OPERATIONAL COMMAND AND CONTROL OF CYBER WARFARE: A COMPARATIVE CASE STUDY ANALYSIS

BY

JONATHAN M. FRENCH

A THESIS PRESENTED TO THE FACULTY OF

THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES

FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES

AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2018

APPROVAL

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

_____

COL TIMOTHY M. CULLEN (Date)

_____

DR. STEPHEN E. WRIGHT (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 Jonathan M. French earned a Bachelor of Science degree in Management as a 2005 graduate of the United States Air Force Academy. His first duty station was Andersen Air Force Base, Guam, where he worked in the base communications squadron. He deployed for a year as a Command and Control Communications Planner and, later, an Iraq Master Air Attack Planner at the Central Command Combined Air Operations Center.

Following a brief tour at the Air Operations Center in Ramstein, Maj French joined the Joint Communications Support Element (Airborne) in Tampa, Florida where he was the Current Operations Chief and the Chief of Special Operations Command and Central Command Plans. Before attending Intermediate Developmental Education, Major French served at the Pentagon in Washington, District of Columbia where he was the Senior Executive Officer to the United States Air Force Chief Information Officer.

Maj French graduated from the School for Advanced Study of Air Mobility (ASAM) at Joint Base McGuire-Dix-Lakehurst while receiving a Master of Science degree in Logistics from the Air Force Institute of Technology. Following graduation from the School of Advanced Air and Space Studies, he will serve as the Director of Operations for the 33d Network Warfare Squadron at Joint Base San Antonio, Texas.

ACKNOWLEDGMENTS

This year has been one of the most challenging and rewarding of my career. First, I want to thank my SAASS XXVII classmates. I am truly honored to call them comrades-in-arms and friends.

I would also like to specifically acknowledge several people without whose help I would never have gotten this study off the ground. My sincere thanks go to Maj Jeremy Sparks for the countless rants and rambles about the woes of cyberspace operations. I especially want to thank my research advisor, Colonel Timothy Cullen, and my reader, Dr. "Wilbur" Wright, for their invaluable insight, advice, and mentoring throughout this project. Without their prodding, prompting, and editorial destruction of my initial drafts, this investigation would have fallen short of its intended goal.

Most importantly, I want to express my sincere appreciation to my wife for her patience and understanding during those times when I was physically or mentally absent while completing this project. Without her support, this paper would not have been possible.

ABSTRACT

The complexity of military operations is increasing as information technologies begin to merge the strategic, operational and tactical levels of warfare. In addition to an increased emphasis on coalition warfare, the introduction of new warfighting domains such as space and cyberspace complicate an already complex array of organizational relationships.

In its infancy, USCYBERCOM rightly focused on building the capacity of its cyber capabilities and maturing the command's staff processes and relationships. In that same period, the command implemented incremental changes to its C2 framework to foster better integration of cyber capabilities on the battlefield. Even the most current C2 framework, however, hinders USCYBERCOM's efforts to build effective warfighting capabilities in the cyberspace domain.

USCYBERCOM should look to its functional counterparts for effective methods to C2 cyber operations. The Air Force employs processes that permit centralized control and decentralized execution to emphasize the unique characteristics of airpower. Special operators use agile organizations and support relationships to facilitate distributed operations, unity of effort, and unified action while maintaining a small tactical footprint. USCYBERCOM has neither the underlying processes nor the agile organizational construct to integrate cyber warfare into the joint fight effectively.

As a unified combatant command, USCYBERCOM must transition from its rigid model of centralized control and centralized execution to a slightly more decentralized role of global synchronization. This transition requires the creation of regional cyber headquarters, collocated with the geographic combatant commands (GCCs), under the Combatant Command (COCOM) of USCYBERCOM. The new cyber components should also distribute liaison elements to the corps or division level equivalent of the existing service air-to-ground C2 systems to foster improved timing and tempo of cyber effects.

CONTENTS

Illustrations

Chapter 1

Introduction

The complexity of military operations is increasing as information technologies begin to merge the strategic, operational and tactical levels of warfare.[1] In addition to an increased emphasis on coalition warfare, the introduction of new warfighting domains such as space and cyberspace complicate an already complex array of organizational relationships.[2] These relationships, when combined with roles, responsibilities, and authorities, represent the command and control (C2) structures required to conduct efficient and effective combat operations in pursuit of national and coalition objectives.

