace Developments," *High Frontier*, May 2009, 9.
[109] Ball, "A Brief History of the Twenty Fourth Air Force," 2.
[110] Ball, "A Brief History of the Twenty Fourth Air Force," 3.
[111] Ball, "A Brief History of the Twenty Fourth Air Force," 4–5.
[112] Ball, "A Brief History of the Twenty Fourth Air Force," 6.

information to command air power through a modern Air Operations Center, its vital importance continues to grow.

This history presented several themes, which are relevant to today's communications and cyber operations organizations. The first is the central management of information and communications technology capabilities. From 1938 to 1988, the Air Force studied the need for a centralized communications organization at least 18 times. Most of the studies centered on the need to support effectively an operational commander through the control over assets supporting the command's mission.[113]

The need to align communications assets to better support the operational mission drove the disestablishment of AFCC as a major command in 1991. The subsequent proliferation of information networks and their associated threats to security demanded that the Air Force seek better control of the management of these systems. It did this first through functional authorities and then through a dedicated command. Still today, the command structure is unfamiliar and uncomfortable to many, with a central organization providing much of the information and communications technology support to operational units that also possess their own communications and cyberspace operations personnel.

The second theme is the dependence of military operations on communications. Communications Airmen have served with honor and distinction throughout our nation's conflicts, with many giving the ultimate sacrifice. Effective communications has been a significant component of air power for generations and will continue to be a large part of future operations.

The third theme is the evolution of information and communications technologies and the ability of communications and cyberspace operations Airmen to integrate them in support of airpower.

---

[113] Davis et al., *The Air Force Communications Command: 1938-1991, An Illustrated History*, 260.

Airmen adapted new radar and microwave technologies to help fight WWII, developed and leveraged robust data and voice networks and satellite communications in fixed and tactical environments, drove the rapid expansion of information networks, and helped harness their subsequent transformation into a new warfare domain. It is clear that flexibility has always been a core attribute of communications Airmen.

The next chapter will continue the *diagnosis* of the situation at hand, identify a *guiding policy*, and propose *coherent actions* in order to form a new strategy for responsive communications and cyberspace support to air bases in a challenged environment. This history informs the next chapter and provides the context for today's structure as well as identifying potential trouble areas to avoid in the future. Air Force communications and cyberspace operations have a come a long way in the 80 years since Hap Arnold's historic Alaska flight, but as this history illustrates, the development of new technologies to support air, space, and cyberspace operations will take it even further.

Chapter 3

Strategy

A Strategy for Air Force Communications and Cyberspace Support

Fighting with a large army under your command is nowise different from fighting with a small one: it is merely a question of instituting signs and signals.

Sun Tzu

Our IT systems do not simply allow us to e-mail one another, chat online, and access the web for administrative tasks. They are the backbone we use to interconnect operations across multiple domains and deliver mission success around the globe.

General Martin E. Dempsey
18th Chairman of the Joint Chiefs of Staff

The history of communications and now its intersection with the emergence of cyberspace operations shows that the Air Force and its Airmen have adapted to overcome many challenges. Today's Air Force has made significant progress operationalizing forces for the cyberspace domain. The creation of the 24th Air Force (24 AF) under the Air Force Space Command (AFSPC) added tremendous focus, rigor, and discipline to cyberspace operations forces. However, the coupling of network operations, core information and communications technology services, and client support into a centralized organization presents challenges for the air bases that depend on these capabilities. This chapter seeks to understand the reasons for those challenges and continues the *diagnosis* of the situation at hand, then present a *guiding policy* with *coherent actions* to form a strategy that addresses them.

A sensible next step in developing a strategy for communications in today's Air Force is critical to this study. Simon Sinek, in his best-selling book *Start with Why*, asserts that successful companies, organizations, and leaders think, act, and communicate in a distinct pattern. He describes the pattern through his Golden Circle concept. At the center of the circle is *why*, enclosed by a ring *how*, and finally an outer ring *what*. Sinek contends very few organizations can articulate why they do what they do and this is the key and essential starting point in defining and building a successful organization.[1]

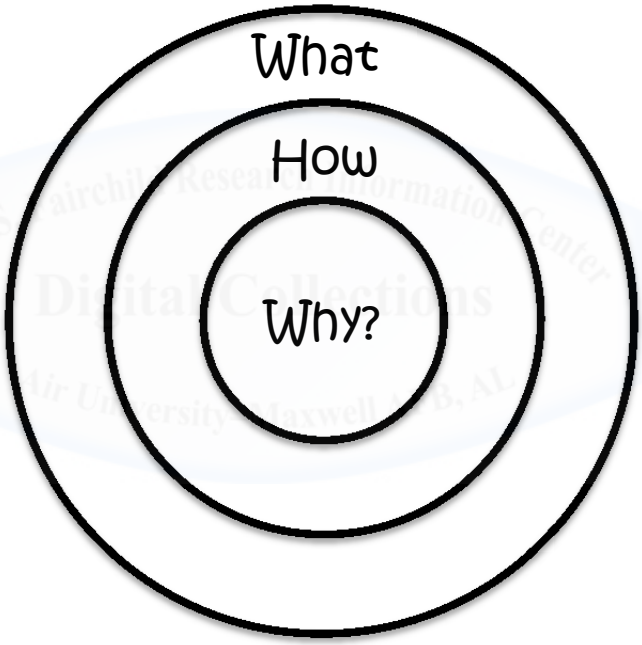

Figure 1: Sinek's Golden Circle

Source: Author's illustration, adapted from Sinek, *Start with Why: How Great Leaders Inspire Everyone to Take Action* (New York: Portfolio, 2009), 37.

The analysis that follows employs Sinek's Golden Circle structure to continue the development of a strategy for communications and

[1] Sinek's book also appeared on the 2012 Chief of Staff of the Air Force reading list. Simon Sinek, *Start with Why: How Great Leaders Inspire Everyone to Take Action* (New York: Portfolio, 2009), 37–39.

cyberspace support in a challenged environment; starting with why, moving to how, and concluding with what. It begins with the question: Why does the Air Force need communications and cyberspace support?

Next, this chapter seeks to determine a method of how the Air Force should provide reliable and responsive air base communications. It introduces agency theory for analyzing relationships among organizations and uses it to analyze the history of communications presented in the previous chapter.

It then discusses the current Air Force network, or AFNET, organizational structure and uses agency theory to analyze the structure to identify potential problem areas. This analysis reveals a three pillar *guiding policy*.

Finally, this chapter seeks to answer the question of what should the Air Force do to provide responsive communications and cyberspace support to its air bases in the future and completes the strategy by identifying two *coherent actions* the service can take to best posture for the future.

Why?

Why does the Air Force need communications and cyberspace support? Why should the Air Force conduct cyberspace operations? In particular, why should the Air Force conduct defensive cyberspace operations and Department of Defense Information Network (DODIN) Operations? Asking these questions may seem like an unnecessary exercise, but they will help expose key ideas in how the Air Force should provide communications and cyberspace support to its force and what a strategy for responsive air base communications and cyberspace support should look like.

For the Air Force, communications and operations in cyberspace must focus on the conduct of its mission, to "fly, fight and win … in air,

space and cyberspace."[2] In other words, the Air Force's defensive and operational actions in cyberspace exist to support operations in all three domains and this support manifests in the form of support to operational commanders. The origin of this answer stems from the links between policy, war, command, information, and the means necessary to exercise command.

When answering the "why" question, it is important to begin with the nature of war and its political purpose. In characterizing the nature of war, celebrated Prussian military theorist, Carl von Clausewitz, makes the connection between military operations and the political purposes they must meet. For Clausewitz, "no one starts a war … without first being clear in his mind what he intends to achieve by that war and how he intends to conduct it. The former is its political purpose; the latter its operational objective."[3] If a nation chooses war as its policy, it must have the means of military power to pursue it.

Modern military power is not only a function of population, wealth, technology, and industrial base; at all levels of war military power depends on the ability to employ forces, through command, in the pursuit of political objectives. Military historian and theorist Martin van Creveld, in his book *Command in War*, makes the link between military power and the ability to implement and exert command.

His study looks at the historical evolution of the modern day concept of command, control, and communications, or C3.[4] Van Creveld defines command as a "function that has to be exercised more or less continuously, if the army is to exist and to operate" and emphasizes, "the extraordinary importance of command," which "few other functions

---

[2] "About the Air Force: Our Mission - Airforce.com," accessed March 21, 2014, http://www.airforce.com/learn-about/our-mission/.
[3] Carl von Clausewitz, *On War* (Princeton, N.J: Princeton University Press, 1976), 579.
[4] Van Creveld uses the term command to represent the modern day command, control, communications, or C3, concept. Martin Van Creveld, *Command in War* (Cambridge (Mass.); London: Harvard University Press, 1985), 1.

carried out by, or inside, the armed forces are as important."[5] In addition, the importance of the role of command in military power is proportional to the complexity and sophistication of a nation's armed forces. The more advanced a military force, the more dependent it is on effective command.[6]

There is debate among the most prominent theoretical literature over the role of information in effective command. Clausewitz emphasizes the cognitive gifts of the commander in his notion of military genius, while discounting largely the value of information as "unreliable and transient."[7] Conversely, Sun Tzu underscores the value of information to a commander in his oft quoted statement, "know the enemy, know yourself; your victory will never be endangered."[8]

Van Creveld's analysis is able to account for modern reality and strike a balance, recognizing the commander's inherent need for information as well as the difficulties in obtaining and managing the right information. He frames the nature of command as "an endless quest for certainty," and ties the amount of information needed to the complexity of the task; the more complex the task, the more information is required to execute it with satisfaction.[9]

Appreciating van Creveld's conclusion, what can one say about the relationship between information and command in a networked world? In a sense, information and the ability to use it is the essence of effective command. Notwithstanding Clausewitz's lack of trust in the intelligence capabilities of his day, his concept of military genius illustrates the need for understanding in command.

---

[5] Van Creveld, *Command in War*, 5.
[6] Van Creveld, *Command in War*, 6.
[7] Clausewitz, *On War*, 100, 117.
[8] Sun Tzu, *The Illustrated Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 2005), 205.
[9] Van Creveld, *Command in War*, 264–265.

Sun Tzu's dictum on knowledge of one's self and the enemy echoes this same sentiment. Whether an individual commander possessed military genius or simply developed an efficient means of coping with information, some of the most successful commanders in history are renowned for their ability to reduce uncertainty through the management of information. Napoleon and the directed telescope, and von Moltke with the telegraph and the general staff are two prominent examples of effective control and management of information.

The pursuit of certainty prevails in current military doctrine and in the procurement of weapon systems. Joint Publication 3-0 uses operational art to describe the concept for commanders to "overcome the ambiguity and uncertainty of a complex environment and understand the problem at hand."[10]

Modern day command and control systems like the AN/USQ-163 Falconer Weapon System, at a cost of $60 million, created "the most advanced operations center in history," requiring "hundreds of people, working in satellite communications, imagery analysis, network design, computer programming, radio systems, systems administration and many other fields."[11] Genius or not, it is natural for commanders to strive to reduce the friction of war through the power of information.

Why does the Air Force need communications and cyberspace support? In the joint community "the communications system is the JFC's [joint force commander] principal tool to collect, transport, process, protect, and disseminate information."[12] In other words, communications and cyberspace support help the commander manage

---

[10] "Joint Publication 3-30: Command and Control of Joint Air Operations," II–3.
[11] "Combined Air and Space Operations Center (CAOC) Fact Sheet" (U.S. Air Forces Central Command, February 6, 2011), http://www.afcent.af.mil/library/factsheets/factsheet.asp?id=12152.
[12] "Joint Publication 6-0: Joint Communications System" (Office of the Chairman of the Joint Chiefs of Staff, June 10, 2010), I–3, http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

and distribute information in order to exercise command. For an Air Force air base commander a significant means of exercising this authority and the unit's mission is through employment of responsive air base communications and cyberspace support. Much of this capability today is provided through the AFNET enterprise, which will come into focus later in this chapter.

In summary, Clausewitz, Sun Tzu, and van Creveld's ideas help demonstrate the origins of the Air Force's need for communications and cyberspace support. This need originates in its commanders' ability to process and disseminate information. In short, the Air Force needs communications and cyberspace support in order for its commanders to exercise command and conduct military operations.

How to do it?

If the Air Force utilizes communications and cyberspace support to enable commanders in air, space, and cyberspace, then how should it go about doing this? To find the answer to this question, the analysis in this section turns to economics and agency theory to explain reasoning. It will employ this logic in examining the history of Air Force communications discussed in chapter two. It will then describe the current organizational structure the Air Force uses to operate its enterprise network, expose some of the tensions this structure causes for supported air bases, and employ agency theory as a framework to analyze those tensions. Finally, it identifies three pillars to construct a strategy for the future.

Agency Theory

Agency theory is a powerful tool for explaining and predicting organizational behavior. It helps reveal rational interests and behavior across a diverse set of disciplines such as political science, history, and business. While far from perfect, it emphasizes strategic interaction and

punishment by shedding light on the incentives and disincentives that drive both individual and organizational decisions. Its applicability is vast, helping to comprehend relationships between the legislative and executive branches of government and the federal bureaucracy and to explain rationale behind simple business transactions.[13] Agency theory is characterized by the assignment of principal and agent roles to relevant actors, as well as identifying the need to monitor behavior and punish or incentivize that behavior.

Agency theory centers on the framework of the principal-agent relationship. In this model, the principal is the party requesting or requiring a service provided by a contracted agent. The theory assumes an agent chooses to act rationally and in its own best interest, which may or may not be in the interest of the principal.[14] The theory uses the terms working and shirking to describe this behavior relative to the performance of the contract. An agent works perfectly when it does what the principal contracts it to do according to the desires and intentions of the principal. The agent engages in some degree of shirking as it deviates from this.[15]

Asymmetric information is a tension point in this framework. Both principal and agent share common information. They also each hold access to their own information and can choose whether to share this with the other party. Because the theory assumes the agent is inclined to act in its own best interest, it is likely to withhold unflattering information from the principal.[16] Therefore, in an efficient relationship,

---

[13] Peter Feaver, *Armed Servants: Agency, Oversight, and Civil-Military Relations* (Cambridge, Mass.; London: Harvard University Press, 2005), 55.
[14] Jurgen Brauer and Hubert P. Van Tuyll, *Castles, Battles, & Bombs: How Economics Explains Military History* (Chicago: University of Chicago Press, 2008), 84.
[15] The author recognizes the terms work and shirk can portray unflattering connotations of laziness, negligence, and even deceit. This is not the intention. The terms are used in accordance with their definitions in economics literature and in Feaver's model. Feaver, *Armed Servants*, 68.
[16] Feaver, *Armed Servants,* 71.

the principal must be able to observe the agent's performance in order to ensure the agent meets the standards set forth in the contract.[17]

Peter Feaver's application of agency theory to explain civilian-military relations highlights another key aspect to the framework: punishment. He cites two prominent features of analysis in principal-agent literature. One strand emphasizes the value of monitoring and advocates efficiency as a factor of the monitoring scheme. The other suggests monitoring is inefficient by nature and instead recommends aligning the interests of the agent with those of the principal.

Feaver develops a convincing argument for a model that incorporates both features of the principal-agent literature.[18] He emphasizes monitoring and at the same time puts a premium on punishment (or incentives) as method for anticipating working versus shirking behavior.[19] The following equation represents a modified version of Feaver's model that captures the influence of punishment and monitoring:[20]

[17] Brauer and Van Tuyll use the principal-agent problem to explain the dilemma for Italian Renaissance city-states in contracting mercenary armies. City-states were unable to verify the actions of the mercenaries and therefore were at a disadvantage in the relationship. Brauer and Van Tuyll, *Castles, Battles, & Bombs*, 84.
[18] Feaver, *Armed Servants*, 56.
[19] Feaver, *Armed Servants*, 87, 95.
[20] Feaver's model is richer as it characterizes degrees of monitoring as an element of punishment. This interpretation accounts for punishment in its purest sense, as an explicit component of working. Feaver, *Armed Servants*.

f(monitor) x *f(punishment or incentive)* = *P(work or shirk);*

Where:
f(monitor) = the level of monitoring available to the principal
f(punishment) = extent to which the principal is able to punish or incentivize the agent
P(work or shirk) = the probability that an agent works or shirks

The complexity of the relationship increases as the number of actors increases. Douglas Bernheim and Michael Whinston's seminal work on common agency reveals a richer understanding of these relationships. The authors extend the framework to account for multiple principals, each depending upon the services of a common agent. In this scenario, the actions of a common agent affect multiple principals in varying degrees.

Examples of common agency fall into one of two major categories, delegated and intrinsic. Delegated common agency exists when principals voluntarily grant the right to make certain decisions to a single agent. For example, in wholesale merchandise trade, manufacturer agents (common agent) represent the potentially conflicting interests of several manufacturers (principals) in the marketing of certain products.[21] Intrinsic common agency describes a relationship when a group of principals "naturally" endows a common agent with the authority to make decisions on their behalf.

For example in democracies, citizens act as principals to elected government officials (intrinsic common agents). Citizens can choose to either participate in government or become a citizen of another government, but voters "naturally" endow government officials with

[21] B. Douglas Bernhein and Michael D. Whinston, "Common Agency," *Econometrica* 54, no. 4 (July 1986): 923.

particular rights to act on their behalf.[22] Bernheim and Whinston demonstrate the value of cooperation (or in economic terms, collusion) amongst principals in achieving equilibrium or the most efficient collective outcome.[23] When multiple principals cooperate to act as a single entity, the relationship moves from one of common agency toward interactions resembling a bilateral principal-agent relationship. This shift enables collective and more efficient influence over the single agent.

In summary, agency theory provides valuable insight into human and organizational behavior. Its applicability is wide, exists across various fields, and helps identify potential difficulties in interaction between organizational actors. The framework outlined here will help explain tension points in the past and present, and guide us toward a strategy for future Air Force communications.

History

One of the central themes to emerge from the history of Air Force communications in chapter two is centralization. For decades the Air Force wrestled with the benefits of centrally controlled communications versus the benefits of assigning control of the communications mission, resources, and personnel to the operational commanders they supported.

Two of the primary drivers for the dissolution of Air Force Communications Command (AFCC) in 1991 were the perceived lack of responsiveness from the headquarters and the inability of commanders to exert control over communications units. It would be irresponsible to not consider these reasons in developing a strategy for communications in the future.

The dual-hat nature of the AFCC command structure proved problematic. The AFCC headquarters exercised administrative control over communications commanders at the division, group, and squadron

[22] Bernhein and Whinston, "Common Agency," 924.
[23] Bernhein and Whinston, "Common Agency," 941.

levels, while operational commanders at the major command and wing levels directed day-to-day operations. In theory, this relationship looked promising, but in practice, it created a tension between the needs of the operational commander and the needs of the AFCC.[24]

In agency theory terms, the AFCC model forced a local base communications unit into the role of an intrinsic common agent, with AFCC and the supported operational wing acting as competing principals over a naturally endowed common agent in the base communications unit (see figure 2). AFCC's administrative control over the local communications unit empowered it with a high level of punishment ability (AFCC was responsible for the communications squadron commander's resourcing).

However, AFCC lacked monitoring capabilities because of its geographic separation from the local communications unit. The operational wings lagged the AFCC in the ability to punish because the command did not evaluate or resource the local communications unit, but the geographic proximity gave the operational wing a higher degree of monitoring capability. Problems arose when the interests of principals collided and they were unable to collaborate or collude on an efficient outcome.[25]

[24] See chapter 2 and Lieutenant General (retired) Robert H. Ludwig, interview.
[25] See Lt Gen (ret) Ludwig's comments in chapter two regarding the "tough position" of the communications squadron commander. His description of the personal computer support center is an example of competing interests.

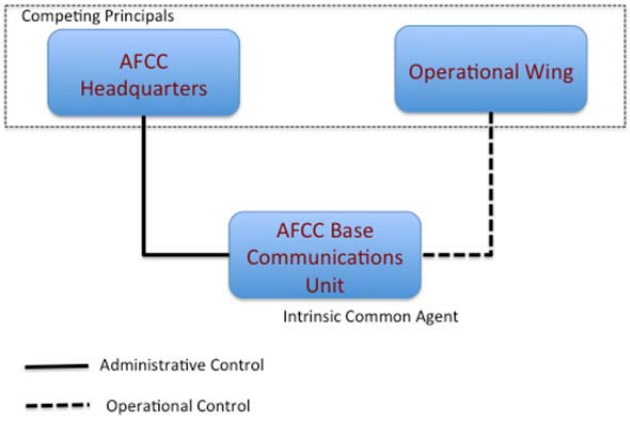

Figure 2: AFCC Model through Principal-Agent Framework
Source: Author's Original Work

As discussed at the beginning of this chapter, communications in military operations exist to support the ability of the operational commander. The commander becomes the rightful principal in a relationship with a supporting agent. This logic drove the Air Force to dissolve the AFCC in 1991 and empower operational commanders with control over their respective communications units. Under this structure, operational commanders possessed both monitoring and punishment functions needed for effective agency. However, old demands of cost efficiencies and standardization coupled with new demands of network security led to a return to centralization of most base communications services.

Today

During the past decade, the Air Force took significant steps to reduce costs and improve the ability to secure and control its networks through centralization of network management functions. This effort culminated in the concept of the Air Force Network, or AFNET, which provides the bulk of communications and cyberspace support services to air bases. Despite the benefits of ease of administration and enhanced

security, the reorganization of forces has put operational wings in a potentially disadvantageous position of having to depend on a centralized organization to provide vital mission enabling capabilities. Agency theory helps reveal tension points in the current AFNET organization model.

Today's AFNET is far more complex than the communications networks operated under the AFCC and the professionalization and centralization of network operations has brought much-needed rigor and discipline to the operation of the AFNET. Today's network is managed by a distributed group of cyberspace units under the purview of the Air Force Space Command (AFSPC), through the 24th Air Force (24 AF) and the 67th Cyberspace Wing. Network operations units such as the 624th Operations Center (624 OC), 26th Network Operations Squadron (26 NOS), 83rd Network Operations Squadron (83 NOS) (Integrated Network Operations Security Centers [I-NOSC] East), the 561st Network Operations Squadron (561 NOS) (I-NOSC West) and the 690th Network Support Squadron (690 NSS) share in network management responsibilities.[26]

Command responsibility for the AFNET derives from the authority of the Commander, AFSPC, who is the Air Force component to United States Strategic Command (USSTRATCOM) for Space and Cyberspace.[27] In addition, the Commander, AFSPC is responsible to "command, control, implement, configure, secure, operate, maintain, sustain, and defend" the Air Force portion of the Global Information Grid.[28]

---

[26] Other units within the 24 AF, such as the 33 NWS and units within the 688th Cyberspace Wing, perform supporting roles in operating the AFNET. However, these squadrons are the primary units that perform network operations and customer support. The "Operating Concept for Air Force Network Increment 1" (Air Force Space Command, June 29, 2010), 4; "Enterprise Service Desk Operating Concept" (Air Force Space Command, February 5, 2013), 39.

[27] "Enterprise Service Desk Operating Concept," 23.

[28] The Global Information Grid (GIG) is defined as "the globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters,

The Commander, USSTRATCOM may delegate operational control of assigned forces to subordinate joint and functional commanders, including the sub-unified command, United States Cyber Command (USCYBERCOM). The 24 AF is the AF Component to USCYBERCOM as the component Numbered Air Force, which means the Commander, 24 AF serves as the Commander of Air Force Forces to USCYBERCOM and executes operational tasks as directed.

The Commander, 24 AF is also responsible for performing service specific tasks as directed by the Secretary of the Air Force through the administrative control chain of command. The commander of the 24 AF is the single commander responsible for the overall operation, defense, maintenance and control of the AFNET.[29] Figure 3 illustrates the command relationships in cyberspace that extend to wings that depend on the AFNET for cyberspace support.

policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. (Joint Pub 6-0)" The AFNET is located within the Air Force portion of the GIG. "Air Force Policy Directive 10-17: Cyberspace Operations" (United States Air Force, July 31, 2012), 5, http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afpd10-17/afpd10-17.pdf.

[29] "Enterprise Service Desk Operating Concept," 23.