Soldiers, Sailors, Airmen, and Marines often take operational and tactical C2 for granted as it is not typically part of the cultural DNA of tactically focused and proficient warfighters.[3] Whether recognized or not, the cause of many issues at the tactical level is inflexible or unresponsive C2 structures. The traditional hierarchical structure of modern military C2 frameworks and processes can cause seams between organizations that lead to challenges with collaboration, information sharing, interoperability, and mission effectiveness.[4]

Command and control plays a critical role in military operations. While advocating for his observe, orient, decide, and act (OODA) loop, Colonel John Boyd suggested that the speed at which one could orient to the combat situation would most likely determine the winners and losers in a given scenario.[5] If Boyd's hypothesis is true, it is imperative that C2 structures promote unimpeded communication between decision

---

[1] Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*, 1.
[2] Alberts and Hayes, 1.
[3] Weems, "Command and Control in the Anti-Access/Area Denial Environment," 8.
[4] Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*, 63.
[5] Hammond, *The Mind of War: John Boyd and American Security*, 162–67.

makers, mission partners, and the front lines.[6] In a study of C2 breakdowns in 20 operational case studies from WWI to present day, however, Marius Vassiliou concluded that all were a result of either the inability or the failure to communicate.[7] Specifically, C2 failures resulted from poor communication due to physical constraints, interoperability issues, security concerns, or "lack of will, knowledge, trust, and tools."[8]

The introduction of cyberspace as a fifth warfighting domain further exacerbates the C2 problems of the Information Age. In 2009, the Department of Defense (DoD) established United States Cyber Command (USCYBERCOM) as a subordinate unified command under United States Strategic Command (USSTRATCOM).[9] In its infancy, USCYBERCOM rightly focused on building the capacity of its cyber capabilities and maturing the command's staff processes and relationships.[10] In that same period, the Secretary of Defense (SECDEF) approved incremental changes to the cyberspace C2 framework to foster better integration of cyber capabilities on the battlefield. Even the most current C2 framework, however, hinders USCYBERCOM's efforts to build effective warfighting capabilities in the cyberspace domain. How can USCYBERCOM best organize its forces to both leverage its budding operational capabilities and integrate the unique characteristics of cyber warfare with the objectives of Joint Force Commanders?

Research Methodology

This paper seeks to develop an unobstructed view of the cyberspace command and control framework and its associated strengths and challenges. This thesis answers the following questions: How well does the cyber command and control framework align with the cyberspace operational environment? Which actions could the DoD take

[6] Ramsey, Ryan, "C2 - Less Is More," 11.
[7] Vassiliou, "How C2 Goes Wrong," 15.
[8] Vassiliou, 16.
[9] Gibney, "Centralized Offense, Decentralized Defense: Command and Control of Cyberspace," 54.
[10] Lundgren, "Examining Command and Control Constructs for Offensive Cyberspace Operations," 17.

to improve cyber warfare integration with Joint Force Commander objectives?

While cyberspace is a new warfighting domain, the way that the military commands and controls the fight in cyberspace is not new. The DoD has experienced varying degrees of success with integrating cyber capabilities into the existing C2 frameworks of the Geographic Combatant Commands (GCCs). However, it is difficult to determine if those successes are the result of the availability of sophisticated tactical capabilities or the introduction of effective C2 structures.

This thesis pursues the research questions through a comparative case study analysis of airpower, special operations and cyber for a few specific reasons. First, all three case studies involve the roles and missions of functional capabilities that services present to the Joint Force Commander.

Second, each of the case studies represent varying degrees of low-density and high-demand capabilities that can produce effects at the strategic, operational, and tactical levels of war. These traits drive creative C2 frameworks that emphasize the strengths of the specific capability.

Third, the C2 framework implementations for airpower, special operations, and cyberspace all differ at a fundamental level. The Air Force employs *processes* that permit centralized control and decentralized execution to emphasize the unique characteristics of airpower. Special operators use *agile organizations* and support relationships to facilitate distributed operations, unity of effort, and unified action while maintaining a small tactical footprint. USCYBERCOM uses a centralized control and centralized execution model to focus its effort on building capacity for tactical team in a trade-off to staff overhead.

Finally, characteristics of the air power and SOF missions are complementary to cyberspace operations in many ways. It is essential

for USCYBERCOM to leverage the lessons learned from these two mission partners as it matures in its new role as a Unified Combatant Command.