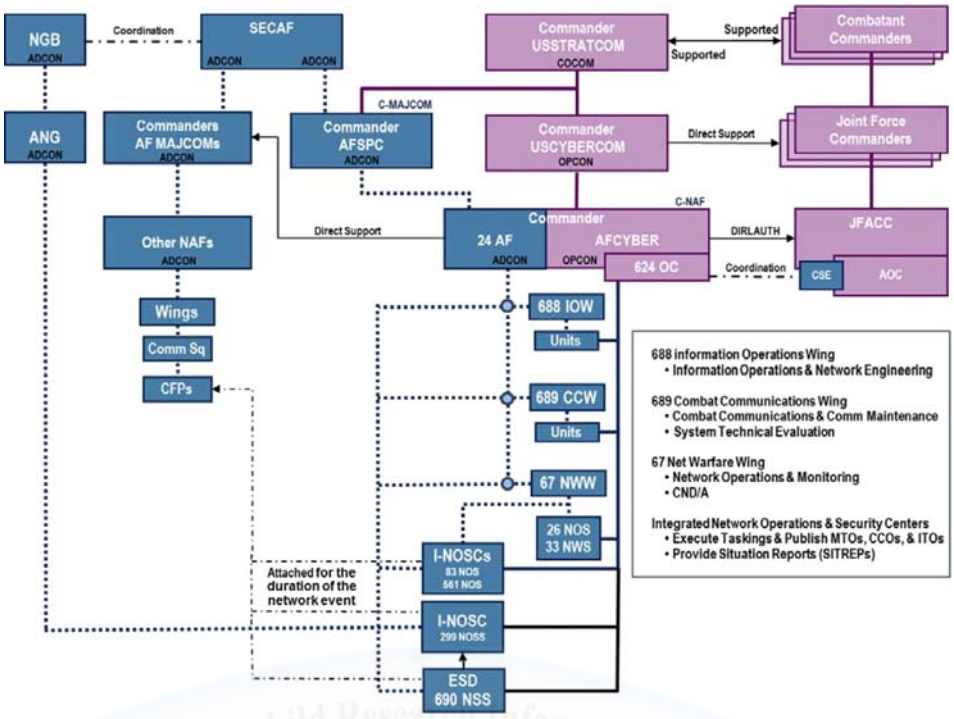

Figure 3: Cyberspace Operations and Support Command Relationships

Source: "Enterprise Service Desk Operating Concept," 24.

Along with the 624 OC, which serves as the 24 AF commander's command and control entity, four squadrons perform the bulk of work to operate, manage and service the AFNET and its users on a day-to-day basis: the 26 NOS, 83 NOS, 561 NOS, and 690 NSS. The 26 NOS manages the Air Force's wide area network portion of the AFNET, including controlling and defending enterprise gateways that connect the AFNET to the outside world as well as the infrastructure that links various air bases into the network.[30]

The 83 NOS and the 561 NOS, as I-NOSC units, manage the network boundaries that connect each Air Force base to the AFNET, controlling and securing network traffic entering and exiting each base in addition to monitoring, assessing, and responding to real-time network

[30] "Operating Concept for Air Force Network Increment 1," 44.

security events. The 83 and 561 NOS also provide air bases with enterprise-level information and communications technology services such as email, collaboration, and data storage.[31]

The 690 NSS operates the Enterprise Service Desk (ESD), an Air Force level helpdesk designed to consolidate and replace similar capabilities previously resident within the base communications squadron.[32] The 690 NSS operates units both inside the continental United States and overseas to provide information and communications technology support to approximately 850,000 users of the AFNET across the globe, 24 hours a day and 365 days a year.[33]

The NOS and NSS units have an important role in interfacing with the air bases supported by the AFNET. These units are responsible to coordinate with the base communications squadron Network Control Centers (NCC) and Communications Focal Points (CFP) to resolve network issues.[34] Much of the base's infrastructure resides on the installation, which is why I-NOSC units depend on and interface with base-level NCCs for touch (physical) maintenance of portions of the network.

In addition, I-NOSC units engage base CFPs to coordinate maintenance activity that affects the service of the base. The NSS utilizes base CFPs to coordinate resolution of end-user issues (in the form of trouble tickets).[35] Figure 4 outlines the tiered enterprise structure currently in place to respond to the needs of individual users at the base level. The AFNET's sheer size, scope, and complexity make

---

[31] "Air Force Cyber Security and Control System Weapon System Fact Sheet" (Air Force Space Command, July 1, 2013), http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=20872.
[32] "Enterprise Service Desk Operating Concept," 1.
[33] "Enterprise Service Desk Operating Concept," 5–6.
[34] "Air Force Cyber Security and Control System Weapon System Fact Sheet"; "Enterprise Service Desk Operating Concept," 17.
[35] "Enterprise Service Desk Operating Concept," 17.

operating it a monumental undertaking, a role that is vital to the success of Air Force operations across the world.

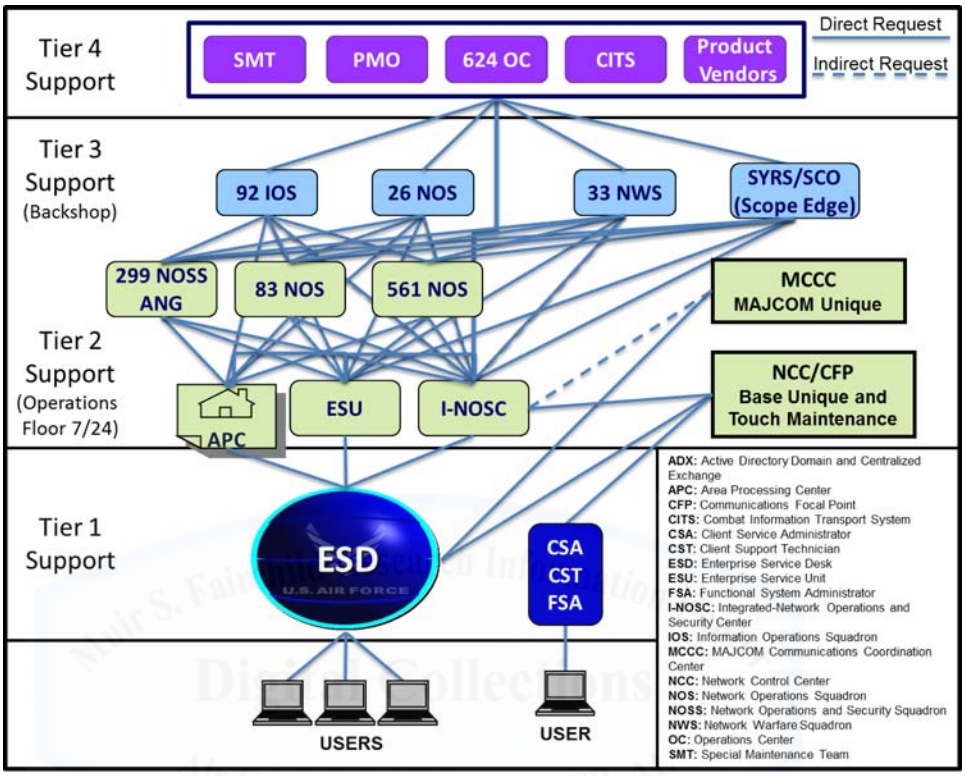

Figure 4: Tiered Operational Support Construct for AFNET user support

Source: "Enterprise Service Desk Operating Concept," 24.

The reliance on a central organization to provide critical capabilities and support can be unsettling at times and the base experience under the current AFNET organizational model is no exception. An online focus group of current base communications squadron commanders revealed the depth of the base's dependence and the tensions associated with centralized management. "We (the air base) are reliant on their (24 AF) support on most (communications) activities," noted one commander. "We (the air base) are almost entirely reliant on their (24 AF) services (to support the wing)," added another.

The participating commanders had an appreciation for the necessity of centralized network operations and for the difficulty in performing those duties. "Understandably, their (24 AF) decisions and actions must be made in the interest of the entire enterprise," acknowledged one commander. However, there was widespread frustration over the base's lack of insight into current AFNET operations and the limited capacity of the AFNET organizational structure to account for individual wing needs. Some believed the organizational structure made it possible for mission assurance of the network to take precedence over mission assurance of a supported wing, when that might not be in the best interest of a supported joint force or operational air commander. "There is no forum currently to exchange information about the wing missions that are supported and to exchange ideas on how to better do so," a commander revealed. Another commander expressed frustration in AFNET directed tasks that lacked insight into the effects on a wing's current missions, sometimes jeopardizing communications during peak flying operations. While some frustration with dependence on a centralized service is normal, the consensus from cyberspace operators at the base level is that there is room for improvement.

Agency theory offers a useful framework for conceptualizing and understanding these tensions and reveals areas for advancement. Since the AFNET now provides much of the capability traditionally provided by the base communications squadron, the units responsible for its operations (the AFNET enterprise) collectively represent an endowed intrinsic common agent. The many bases (or principals) that depend on the AFNET "naturally" endow network operations units with the ability to make decisions on their behalf concerning communications and cyberspace support.

In addition, the administrative (AFSPC) and operational (USCYBERCOM) chains of command also act as principals to the AFNET enterprise's agency. Figure 5 depicts these relationships graphically.

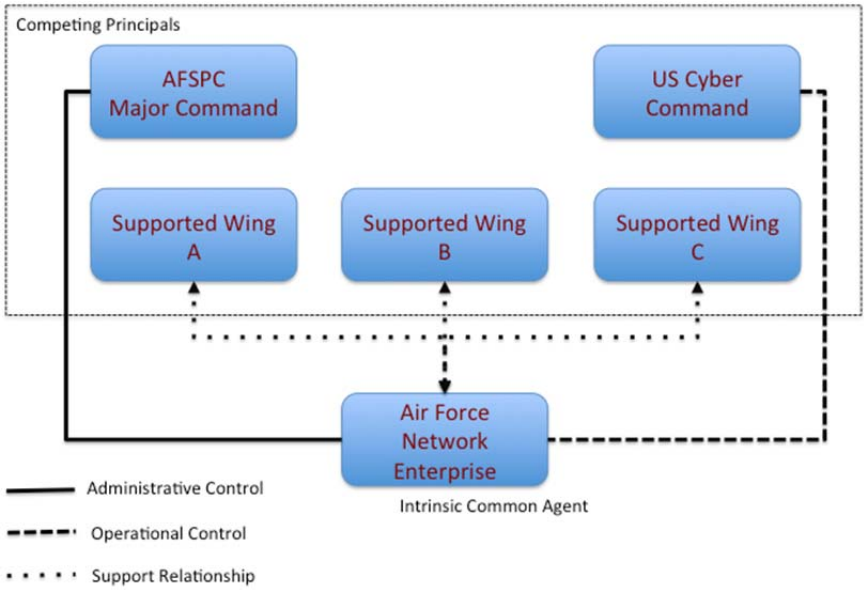

Figure 5: AFNET Model through Principal-Agent Framework

Source: Author's Original Work

Examining the position of each principal relative to the agent explains the nature of the relationships the current structure generates. The AFSPC, with administrative control, possesses a high level to punish and at least a medium level of monitoring capability, accomplished through institutional service command structure.

Similar to the wing with operational control over the base communications unit under the AFCC model, USCYBERCOM retains a high capability to monitor through operational reporting and a common mission of network operations. However, unlike the AFCC model, USCYBERCOM's ability to punish is also significant because the 24 AF operates the AFNET and serves as a component to USCYBERCOM. As a sub-unified command under USSTRATCOM, USCYBERCOM issues legally binding orders for the operation and defense of the network.[36]

[36] "Operating Concept for the Air Force Cyberspace Operations Center" (Air Force Space Command, October 5, 2011), 21.

The supported air base, acting as a principal, clearly lacks both the ability to punish and the ability to monitor the agent. The base, through its communications squadron, possesses limited insight into the daily workings of the AFNET enterprise and therefore lacks the ability to monitor its agent.

Since the preponderance of the air base's communications and cyberspace support capabilities come from the AFNET enterprise and not the base communications squadron, the base also lacks the ability to punish. The only recourse for a base dissatisfied with the level of service it receives from the enterprise is to begin peer engagement at the wing commander level and escalate to higher-level commanders as necessary. In addition, the needs of each base are in competition not only with the needs of the administrative and operational chains of command, but also with the needs of every other supported base. This framework illustrates the barriers that pose risk to providing air bases the support they require.

Towards a Strategy

Agency theory, combined with this analysis suggests three key areas for improvement in the AFNET's ability to support the needs of air bases. These areas will form the foundational pillars to a successful strategy that can better deliver responsive communications and cyberspace support to air bases. All three areas concern empowering air base commanders with the abilities needed to thrive in a relationship with a common agent. Feaver surmised the ability of a single principal to exert control over an agent is a function of monitoring and punishment capability.[37]

Bernheim and Whinston argued that when multiple principals are acting on a common agent, the more the relationship resembles a

[37] Feaver, *Armed Servants*.

bilateral principal-agent framework, the more efficient the outcome for the group.[38] This analysis shapes the strategy's *guiding policy*, which takes form in three pillars.

First, air base commanders must have the ability to monitor the agent. The base commander's primary means of interfacing with and monitoring the AFNET is through the base communications squadron. This section noted earlier that the frustration of those charged with this responsibility in the wing's lack of situational awareness. Increasing the wing's awareness of the status of the network and, just as importantly, increasing the AFNET's awareness of the wing's operations will reduce some of the fog and friction generated by the current organizational structure.

Second, air base commanders must have at least some ability to punish the agent. Even with tremendous monitoring capability, a principal is still helpless without the capacity to influence through punishment. This was the case under the AFCC structure, where the base commander's lack of control over the communications squadron led to the command's dissolution. A base commander can only punish entities under its purview, such as the base communications squadron, and not its supporting communications provider. In the Air Force, a base cannot cancel its subscription to the AFNET and the services it provides.

Third, air base commanders must be able to collude with one another and with other principals. Bernheim and Whinston's analysis is compelling and offers a helpful lens for today's AFNET organizational structure. When principals have the opportunity to collude, or better yet cooperate, they are able to achieve the most efficient outcome for the group. It is tempting to omit this component when designing a centralized support organization, but its net effect could provide

[38] Bernhein and Whinston, "Common Agency."

significant returns and go a long way in satisfying the needs of as much of the operational community as possible.

Summary

This section identified how the Air Force can best provide responsive air base communications and cyberspace support. It introduced agency theory as a method for analyzing motivations and incentives among organizations. It then analyzed the history presented in chapter two in terms of agency theory to reveal tension points that could inform a future strategy. Next, it presented the current model with which the Air Force provides air base communications and used agency theory to analyze potential pitfalls with its structure. Finally, it introduced three pillars for building a strategy for reliable and responsive air base communications. The next section uses these pillars to identify the *coherent actions* necessary in such a strategy.

What to do?

The first section of this chapter answered the question, "why does the Air Force need communications," with an analysis that tied the purpose of providing communications and cyberspace support to a commander's ability to exercise command.

The second section introduced agency theory and used it answer the question of how the Air Force can best provide communications and cyberspace support to its force. In doing so, it identified a *guiding policy* consisting of three pillars with which to construct a strategy for air base communications and cyberspace support, empowering commanders with capabilities to monitor, punish, and collude.

This section seeks to determine what the Air Force can do and what *coherent actions* it can take to provide responsive air base communications and cyberspace support. The three pillars guide this

simple strategy and drive two strategic actions or focus areas: partnership and ownership.

First, the Air Force must embed representation and partnership from supported wings into the AFNET structure. This action supports two of the three pillars: monitoring and collusion. Supporting the first pillar, it empowers the wings with the ability to monitor the performance of the AFNET enterprise against the needs of the wing. This is supposed to be the role of the base communications squadron, but continued frustration suggests that this structure could improve.

In addition to the access provided to the base communications squadron, the AFNET should accommodate base operational liaison teams (BOLTs) that belong to the supported wing, are familiar with its mission and current operations, and possess a background in network operations. These teams, geographically co-located and partnered with key AFNET operational units like the servicing network operations squadrons, would represent a base commander on network operations issues, serving as a monitoring and coordination capability for the base much like liaisons from ground, maritime, and special operations components do inside Air Operations Centers.[39] This action will also provide network operations units with the critical situational awareness needed to make sound decisions in times of normal operations and in times of crisis.

In addition to empowering commanders with the ability to monitor, embedded representation also offers an opportunity for collusion and cooperation among supported entities. This allows the AFNET and its supported bases to analyze collectively tactical and operational trade-offs, with the goal of producing the most efficient outcome for the AFNET and the collective missions it supports.

[39] Liaison roles within the Air Operations Center are covered in, "Joint Publication 3-30: Command and Control of Joint Air Operations," II–21.

The act of embedding base representation into the AFNET with the expectation that it produces meaningful improvement may be an overly optimistic view to some. This is a worthy concern because this action is based largely on theoretical principles that are just that, theoretical. However, this endeavor adds new informational and cognitive insight into network operations; insight that is not accessible in the current organizational structure. This action deserves consideration if for no other reasons than access and the ability to leverage information previously unavailable for decisions.

In the second strategic action, the Air Force must shift at least partial ownership of the AFNET to the units it supports. This action empowers the supported base with some ability to punish its agent. On the surface, this move may seem draconian to some, but upon closer examination, it also deserves serious consideration. The Air Force possesses a tremendous amount of underutilized network operations talent at the base level. The Air Force removed much of this talent during personnel cuts under Program Budget Decision 720. Yet some of it remains.

Skill sets similar to those that exist at the network operations units also exist within the base communications squadron. However, those technicians have limited authority and permissions to shape the network. In addition to the industry standards directed by the Department of the Defense through its 8570 directive, the Air Force has invested in a robust and disciplined training program for its cyberspace operations and support personnel.[40] The talent exists and is available.

A similar effort is already underway in a limited manner through the Federated Enterprise Administrative Rights program that provides regulated administrative rights base communications personnel to give

[40] "Deperatment of Defense Directive 8570.1: Information Assurance Training, Certification, and Workforce Management" (Department of Defense, August 15, 2004).

bases more control.[41] An expansion of this effort offers bases greater flexibility to operate some capabilities during a crisis where the AFNET enterprise was either task saturated or an individual base with servers and services geographically co-located was otherwise isolated.

In addition, divesture of the user support responsibilities and resources from the ESD to local bases further enhances the base's stake in the AFNET. This move would also free the AFNET organizations to concentrate more efforts on defensive cyberspace operations and DODIN operations versus the customer support operations of the ESD.

This strategy aims to ease the tension points that exist in today's AFNET organizational structure. These actions identify two areas where the Air Force should focus on change; both involve better integration of air bases into the AFNET enterprise. The author acknowledges there will be tactical hurdles in the implementation of such a strategy, but these should not deter leaders from taking bold action where necessary in the name of improved service to air bases.

Conclusion

This chapter followed the structure of Sinek's Golden Circle in developing a strategy for communications and cyberspace support; starting with why, moving to how, and concluding with what. First, it articulated why the Air Force needs communications and cyberspace support. It linked the need for communications and cyberspace support to the needs of the commander, military power, and the policy it ultimately supports.

Next, this chapter sought to determine a method of how the Air Force should provide reliable and responsive air base communications and cyberspace support. It introduced agency theory as an instrument for understanding relationships between supporting and supported

[41] Stratton, "Cyberspace Support as a Strategic Vulnerability of USAF Operational Wings," 21, 40.

organizations. Feaver's work highlighted the value of concepts such as monitoring and punishment in principal-agent relationships, while Bernheim and Whinston's analysis highlighted the value of collusion amongst multiple principals in a relationship with a common agent.

This framework helped evaluate the centralized Air Force communications organizational structure discussed in Chapter 2 as well as the current AFNET enterprise centralized organizational structure. Feaver, Bernheim and Whinston's works helped identify three potential tension areas that inform a *guiding policy* for the new strategy for communications and cyberspace support. The first and second pillars assert that commanders (acting as principals) must be able to monitor and punish (or incentivize) the common agent. The third pillar states that competing principals must be able to collude with one another in the hopes of achieving an efficient outcome.

Finally, this chapter sought to answer the question of what should the Air Force do to provide reliable and responsive air base communications and cyberspace support. It presented two *coherent actions* the Air Force can implement to strengthen the future of communications and cyberspace support to its air bases. This two-pronged strategy focuses on partnership and ownership and aims to place information, understanding, and influence in places where it does not currently exist. Embedding wing representation inside the AFNET organization structure creates opportunity for collaboration and cooperation among the diverse set of missions dependent upon the AFNET. Transferring partial ownership of the AFNET to the units that use it, gives each base a stake in its success.

The communications and cyber space operations community has come a long way and made much progress since its origins in the U.S. Army Air Corps. It is the author's hope that the strategy presented here helps continue that progress. The next chapter aims to test and demonstrate this strategy in action.

Chapter 4

Case Studies

The Air Force … needs to think about how to carry out its mission in the event that some cyber attacks do, in fact, succeed.

Dr. Martin Libicki
Senior Management Scientist
RAND Corporation

and

Lt Gen (ret) Robert Elder, USAF
Research Professor
George Mason University

Keeping an enterprise network of any size safe, secure, and available is an incredible challenge for any organization. When one considers the enormous size and scope of the Air Force Network (AFNET) and the operations it must support, that challenge appears even more daunting. The communications and cyberspace support strategy presented in chapter three aims to add to the significant progress the Air Force has made in operationalizing its network by enhancing the responsiveness and resiliency of the capabilities it provides.

A good strategy must be able to perform under both typical and stressed conditions. The aim of this chapter is to test the air base communications and cyberspace support strategy put forth in chapter three with conditions it could likely face in the future. This chapter begins with an overview of the case study approach and then presents two case studies to test the strategy. The first case study considers how the strategy responds during normal operational conditions. The second case intends to put the strategy under significant stress to determine

strengths and weaknesses. Finally, the chapter concludes with a summary of the analysis gleaned from each case.

Approach

A methodical approach is important to this study. This section details the chapter's case study approach. It restates the strategy presented in chapter three and presents the logic, limitations, and outline of the case studies considered. The section concludes with a brief review of relevant military strategy and doctrine, cyber security literature, and history of cyberspace conflict that will inform the construction of each case.

Chapter three introduced a strategy that aims to supplement the current AFNET organizational model and consists of two *coherent action*s. The first action is the addition of base operational liaison teams (BOLTs) geographically co-located with the Network Operations Squadrons (NOS) that support their respective bases. The intent of the teams is to embed representation and partnership from supported bases into the AFNET operational structure, giving bases a voice in prioritizing network activities and arming AFNET decision makers with critical information about the operations they support.

The second action involves shifting more network administration rights from the NOS units to the base communications squadrons. This division of labor not only allows bases to possess a greater stake in the operation of the network it relies upon, but it also offers greater force capacity during times of crisis. The strategy is simple and logically developed, but it must be able to add value to the current organizational structure. The cases presented here aim to determine its value.

This chapter tests the strategy against two scenarios. As mentioned above, the first is a demanding, but normal operational scenario. The second case emulates an advanced and sophisticated cyber threat environment designed to cloud and disrupt the conduct of a

base's operations during a military conflict. The author chose these scenarios because they offer insight into the strategy's value in moderate and stressed conditions. As the strategy succeeds or falters under either scenario, the studies will reveal its strengths and weaknesses.

The author designed both cases to be realistic and plausible, but they are still nonetheless hypothetical. One limit of each case is its hypothetical nature, meaning that the author controls both the stimulus and response throughout each scenario. However, considering the operational sensitivity and classification issues associated with evaluating actual cyber attack scenarios, postures, and responses, this approach is the best available means to test the strategy and demonstrate its coherency. This effort should still reveal useful analysis and insight.

Each scenario includes operational context, plausible threats, and application of the strategy presented in the form of a narrative vignette. Each case concludes with analysis of the strategy's performance. It will assess whether or not, and to what degree, the strategy enhanced responsiveness to the needs of the supported operations and to the reliability for overall network operations.