The research primarily focuses on the operational level of war. It will briefly touch on both strategic and tactical issues; however, the focus is on operational level command and control as this layer connects the two. Furthermore, this research will not venture into the realm of classified material. While the realm of cyber operations is heavily classified, its C2 structures and most of the associated processes are unclassified and are suitable for this research. Finally, this research assumes that USCYBERCOM, its capabilities, and operational partnerships are in a period of growth and maturity. As the command and the cyberspace domain continue to develop, USCYBERCOM will pursue avenues for stronger integration and collaboration at both the global and theater levels.

Chapter Outline

Chapter one, Command and Control Primer, introduces some of the broader thinking behind how the military organizes and employs its forces. This chapter decouples command from control and examines the separate functions of each to demystify the elusive concept of command and control. The basics of command and control build into an exploration of classic and contemporary C2 frameworks to identify the strengths and weaknesses of each. Finally, the primer concludes with a review of DoD terminology and requirements for command relationships and support relationships. The case studies will use concepts from throughout this chapter.

Next, the first case study examines the C2 framework for the application of airpower. The chapter begins with the operational context of the domain and builds into the background of the C2 framework itself. The airpower case study focuses on the single air manager debate of the Vietnam War at the Battle of Khe Sanh. The single air manager debate is

a crucial moment for the command and control of airpower as it argues the merits of unity of command and unity of effort against the Marine Corps' demand to retain organic airpower tethered to a limited geographic area. The analysis of this case study highlights how air power's ability to transcend geographic terrain shapes its C2 framework. Conversely, the rigidity and robustness its C2 framework creates both strengths and weaknesses for air power in a future fight.

The second case study investigates the C2 framework for the application of special operations. The chapter opens with the operational context of special operations and continues to examine the background of the special operations C2 framework. The special operations case study focuses on integration between SOF and conventional forces in Afghanistan. The case study is relevant in that the secretive and "special" nature of SOF mission is paradoxical. To maintain the initiative and surprise required to employ small teams, special operators must strictly protect sensitive operational information. That same protectiveness can drive interoperability issues with conventional forces due to a lack of communication and collaboration. Additionally, special operations forces leverage their C2 frameworks to institutionalize a whole-of-government approach, known in C2 vernacular as unified action.[11]

The third and final case study examines the C2 framework for the application of cyber warfare. The chapter begins with the operational context of the cyberspace domain and builds into the background of the C2 framework itself. While the cyber case study does not use specific operational examples due to classification reasons, the maturation of the C2 framework over the last nine years is discussed, analyzed, and assessed against CDRUSCYBERCOM's stated vision and goals for the command.

[11] Joint Chiefs of Staff, Doctrine for the Armed Forces of the United States, II–8.

Overall Recommendations

USCYBERCOM has neither the underlying processes nor the agile organizational construct to integrate cyber warfare into the joint fight effectively. As a unified combatant command, it must transition from a rigid model of centralized control and centralized execution to a slightly more decentralized role of global synchronization. This transition requires the creation of regional cyber headquarters, collocated with the geographic combatant commands (GCCs), under the Combatant Command (COCOM) of USCYBERCOM. The new cyber components should also distribute liaison elements to the corps or division level equivalent of the existing service air-to-ground C2 systems to foster improved timing and tempo of cyber effects.

Chapter 2

Unpacking Command and Control

If C2 is so important, why does the military struggle to get it right? One reason is that the terms "command" and "control" mean different things collectively and individually to different communities.[1] In fact, even U.S. joint military doctrine describes the terms differently among the various publications. Therefore, it is imperative to understand the terms command and control before moving forward to examining applications and challenges of C2 in the remaining chapters.

JP 1 *Doctrine for the Armed Forces of the United States* defines command as:

> Command is central to all military action, and unity of command is central to unity of effort. Inherent in command is the authority that a military commander lawfully exercises over subordinates including authority to assign missions and accountability for their successful completion. Although commanders may delegate authority to accomplish missions, they may not absolve themselves of the responsibility for the attainment of these missions. Authority is never absolute; the extent of authority is specified by the establishing authority, directives, and law.[2]

Joint Publication 3-0 *Operations* expands on the limited definition of command in JP 1 by adding:

> Command includes both the authority and responsibility to use resources to accomplish assigned missions. Command at all levels is the art of motivating and directing people and organizations to accomplish missions.[3]

While the joint definitions are not conflicting, neither provides a clear and concise explanation of command. The key phrases included in the descriptions are authority, mission assignment, and direction. In

[1] Alberts and Hayes, *Understanding Command and Control*, 7.
[2] Joint Chiefs of Staff, Doctrine for the Armed Forces of the United States, V–1.
[3] Joint Chiefs of Staff, Joint Operations, III–3.