A brief review of military strategy, doctrine documents, cyber security literature, and an examination of the recent history of cyberspace conflict help to inform the construction of the case studies. The 2011 Department of Defense Strategy for Operating in Cyberspace rightly acknowledges that, "cyber threats to U.S. national security go well beyond military targets and affect all aspects of society."[1] Foreign cyberspace operations targeted against US military, government, and private sector systems are increasing in quantity and sophistication.[2] While vulnerabilities in cyberspace are not isolated to military targets,

[1] "Department of Defense Strategy for Operating in Cyberspace" (Department of Defense, July 2011), 4, http://www.defense.gov/news/d20110714cyber.pdf.
[2] "Department of Defense Strategy for Operating in Cyberspace," 3.

they represent a significant threat to operations today and in the future. The Chairman of the Joint Chiefs of Staff *Capstone Concept for Joint Operations: Joint Force 2020* document recognizes the future security environment as one where operations in cyberspace "will become both a precursor to and integral part of armed combat in the land, maritime and air domains."[3]

While current joint doctrine for cyberspace operations remains classified, Air Force Doctrine Annex 3-12 acknowledges threats from an array of sources including nation states, transnational actors, criminal organizations, individuals, or small groups.[4] Consistent with the Chairman's Capstone Concept, Air Force doctrine recognizes a significant menace stemming from traditional threats, which concentrate, "against the cyberspace capabilities that enable our air, land, maritime, special operations, and space forces and are focused to deny the US military freedom of action and use of cyberspace."[5] The criticality of the cyberspace domain creates many new and unique challenges to cyberspace operators, but it also enhances traditional challenges to military operators across the range of military operations.

In addition to considering military strategy and doctrine, it is also important to consider the existing cyberspace security literature in order to inform realistic case studies. There is debate in contemporary literature about the classification and meaning of conflict in cyberspace. One school of thought, best represented in the writings of Richard

---

[3] "Capstone Concept for Joint Operations: Joint Force 2020" (Office of the Chairman of the Joint Chiefs of Staff, September 10, 2012), 2.
[4] "Compendium of Key Joint Doctrine Publications" (Office of the Chairman of the Joint Chiefs of Staff, January 3, 2014), http://www.dtic.mil/doctrine/new_pubs/compendium.pdf; "Air Force Doctrine Annex 3-12: Cyberspace Operations" (United States Air Force, November 30, 2011), 13–14, https://doctrine.af.mil/download.jsp?filename=3-12-Annex-CYBERSPACE-OPS.pdf.
[5] "Air Force Doctrine Annex 3-12: Cyberspace Operations," 15.

Clarke, asserts that, "cyber war has (already) begun" and that "nations are already 'preparing the battlefield,'" in anticipation of hostilities.[6]

In making an argument for an increased focus on cyberspace security, he presents an Armageddon-like scenario that exposes the vulnerabilities of a networked and sophisticated nation like the United States.[7] Clarke describes networks as a place where militaries can fight, steal information, transfer money, spill oil, release gas, cause generators to explode, derail trains, make airplanes fall from the sky, send a platoon into a waiting ambush or cause a weapon to detonate in the wrong place.[8] Finally, he asserts that hostile actions between states in cyberspace could escalate to the use of conventional force and, conversely, the use of conventional force could generate a response with actions predominately conducted in cyberspace.[9]

In contrast to Clarke's analysis of conflict in cyberspace, Thomas Rid emphatically argues, "cyber war has never happened in the past, it does not occur in the present, and it is highly unlikely that it will disturb our future."[10] His argument focuses on the Clausewitzian idea of war, with its unchanging violent, instrumental, and political nature. Rid rationalizes that since no cyber attack has met or is likely to meet all of these criteria, that actions conducted in cyberspace, cannot by themselves be considered war.[11]

---

[6] 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: Ecco, 2010), 31.
[7] Clarke and Knake, *Cyber War*, 64–68.
[8] Clarke and Knake, *Cyber War*, 70.
[9] Richard A. Clarke, "Cyber Attacks Can Spark Real Wars," *Wall Street Journal*, February 16, 2012, sec. Opinion, http://online.wsj.com/news/articles/SB10001424052970204883304577219543897943980.
[10] Thomas Rid, *Cyber War Will Not Take Place* (Oxford ; New York: Oxford University Press, 2013), xiv.
[11] Rid, *Cyber War Will Not Take Place*, 1–4.

Instead, he classifies aggressive actions in cyberspace into three categories: subversion, espionage, and sabotage.[12] Rid goes further, arguing that because cyberspace offers opportunities in these three categories that were once restricted to physical actions, political violence is likely to diminish rather than increase due to cyber attacks.[13]

Despite the polarity between the characterizations of aggressive behavior in cyberspace that Clarke and Rid represent, there is consensus that cyberspace represents a significant area of competition in national security. Specifically, experts see operations in cyberspace as critical to current and future military operations. "It goes without saying that subversion, espionage, and sabotage—digitally facilitated or not—may accompany military operations," Rid acknowledges.[14]

The nation state is still the most capable adversary in cyberspace. Steven Bucci points out that nation states can "marshal the intellectual capital of their countries to develop cyber armies composed of large numbers of operators with the best equipment, skilled at developing and using new forms of attack."[15] This threat, coupled with the military's dependence on cyberspace capabilities, makes the US Air Force vulnerable to aggressive cyber attacks in both conjunction with and independent of kinetic operations.

The history of conflict and competition in cyberspace is a short one, but it is nevertheless important to look at the available record in order to construct strong case studies. Cyber attacks in Estonia in 2007, Georgia in 2008, and in the Ukraine in 2014 offer insight to the advantages and limitations to conducting operations in cyberspace.

---

[12] Rid, *Cyber War Will Not Take Place*, 10.
[13] Rid, *Cyber War Will Not Take Place*, xiv.
[14] Rid, *Cyber War Will Not Take Place*, 10.
[15] Steven Bucci, "Joining Cybercrime and Cyberterrorism: A Likely Scenario," in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 61.

On April 27, 2007, after the controversial removal of a Red Army War Memorial in the center of its capital city, the tiny Eastern European nation of Estonia experienced a severe round of cyber attacks, including distributed denial of service attacks, colossal email spam, domain name system (DNS) server attacks, and website defacement.[16] Evidence linked the attacks to Russian sources, but it was unable to link the Russian government conclusively to a direct role in the assault.

Still, Estonian officials had minimal reservations in assigning at least some blame toward the Russian government.[17] While the attacks did cause damage, including the loss of services for government, communication, and banking, overall they only had a mild effect on Estonian society.[18] However, the Estonia cyber attacks are widely considered a groundbreaking event in the context of national security because they illustrate how the use of cyberspace operations can be a tool in international conflict.[19]

In contrast to the Estonian experience, the cyberspace operations witnessed in the Georgia-Russian conflict in 2008 were significant because they integrated cyber attacks with the deployment of Russian military forces across a sophisticated campaign.[20] Prior to and during the Russian military campaign into South Ossetia, cyber attacks targeted Georgian civilian and government infrastructure in order to deny and degrade communications systems.[21] In addition, aggressive actors attempted to use cyberspace to influence international opinion by

---

[16] Andreas Schmidt, "The Estonian Cyberattacks," in *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, ed. Jason Healey (Vienna, Virginia: Cyber Conflict Studies Association, 2013), 174–176.
[17] Schmidt, "The Estonian Cyberattacks," 188–191.
[18] Schmidt, "The Estonian Cyberattacks," 186, 191.
[19] Schmidt, "The Estonian Cyberattacks," 191.
[20] Andreas Hagen, "The Russo-Georgian War 2008," in *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, ed. Jason Healey (Vienna, Virginia: Cyber Conflict Studies Association, 2013), 194.
[21] Hagen, "The Russo-Georgian War 2008," 196.

manipulating online quick-vote polls on websites like cnn.com while blocking access to international media inside Georgia.[22] Like the events in Estonia, conclusively linking the events to the Russian government has been problematic. Still, the evidence of attacks originating from within Russia coupled with the near simultaneous commencement of aerial bombing raids and cyber attacks is too much for most experts to ignore.[23]

Observers expected to see similar activity amid the recent tensions between the Russian and Ukrainian governments in 2014. However, aside from minor disruptions to communications networks, experts conclude that Russia has remained rather subdued in the realm of cyberspace in Ukraine.[24] The reasons of course are impossible to know, but interesting nonetheless. This history, along with military strategy, doctrine, and prominent cyber security literature will help inform the construction of the following cases.

Case 1 – Normal Operations

The first case seeks to construct a scenario of eventful and demanding, but largely normal operations at a notional Air Force base and in the AFNET. Events are hypothetical of course, but meant to reflect a realistic scenario that a base must be prepared to face. This section presents a narrative of the scenario followed by analysis of the strategy's performance.

Scenario

On January 8, 2015, a nation in the Pacific region hostile to the United States and its allies places its military on an increased alert

[22] Hagen, "The Russo-Georgian War 2008," 198.
[23] Hagen, "The Russo-Georgian War 2008," 203.
[24] Max Strasser, "Why Ukraine Hasn't Sparked a Big Cyberwar, So Far," *Newsweek*, March 18, 2014, http://www.newsweek.com/why-ukraine-hasnt-sparked-big-cyber-war-so-far-232175.

status and begins increasing anti-American rhetoric. The hostile nation launches several unscheduled missile tests the same day. The President issues a statement that "the United States and its allies view these actions as unacceptable and will not stand for reckless behavior spewing across the region." The Secretary of Defense issues warning orders to various units in the US Pacific Command (USPACOM) area of responsibility (AOR) to increase the pace of normal operations and prepare to execute major combat operations if called upon.

Viper Air Base, a small Air Force installation in the USPACOM AOR, hosts an operational F-16C wing. The wing consists of two flying squadrons enabled by the standard contingent of support units, including a base communications squadron. Viper Air Base is unique in that it hosts its own installation processing node (IPN), meaning that much of the installation's data is stored on servers that reside on the base and are managed on a day-to-day basis by a Network Operations Squadron (NOS).[25]

The following day, in response to heightened security and in conjunction with the Secretary's warning order, the Commander, US Strategic Command raises the global Cyber Condition (CYBERCON), a rating that sets the security posture for networks across the military.[26] Later in the day, a squadron of F-22 Raptors receives orders to deploy to the region and to Viper Air Base, a move that requires significant logistical support from various units across the base, in the theater, and in the continental United States. The squadron is scheduled to arrive on January 15th.

---

[25] Data for most Air Force installations resides across several large and geographically separated enterprise data centers. For background on the Air Force and Department of Defense data center architecture see. "Air Force Data Center Strategy" (Air Force Office of Cyberspace Operations, AF A3CS/A6CS, February 25, 2014), 2.

[26] For an explanation of the CYBERCON system see "Chairman of the Joint Chiefs of Staff Manual 6510.01B: Cyber Incident Handling Program" (Office of the Chairman of the Joint Chiefs of Staff, July 10, 2012), G–5, http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf.

The previous week, as part of a routine validation effort, cyber security experts from a global cyber security firm discovered a moderate vulnerability in the operating system of a prominent router deployed widely throughout the Department of Defense Information Network. The manufacturer promptly issued a new version of software to close the vulnerability and US Cyber Command directed an update. After initial testing on January 14th, the 624th Operations Center (624 OC) releases a Time Compliance Network Order (TCNO) directing NOS units to complete the update by January 16th.[27] Testing indicates that NOS units can conduct the updates safely, but with some impact to operations, as services will likely degrade substantially during the change.

BOLT members from bases within the USPACOM AOR review the CCO during its development and initially concur with the order's release. Platforms servicing Viper Air Base are scheduled for updates on January 15th, the day of the Raptor squadron's arrival. Able to understand the network configuration and potential impact of the TCNO, in addition to the intimate knowledge of the base's current operations, the Viper BOLT advocates for completion of the order on a later date.

The BOLT provides the operational justification, with details on the base's anticipated deployment schedule, and recommended alternative times. The 624 OC engages USCYBERCOM for an extension on the mandatory compliance date. USCYBERCOM notes the vulnerability's existence, while intelligence specialists advise the NOS units of potential signatures to monitor that could indicate exploitation of the vulnerability.

---

[27] "TCNOs are orders issued to direct the immediate patching of information systems to mitigate or eliminate exploitation vulnerabilities. These orders have a significant implication if not accomplished in a timely manner." For a description of Air Force cyberspace operations command and control processes see, "Air Force Instruction 10-1701: Command and Control for Cyberspace Operations" (United States Air Force, March 5, 2014), 4, http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-1701/afi10-1701.pdf.

Viper Air Base and other areas of the AOR are re-scheduled accordingly and the update is completed on January 17th.

Beginning January 8th, NOS units detect incremental increases in traffic flow across the AFNET's gateways.[28] The first day traffic increases by 3 percent over normal traffic rates, followed by a 5 percent increase on January 9th and 6 percent by January 10th. The NOS determines that nearly all of the increased traffic originates or terminates from bases in the USPACOM AOR.

BOLTs from the respective bases, with the assistance of cyberspace defense personnel in the base communications squadron at the home installation, begin to assist in the investigation. Familiar with traffic patterns associated to various missions across the base, the BOLTs and base communications squadron personnel engage various units across the base to validate the increase in traffic. The teams are able to correlate some of the traffic increases to base mission data, however both the base and NOS personnel are still uncertain over the increases.

More analysis continues and by January 13th, average traffic flow hovers around 14 percent above normal operating levels, with increased activity flowing across the entire AFNET. Understanding the problem and determining actions to control it now consumes the attention of the NOS and other cyberspace defense units.[29]

In preparation for the arrival of the F-22 squadron at Viper Air Base, the base communications squadron requests several changes to

---

[28] "16 Secure Gateways that link Air Force bases worldwide together into a global, secured AFNET. These Gateways also form the primary interface between each base and the Internet. AF Gateways are the global-level entry points into the AF provisioned portion of the Global Information Grid (GIG). They establish clear boundary protection lines between the AFNET, other DoD networks and commercial internet communications." See "Operating Concept for Air Force Network Increment 1," 1.

[29] This scenario demonstrates the fog associated with discerning normal and abnormal activity on the AFNET. Here, the BOLT's knowledge of network operations and the ability to understand the operations on the base can enhance the NOS's situational awareness.

the information services configuration to support the inbound unit.[30] The request is given a medium priority when it is submitted on January 10th, but the NOS's current workload in this area is substantial due to the increases in operational tempo.

BOLTs representing various bases work together to advise on a collective priority scheme for carrying out the work, but it becomes clear that the changes Viper Air Base requires will not be ready in time. The BOLT advises the NOS to allow the local communications squadron to perform the work. The NOS, now fully informed and aware of the prioritization across the global network and understanding the importance of the needs at Viper Air Base, agrees and directs the base communications squadron network operations personnel to complete the changes on January 11th.

On January 12th, the Viper Air Base wing public affairs officer (PAO) alerts the wing information assurance officer and the communications squadron about suspicious activity on one of the base's social media sites. No information on the site looked out of the ordinary, but an empty post appeared on the account and then mysteriously disappeared. No one in the office had accessed the account at the time of the post; however, given the heightened state of alert at the base, the PAO noticed the blank post and reported it.

The base communications squadron quickly conveyed the information to the BOLT, who relayed the details to other wing representatives and the NOS. After the report from Viper, two other base PAOs in the region found similar activity. Collectively, the BOLTs correlated account management procedures of the offices and discovered that access to both accounts originated from the AFNET. The BOLTs advised the NOS that credentials were likely compromised from an

[30] Common tasks associated with the movement of unit would include the creation of network accounts or movement of data to an installation processing node.

AFNET computer and the NOS launched an investigation that commenced on January 14th.

Analysis

The scenario above offers several opportunities to observe the communications and cyberspace support strategy in action. To determine the strategy's value, it is necessary to examine its ability to enhance responsiveness to the base's mission and the overall operations of the AFNET.

First, the BOLT added significant enhancement to the situational awareness of both the base and the AFNET enterprise. During the decision process to implement the CCO and neutralize the router vulnerability, the BOLT armed the NOS with the insight needed to link the risk to the network to the risk to the base's mission. One could argue that coordination through the normal authorized service interruption (ASI) program offers this insight as well and it is therefore not an enhancement.

However, the BOLT's position inside the centralized AFNET organization structure allows it to offer an independent assessment of the network impact and then tie it to an operational impact at the base. The base communications squadron, as an organization outside the AFNET, does not possess this level of insight. In agency theory terms, this allows the base to monitor the work of the AFNET.

Next, the presence of the BOLTs inside the AFNET organization empowered the bases with the ability to collaborate in advising in decisions. The ability of the BOLTs to communicate and collaborate with one another not only increased the situational awareness of the NOS, it also enabled bases to collaborate with one another on the prioritization of work needed.

Without the presence of BOLTs from the supported bases, the request from Viper Air Base was doomed to enter a cue, likely prioritized

by a person or system without the full information and site picture needed to make the best decision for the supported mission. Again, in agency theory terms, this allowed the BOLTs to collude with one another to determine the best possible outcome for the collective group.

Third, the physical and organizational position of the BOLT adds a valuable cyber security vantage point. In the case of the suspected social media compromise, the position and focus of the Viper BOLT allowed it to share relevant information rapidly with representatives from other bases, who were able to direct personnel at their bases to search for a particular vulnerability. The NOS, with its natural focus on cyber security, is equipped to coordinate this activity as well, however, the ability of BOLT collaboration and coordination allows it to discover and understand the threat much quicker than if this unique vantage point did not exist.

Finally, the ability for NOS personnel to shift overflow work to operators at the base communications squadron significantly enhances the capacity of both cyber security and network operations. Again, without the ability to transition work that requires administrative privileges on the AFNET to base personnel, requests from bases are subject to the NOS's capacity to perform the work.

In addition, it brings ownership of the AFNET back to the base. In this instance, the base commander has the ability to prioritize the work of communications squadron personnel and can prioritize this work, along with the squadron's other work accordingly. This capability strengthens both responsiveness and reliability.

Overall, the strategy appears to perform well in enhancing responsiveness of both the needs of the base and the needs of the AFNET enterprise. It is worth noting that base communications squadron personnel are able to perform some of the BOLT functions depicted in this scenario. However, the BOLT's unique perspective and locations

inside the AFNET organizational structure adds substantial value to both organizations. The next case will test the strategy even further.

Case 2 – Stressed Operations

The second case now seeks to examine how the communications and cyberspace support strategy performs under significant stress. The scenario builds on the one presented in the previous case by introducing hostile cyberspace attacks and actions likely to be directed against air bases during a military conflict. This section begins with a description of events that create the scenario. The author then analyzes these events in terms of the strategy's performance.

Scenario

Amidst rising political tensions in the region and in response to confrontational actions from the hostile nation, the President, in coordination with allies in the region, orders the use of decisive military force. The Air Tasking Order for January 18th assigns combat air missions to units at Viper Air Base. The order scheduled the first jets to launch at 0100 hours on the morning of the 18th. Personnel across the base have been on alert for over a week in anticipation of combat operations. At 0100 local time, units at Viper Air Base commence operations as scheduled.

In the early morning hours of the 18th, operators at NOS units detect a rapid increase in inbound data traffic at the AFNET gateways. At 0500, the Crew Commander at the 26 NOS, with advice and information from experts at other network operations units, makes an assessment that the AFNET is under a distributed denial of service

(DDoS) attack.[31] Traffic into the AFNET grinds to a crawl and renders communication outside the network nearly impossible.

Trouble calls from across the globe inundate the Enterprise Service Desk as Air Force bases everywhere share this experience. Air bases conducting operations in the Pacific are particularly sensitive to this situation not only because of the loss of service, but more importantly, because the massive coordinated effort appears targeted toward air operations in the region.

The Viper Air Base BOLT is able to provide updated analysis to the communications squadron and base leadership. While most of the base's operational and mission critical information is processed over the classified Secure Internet Protocol Router Network (SIPRNET), it depends heavily on the AFNET to process much of its logistics, maintenance, and support information. The Viper Air Base commander issues an order to begin utilization of other means of communication and data processing where possible.[32]

At 1100, the 561 NOS reports that large numbers of servers begin to fail at two core data centers in the continental U.S. The NOS and the Viper Air Base BOLT analyze the impact of the failure as minimal to the

---

[31] DDoS attacks were employed in both Estonia and Georgia. For background on DDoS attacks see, Bucci, "Joining Cybercrime and Cyberterrorism: A Likely Scenario"; While a DDoS attack of a size and scope massive enough to disrupt the entire AFNET would be monumental, it should not be discounted as impossible. A 2013 attack on Spamhaus, an anti-spam company, demonstrates the exponential increase in size and scope possible, noting that attacks, "resulted in a rate of 300 Gbps traffic and nearly took down the Internet Exchange points, which could have brought down the Internet as a whole." Bryan Harris, Eli Konikoff, and Phillip Petersen, "Breaking the DDoS Attack Chain" (Carnegie Mellon University, 2013), http://www.cmu.edu/mits/files/breaking-the-ddos-attack-chain.pdf.

[32] A base's likely alternate methods of communications and data processing would begin with the increased use of higher classification networks such as SIPRNET and JWICS. These networks are generally considered to be more secure due to the fact that they do not connect to the Internet, however their presence across an air base is limited because of the higher measures of physical security required and some units do not have ready access to them.

operations at Viper since the base hosts its own data processing capability on the IPN. The BOLT puts together a hasty preliminary report detailing the events at the two compromised data centers and provides it to the base communications squadron.

At 1200 local time, Viper Air Base begins experiencing problems with all traffic leaving the base. Within the next 20 minutes, the Viper base communications squadron receives notification from the local commercial telecommunications provider that several of their network's key nodes are experiencing problems. In particular, communications nodes servicing the base have started to power down remotely, requiring manual restarting to bring them back online. The company is still trying to determine the scope and source of the issues as the communications connectivity to the base cycles through periods of full functionality, degradation, and complete isolation.[33] Air base personnel continue to attempt to conduct business through the classified networks; however, the use of wireless communications provides some relief by allowing for the exchange of information with entities outside the base.

Later in the afternoon, the NOS and Viper Air Base communications personnel notice symptoms in IPN servers similar to those seen in the core data centers and detailed in the BOLT's preliminary report a few hours earlier. At 1400 local time, platforms in the IPN begin to fail. By 1430, most of the messaging and collaboration data in the IPN has disappeared and the server functionality is severely impaired. Back-up data exists and is unharmed, but the IPN is in need of significant reconstruction. The BOLT consults with network operations personnel at the base and inside the NOS. The NOS assigns

[33] "AFNET Increment 1 … creates base-level diversity by providing two circuits at each base within the AFNET Increment 1 architecture." Local telecommunications service providers typically provide the two (or more) circuits that provide connectivity between each base and the larger network. "Operating Concept for Air Force Network Increment 1," 2.

the rebuilding task to the base communications squadron and its personnel quickly begin work to rebuild the base's information services.

At 1500, personnel in the Viper Air Base command post notice a report on CNN detailing social media and news releases from various military public affairs offices. The reporter runs through several posts and releases that are obviously fraudulent, including one from the Viper Air Base PAO boasting about the unit's responsibility for the destruction of a hospital earlier in the day. The command post alerts the PAO, who is unable to access the base's social media account with the last known password. The USPACOM public affairs office determines that an unknown threat is targeting installations across the theater.[34] Adding to the confusion, reports and transmissions from some entities are accurate and authentic. US media outlets easily detect the discrepancies and are able to filter through to the real information, but foreign news sources are not able to sift through as effectively and continue to report inaccurate information.

The problems in the local commercial telecommunications network continue to plague Viper Air Base. At 1630 local time, the commercial network finally gives in and experiences catastrophic failure in the geographic area surrounding the base. Viper Air Base, now almost in communications isolation, continues to operate with severely degraded communications capabilities, able to utilize only wireless and limited satellite communications for voice and data connectivity. Units at the base still have access to SIPRNET processing capabilities and are able to exchange information locally.

Soon the NOS begins to receive reports of SIPRNET failures from two bases in the USPACOM AOR. Both bases report a near complete loss of data. An initial assessment attributes the failures to a possible zero-

[34] The Russo-Georgian war of 2008 demonstrates that public opinion is a target for cyber operations. The significant number of social and electronic media outlets within the Department of Defense present potential targets for this type of attack.

day exploit lurking on the classified network.[35] The Viper Air Base BOLT passes all available intelligence, including an event log from the targeted bases, to the base communications squadron. At approximately 1745, network operators begin seeing signs of the same attack on the remaining SIPRNET infrastructure at Viper Air Base.

Soon, nearly all of the base's data on the network begins to transform from valuable and meaningful patterns of "0s" and "1s" to a near endless meaningless string of "0s". Fortunately, the base's Top Secret data remains intact, although connectivity to the outside world is still largely unavailable. Network operators at the base shift attention from restoring unclassified AFNET systems in the IPN to restoring the base's SIPRNET.

Although not ideal, the wing confirms the next day's ATO through alternate and rudimentary communications channels.[36] Viper Air Base continues to execute its mission, although severely limited in its ability to process and exchange pertinent data with its headquarters. In short, the base powers through despite the disruption.

The day ends considerably different from how it began. The communications capabilities of Viper Air Base went from substantial to almost irrelevant in less than a day. Significant work lies ahead for the cyber operators at the NOS and in the base communications squadron. Luckily, operators from the base and the NOS have forged a powerful and efficient team, able to use all available skills and manpower to restore vital capabilities to the base.

---

[35] Zero-day exploits increased more from 2012 to 2013 than any other period since 2006. *Internet Security Threat Report 2014* (Mountain View, California: Symantec Corporation, April 2014), 34, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[36] Alternate means of confirmation of the ATO could be the use of tactical satellite radio for secure data, fax, or voice.

Analysis

The nature of the second scenario adds significant fog in the evaluation of the strategy. Although not as clear because of the extreme stress, enhancements and value still emerge in the analysis of these events.

First, the BOLTs continue to enhance situational awareness for the base and the AFNET enterprise, even when threats challenge that awareness significantly. The BOLT's access to information at the NOS allows it to specifically observe activities across the enterprise in the context of how they impact a single installation. This capability does not exist as base communications squadrons lack this insight because of their geographic position and expertise. Naturally, as fog and friction during a conflict increases, this situational awareness deteriorates. However, the capacities to observe, orient, advise on decisions, and monitor actions in the interests of the base's mission simultaneously enrich the operations of the base and the network.

Second, the enhanced administrative rights and cyber operations training of the base communications squadron personnel offer potential value during a crisis. The Viper Air Base case is unique because the base's data resides locally on an IPN. In the case of lost connectivity, the base still has the ability to operate and manage the installation's information. The strategy is more limited in a scenario where a base's data resides at a geographically separated location as part of a cloud-based architecture.[37] In the event of lost connectivity in this scenario, these administrative rights would have little value to the base.[38]

---

[37] As the Air Force transitions to the Joint Information Environment, the cloud architecture expands. However, some IPNs will remain across the service. For more information on the future of the Air Force's data infrastructure see, "Air Force Data Center Strategy."

[38] For more analysis and further implications on the vulnerability of operational wings to a cloud-based data architecture see, Stratton, "Cyberspace Support as a Strategic Vulnerability of USAF Operational Wings," 17–20.

Therefore, the actual value of this aspect of the strategy during a crisis largely depends on the ability of cyber operators at the base to access and control their installation's data infrastructure.

Naturally, as threats challenge operations by adding to the fog and friction of the situation, plans and strategies break down. This strategy is certainly no exception. However, what the strategy does do is place information, understanding, and capability at places where it does not currently exist. For this reason, it certainly deserves consideration.

Conclusion

This chapter tested the communications and cyberspace support strategy presented in chapter three and determined its value under different conditions. It first articulated the approach used to construct the cases, detailing the logic behind the construction of each scenario as well as the limitations of the approach. It briefly reviewed relevant military strategy and doctrine, contemporary cyber security literature, and recent history of cyberspace conflict in order to inform the construction of each case.

The first case presented a demanding, but still normal scenario of events at a notional operational Air Force base. The second scenario added significant stress by integrating defensive cyberspace operations and Department of Defense Information Network operations with traditional combat air operations; highlighting potential crisis bases could face under similar conditions.

The analysis of the two cases indicated that the strategy is useful in enhancing the responsiveness of the AFNET enterprise to the requirements of the base's mission and is worthy of consideration. It experienced limitations under conditions of communications isolation and its overall value in this context was largely dependent upon the data infrastructure used to support a particular base. However, a status quo

strategy would be subject to similar limitations and the strategy offered here succeeds where it would fail or provide a delayed response.

In summary, the case studies depicted here illustrate the potential strengths and pitfalls of the current AFNET organizational model. The strategy put forth in this paper seeks to strengthen the current structure by placing the right information, understanding, and capability in places where it does not currently exist. The next and final chapter offers concluding thoughts as well as implications for the future of information and communications technology services in the Air Force.

Chapter 5

Conclusion

> *The quality of the United States' human capital and knowledge base in both the public and private sectors provides DoD with a strong foundation on which to build current and future cyber capabilities.*
>
> *2011 Department of Defense Strategy for Operating in Cyberspace*

This thesis answers the question of how should the Air Force posture itself to best provide responsive communications and cyberspace support to its air bases in a challenged environment. It does this by introducing a strategy that places information, understanding, and influence at key positions in the service's organizational structure. Following Richard Rumelt's blueprint, it developed a strategy with three core components: "a *diagnosis* of the situation at hand, the creation or identification of a *guiding policy* for dealing with the critical difficulties, and a set of *coherent actions*."[1] The first chapter introduced the research background, definitions, evidence, methodology, scope, and limitations.

To initiate the *diagnosis* of the situation at hand and appreciate the history of how the Air Force has approached communications in the past, chapter two provided a short history of Air Force communications over the past 80 years. Among the stories of sacrifice and ingenuity of communications Airmen, the chapter revealed three themes. The first involves the centralized management of Air Force communications. The second is the dependence of military operations on these capabilities and their integration into operational missions. The third theme is the acquisition, integration, and employment of new technologies and the ability of communications Airmen to apply them in support of airpower.

[1] Rumelt, *Good Strategy, Bad Strategy*, 7.

The third chapter constructed the main argument of the thesis and put forth a strategy for responsive communications and cyberspace support to air bases. It began with a continuation of the *diagnosis* of the situation at hand and concluded by identifying a *guiding policy* and *coherent actions* that form the strategy. The chapter introduced agency theory, an economic theory that explains rational behavior between a principal requiring a service and a contracted agent providing that service. The theory is useful in explaining behavior between individuals and organizations in business, political, and other social sciences. The chapter utilized logic consistent with Peter Feaver's application of the principal-agent model to identify the need for principals to monitor and punish (or incentivize) agent behavior in order to align it with the needs of the principal.

Chapter three examined both the historical communications organizational structure and the current AFNET organizational model to help explain the dissolution of the Air Force Communications Command in 1991 and identify some of the tension points in today's structure. These tension points helped reveal a *guiding policy* consisting of three pillars. The first and second pillars assert that each base commander (acting as a principal) must be able to monitor and punish (or incentivize) its communications and cyberspace support provider (its agent). The third pillar states that base commanders (competing principals) must be able to collude with one another in influencing the agent, with the goal to achieve the most efficient outcome.

The chapter then presented a simple strategy, culminating in two *coherent actions,* for the Air Force to consider. The first action is the introduction of base operational liaison teams (BOLTs), consisting of personnel familiar with network operations and knowledgeable of the base's missions and operations. The teams would be geographically co-located with their respective Network Operations Squadrons (NOS) in

order to provide a crucial operational perspective in the prioritization of missions on the AFNET. The BOLT concept also gives the supported bases better insight into the operations of the AFNET and at the same time allows representatives from various missions the ability to interact with one another in advising and advocating for actions in the AFNET.

The second component of the strategy involves sharing enhanced network administration rights between the NOS units and trained cyberspace support personnel inside the base communications squadrons. This division of labor not only allows bases to possess a greater stake in the operation of the AFNET, but it also offers greater force capacity during times of increased operational tempo and crisis. Overall, the strategy is a simple one and aims to place information, understanding, and influence at places where it does not currently exist.

Finally, the fourth chapter tested and demonstrated the strategy with realistic case studies. The chapter constructed the case studies based on a review of relevant military doctrine, cyber security literature, and notable cyber attacks in Estonia, Georgia, and Ukraine. The first case presented a demanding, but reasonable scenario of likely operations at an air base in the US Pacific Command area of responsibility. The second case built upon the events in the first scenario and added significant stress through the introduction of large-scale cyber attacks in response to the base's combat operations. The strategy performed well in enhancing the responsiveness to the base's needs, especially when compared with the status quo.

One area of concern showed that the success of the second component of the strategy depended largely on the ability of base cyberspace operators to access the base's data infrastructure. When the base lost access to its data, it lost its ability to operate or utilize its information services. Continued Air Force efforts toward the cloud-based data infrastructures in the Joint Information Environment (JIE) could limit the usefulness of this part of the strategy during a catastrophe.

Conclusions

The development of a strategy for air base communications and cyberspace support reveals three noteworthy conclusions. These ideas help answer the central research question: how should the Air Force posture itself to best provide responsive communications and cyberspace support to its air bases in a challenged environment?

The first conclusion to emerge is that airpower demands responsive communications and cyberspace support. History provides excellent examples in Arnold's 1934 flight of B-10s, the Berlin Airlift, and the Air Force's experiences in Korean and Vietnam. Today's sophisticated information and cyber systems that drive the command and control of airpower and its necessary enabling components continue to illustrate that communications, and now cyberspace support, are just as critical today as they were during Arnold's time.

The scenarios presented in chapter four demonstrate just how dependent today's air bases are on communications and cyberspace support capabilities to execute air operations. At the same time, those capabilities are more vulnerable today than at any point in the history of airpower. Today's communications and cyberspace support capabilities need to be both secure and responsive to the needs of the operations they enable.

This leads to the second conclusion that AFNET units must be able to perform two critical functions for airpower. First, the AFNET must be a communications and cyberspace support capability provider for the Air Force. With the creation of the AFNET enterprise, most of the communications and cyberspace support capabilities belonging to air bases were absorbed into the AFNET. This meant that many of the services managed locally, now fell under the control of the 24 AF. However, the demand for these services never waned and in some cases grew stronger.

In addition to being a capability provider, AFNET units must also be able to defend against the serious and diverse threats that exist today. This is no easy task and the scenarios in chapter four illustrate just how vulnerable air operations may be to a determined adversary. However, the DoD, US Cyber Command, Air Force Space Command, and the 24th Air Force have made tremendous strides in this area. While there is always a need for continuous progress and improvement, these organizations have established a strong cyber security culture that the military must have as it moves forward. However, given airpower's dependence on these resources, there must be a balance between security and capability.

This leads to the third and final conclusion, the need for balance. Today's AFNET has a strong (and necessary) security focus, but its organizational structure prevents it from maximizing responsiveness in its role as the Air Force's communications and cyberspace support provider. Agency theory helps explain this predicament. Because of its command structure, the US Cyber Command, with its focus on cyber security and network defense, exerts enormous influence over the operation of the AFNET. This is essential as it drives a strong security focus, but there is always a need for balance between security and capability.

The current AFNET structure provides air bases with too little influence into the decisions that affect the communications and cyberspace support capabilities they depend on for the execution of their missions. Chapter three's description of the AFNET organizational structure and its command relationships, along with the comments from current base communications squadron commanders highlight this issue. The current AFNET structure lacks access to information about the base's day-to-day operations as well as the ability to understand the impact of its decisions and actions on those operations. At the same time, air bases lack the ability to influence the decisions made by AFNET

units. Again, agency theory explains that influence, more than anything else, will establish interests and motivations and drive behavior. If the Air Force desires a balance between security and capability in communications and cyberspace support for its air bases, it must act accordingly.

The strategy presented here is a posture the Air Force can take to achieve this rebalance between security and capability. Its emphasis on liaison elements and the realignment of network operations responsibilities intends to arm AFNET units with the right information, understanding, and influences in order to achieve that balance. It is a simple and practical approach, but one the Air Force must consider as it embarks on major changes to its communications and cyberspace support structure in the Joint Information Environment.

Implications for the Joint Information Environment

This study examined deliberately the current Air Force communications and cyberspace support model. The author acknowledges that many of the specific details used to construct the strategy presented here will soon be outdated, if they are not already. However, the tension points that exist under the current organizational model are likely to persist under the JIE, where cyberspace infrastructure and information services operated at present by the Air Force will be managed at the Department of Defense level.[2] It is the author's hope that some of the ideas presented here can inform strategies to influence the performance and responsiveness of

[2] The JIE incorporates similar consolidation at the DoD level that the AFNET consolidation accomplished at the Air Force level. "The Joint Information Environment will take all of those separate networks and collect them into a shared architecture," with expected "full capability to be realized between 2016 and 2020." Claudette Roulo, "Official Describes Joint Information Environment," *American Forces Press Service*, October 3, 2012, http://www.defense.gov/news/newsarticle.aspx?id=118092.

communications and cyberspace support to Air Force units through the JIE.

Under the JIE structure, control over critical systems and assets will be divested to organizations whose capabilities to understand the complete operational environment are limited.[3] While providing attractive cost savings, the Air Force should also expect a cost in operational responsiveness. The author believes that the application of agency theory and the communications and cyberspace support strategy presented here can still offer solutions. In particular, the *guiding policy* of empowering Air Force operational units with monitoring and punishment (or incentive) capabilities and integrating them into JIE organizations could hedge against likely costs in operational responsiveness. This area will benefit from more study and research.

Concluding Thoughts

At an important crossroads, the US Air Force seeks more efficient ways of doing business, while still providing the key capabilities its sister services, joint partners, and the nation require. A strategy that places information, understanding, and influence in key positions throughout the organization is one humble approach to this challenge. Airmen for nearly a century have represented a culture of innovation, resilience,

[3] The primary means of support to air bases will be provided through "joint (multi-service) organizations that are run by a lead Service or Agency designated in the JIE governance structure," known as Enterprise Operations Centers. The stakes associated with this divestiture are particularly critical to Air Force operations, as opposed to those of the Army or Navy, because the Air Force plans and initiates its operational missions from fixed (not deployed) bases. The JIE offers tactical capabilities for deployed units through a more autonomous Joint Communications Node that, "is a defined set of standards, specifications, and capabilities (transport, systems, security, applications, and services) that can deliver cross-Service JIE capabilities to both commanders and warfighters." In other words, the JCN concept provides operational commanders more control over the services they need. Operational Air Force bases will not have this luxury under the JIE and will depend on a centralized Enterprise Operations Center for support. "Joint Information Environment Operations Concept of Operations" (JIE Operations Sponsor Group, January 25, 2013), 26, 41–42, 80.

creativity, determination, and dedication in response to great challenges. Today's challenges are certainly complex and daunting at the same time, but there is no doubt that Airmen from the cyberspace operations and support communities will continue to innovate and add to this important legacy.

Bibliography

"About the Air Force: Our Mission - Airforce.com." Accessed March 21, 2014. http://www.airforce.com/learn-about/our-mission/.

"Air Force Cyber Security and Control System Weapon System Fact Sheet." Air Force Space Command, July 1, 2013. http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=20872.

"Air Force Data Center Strategy." Air Force Office of Cyberspace Operations, AF A3CS/A6CS, February 25, 2014.

"Air Force Doctrine Annex 3-12: Cyberspace Operations." United States Air Force, November 30, 2011. https://doctrine.af.mil/download.jsp?filename=3-12-Annex-CYBERSPACE-OPS.pdf.

"Air Force Instruction 10-1701: Command and Control for Cyberspace Operations." United States Air Force, March 5, 2014. http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afi10-1701/afi10-1701.pdf.

"Air Force Policy Directive 10-17: Cyberspace Operations." United States Air Force, July 31, 2012. http://static.e-publishing.af.mil/production/1/af_a3_5/publication/afpd10-17/afpd10-17.pdf.

Ball, Gregory W. "A Brief History of the Twenty Fourth Air Force." 24th AF Historian, October 15, 2012. http://www.24af.af.mil/media/document/AFD-131101-082.pdf.

Basla, Michael J. "Toward a Single AFNet: Three Reasons Why the Air Force Must Migrate." *High Frontier*, May 2011.

Bernhein, B. Douglas, and Michael D. Whinston. "Common Agency." *Econometrica* 54, no. 4 (July 1986): 923–42.

Boyce, Betty A., Shelley L. Davis, Laurence B. Epstein, Cora J. Holt, Larry R. Morrison, Daniel R. Mortensen, Thomas S. Snyder, Melinda A. Wigginton, and Tommy R. Young. *The Air Force Communications Command: 1938-1986, An Illustrated History*. Edited by Thomas S Snyder. Revised Edition. Scott AFB, IL: Air Force Communications Command, 1986.

Brauer, Jurgen, and Hubert P. Van Tuyll. *Castles, Battles, & Bombs: How Economics Explains Military History*. Chicago: University of Chicago Press, 2008.

Brown, Nancy E. "Difficulties Encountered as We Evolve the Cyber Landscape for the Military." *High Frontier*, May 2009.

Bucci, Steven. "Joining Cybercrime and Cyberterrorism: A Likely Scenario." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S. Reveron. Washington, DC: Georgetown University Press, 2012.

Cacas, Max. “The Best Laid Plans Fly Awry.” *SIGNAL Magazine*. Accessed January 8, 2014. http://www.afcea.org/content/?q=node/11125.

“Capstone Concept for Joint Operations: Joint Force 2020.” Office of the Chairman of the Joint Chiefs of Staff, September 10, 2012.

“Chairman of the Joint Chiefs of Staff Manual 6510.01B: Cyber Incident Handling Program.” Office of the Chairman of the Joint Chiefs of Staff, July 10, 2012. http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651001.pdf.

Clarke, Richard A. “Cyber Attacks Can Spark Real Wars.” *Wall Street Journal*, February 16, 2012, sec. Opinion. http://online.wsj.com/news/articles/SB10001424052970204883304577219543897943980.

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: Ecco, 2010.

Clausewitz, Carl von. *On War*. Princeton, N.J: Princeton University Press, 1976.

“Combined Air and Space Operations Center (CAOC) Fact Sheet.” U.S. Air Forces Central Command, February 6, 2011. http://www.afcent.af.mil/library/factsheets/factsheet.asp?id=12152.

“Compendium of Key Joint Doctrine Publications.” Office of the Chairman of the Joint Chiefs of Staff, January 3, 2014. http://www.dtic.mil/doctrine/new_pubs/compendium.pdf.

Cossaboom, Robert T., Tommy R. Young, Larry R. Morrison, and Feyette G. Haase. “History of the Air Force Communications Command: 1 January - 31 December 1991,” July 1, 1992. (AR) 7101. HAF-HO.

Davis, Shelley L., Laurence B. Epstein, Cora J. Holt, Larry R. Morrison, Daniel R. Mortensen, Thomas S. Snyder, Melinda A. Wigginton Trapp, Tommy R. Young, Robert T Cossaboom, and Linda G. Miller. *The Air Force Communications Command: 1938-1991, An Illustrated History*. Edited by Thomas S Snyder. Third Edition. Scott AFB, IL: Air Force Communications Command, 1991.

“Department of Defense Strategy for Operating in Cyberspace.” Department of Defense, July 2011. http://www.defense.gov/news/d20110714cyber.pdf.

“Deperatment of Defense Directive 8570.1: Information Assurance Training, Certification, and Workforce Management.” Department of Defense, August 15, 2004.

“Enterprise Service Desk Operating Concept.” Air Force Space Command, February 5, 2013.

Feaver, Peter. *Armed Servants: Agency, Oversight, and Civil-Military Relations*. Cambridge, Mass.; London: Harvard University Press, 2005.

Ghoshal, Sumantra. “Bad Management Theories Are Destroying Good Management Practices.” *Academy of Management Learning & Education* 4, no. 1 (March 1, 2005): 75–91.

Golembiewski, Joseph R. “From Signals to Cyber: The Rise, Fall, and Resurrection of the Air Force Communications Officer.” School of Advanced Air and Space Studies, 2010.
Hagen, Andreas. “The Russo-Georgian War 2008.” In *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, edited by Jason Healey. Vienna, Virginia: Cyber Conflict Studies Association, 2013.
Harris, Bryan, Eli Konikoff, and Phillip Petersen. “Breaking the DDoS Attack Chain.” Carnegie Mellon University, 2013. http://www.cmu.edu/mits/files/breaking-the-ddos-attack-chain.pdf.
Hinton, Ben. “Harnessing the Power of Cyberspace.” *Intercom*, April 2006.
Internet Security Threat Report 2014. Mountain View, California: Symantec Corporation, April 2014. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.
“Joint Information Environment Operations Concept of Operations.” JIE Operations Sponsor Group, January 25, 2013.
“Joint Publication 3-30: Command and Control of Joint Air Operations.” Office of the Chairman of the Joint Chiefs of Staff, February 10, 2014. http://www.dtic.mil/doctrine/new_pubs/jp3_30.pdf.
“Joint Publication 6-0: Joint Communications System.” Office of the Chairman of the Joint Chiefs of Staff, June 10, 2010. http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.
Kenyon, Henry S. “Joint Information Environment Is Under Way.” *SIGNAL Magazine*. Accessed January 8, 2014. http://www.afcea.org/content/?q=node/11696.
Lawlor, Maryann. “Command Takes Network Control.” *SIGNAL Magazine*, October 2006. http://www.afcea.org/content/?q=node/1206.
Lieutenant General (retired) Robert H. Ludwig. Interview by Robert T. Cossaboom, April 30, 1993.
Maluda, John W. “On Cyberspace Developments.” *High Frontier*, May 2009.
Miller, Linda G., and Cora J. Holt. *Window to the Future: Air Force Communications Command Chronology 1938-1988*. Scott AFB, IL: Air Force Communications Command, 1989.
Morrison, Larry R. *From Flares to Satellites: A Brief History of Air Force Communications*. Scott AFB, IL: Air Force Communications Agency, 1997.
Moseley, T. Michael. Letter to Commander, 8th Air Force. “Operational Cyberspace Command ‘Go Do’ Letter,” November 1, 2006. http://www.24af.af.mil/shared/media/document/AFD-111003-055.pdf.
“Operating Concept for Air Force Network Increment 1.” Air Force Space Command, June 29, 2010.
“Operating Concept for the Air Force Cyberspace Operations Center.” Air Force Space Command, October 5, 2011.

Pellerin, Cheryl. “Cyber Command Adapts to Understand Cyber Battlespace.” *American Forces Press Service*, March 7, 2013. http://www.defense.gov/news/newsarticle.aspx?id=119470.

Petruska, Shelly. “Historical Milestone Reached for Air Force Cyberspace.” *Air Force Network Integration Center*. April 1, 2014. http://www.afspc.af.mil/news1/story.asp?id=123405483.

“Program Action Directive 07-08, Change 1: Implementation of the Secretary of the Air Force Direction to Establish Air Force Cyberspace Command (AFCYBER).” Headquarters United States Air Force, January 24, 2008.

“Program Action Directive 07-10: The Implementation of the Chief of Staff of the Air Force Direction to Establish the Air Force Network Operations Organization Structure.” Headquarters United States Air Force, November 13, 2007.

Rid, Thomas. *Cyber War Will Not Take Place*. Oxford ; New York: Oxford University Press, 2013.

Roulo, Claudette. “Official Describes Joint Information Environment.” *American Forces Press Service*. October 3, 2012. http://www.defense.gov/news/newsarticle.aspx?id=118092.

Rumelt, Richard P. *Good Strategy, Bad Strategy: The Difference and Why It Matters*. 1st ed. New York: Crown Business, 2011.

Schmidt, Andreas. “The Estonian Cyberattacks.” In *A Fierce Domain: Conflict in Cyberspace 1986 to 2012*, edited by Jason Healey. Vienna, Virginia: Cyber Conflict Studies Association, 2013.

Shelton, William L. “Integrating, Air, Space & Cyberspace Capabilities.” presented at the Air Force Association - Air and Space Technology Exposition, National Harbor, MD, September 17, 2013. http://www.afspc.af.mil/library/speeches/speech.asp?id=742.

Shores, Louis. *Highways in the Sky*. New York: Barnes & Noble, 1947.

Sinek, Simon. *Start with Why: How Great Leaders Inspire Everyone to Take Action*. New York: Portfolio, 2009.

Sterling, Christopher H., ed. *Military Communications: From Ancient Times to the 21st Century*. Santa Barbara, Calif: ABC-CLIO, 2008.

Strasser, Max. “Why Ukraine Hasn’t Sparked a Big Cyberwar, So Far.” *Newsweek*, March 18, 2014. http://www.newsweek.com/why-ukraine-hasnt-sparked-big-cyber-war-so-far-232175.

Stratton, Todd. “Cyberspace Support as a Strategic Vulnerability of USAF Operational Wings.” Air War College, 2014.

Sun Tzu. *The Illustrated Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 2005.

Van Creveld, Martin. *Command in War*. Cambridge (Mass.); London: Harvard University Press, 1985.

Wynne, Michael W., and T. Michael Moseley. “Establishment of an Operational Command for Cyberspace,” September 6, 2006. http://www.24af.af.mil/shared/media/document/AFD-111003-051.pdf.
———. “Letter to the Airmen of the United States Air Force,” December 7, 2005. http://www.24af.af.mil/shared/media/document/AFD-111003-050.pdf.