Understanding Command and Control, David Alberts agrees with the doctrinal interpretation but adds the missing pieces of providing intent and assessing the situation to the list. This is an essential addition to the DoD description as a commander's direction is usually delivered in the form of a broad intent statement and execution is assessed through feedback from lower echelons.

Joint Publication 3-0 *Operations* defines control as:

> Control is inherent in command. To control is to manage and direct forces and functions consistent with a commander's command authority. Control of forces and functions helps commanders and staffs compute requirements, allocate means, and integrate efforts. Control is necessary to determine the status of organizational effectiveness, identify variance from set standards, and correct deviations from these standards. Control permits commanders to acquire and apply means to support the mission and develop specific instructions from general guidance. Control provides the means for commanders to maintain freedom of action, delegate authority, direct operations from any location, and integrate and synchronize actions throughout the OA. Ultimately, it provides commanders a means to measure, report, and correct performance.[4]

The definition of control overlaps with that of command in that it is also identified as a means to direct forces. The direction of action in the control mechanism, however, is a means to ensure that the resulting behavior remains within the limits of the "intent" of the command function. Alberts' definition of control more clearly states the function of control as keeping "the values of specific elements of the operating environment within the bounds established by command, primarily in the form of intent."[5]

[4] Joint Chiefs of Staff, III–6.

[5] Alberts and Hayes, *Understanding Command and Control*, 59.

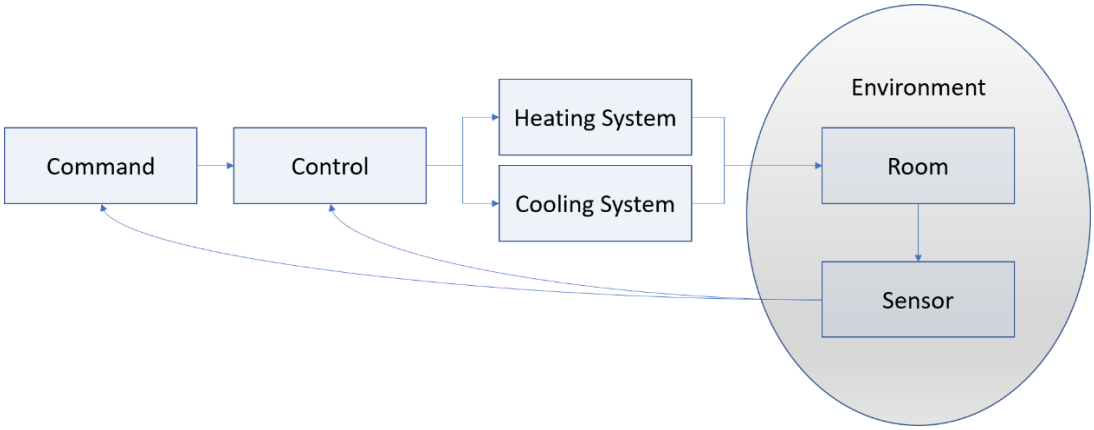

Figure 1: Representative C2 Model for Home Air-Conditioning
Source: Adapted from Alberts and Hayes, Understanding Command and Control

The description of a home air conditioning unit provided by Alberts (see Figure 1 above) explains the mutually supporting concepts of command and control in a way that is easy to comprehend.[6] The homeowner, the command function in this vignette, sets the desired conditions or environmental outcomes for the house. For example, the homeowner could set the broad intent for the air conditioner to cool the house if the temperature rises above 72 degrees. The thermostat, the control function in the vignette, manages the execution of the system according to the home owner's direction. To do this, the control function directs the cooling system to cool the house.

Perhaps most importantly, both the command and the control function receive feedback from environmental sensors in the house.[7] The control function uses the feedback to determine if it has successfully met the intent of the command function. Stated differently, the thermostat uses sensor feedback to determine whether the home has reached the desired temperature or to continue running the cooling system.

The command function uses the environmental sensor data in a slightly different way by deciding whether the original intent was

[6] Alberts and Hayes, 20–21.
[7] Alberts and Hayes, 21.

adequate or to adjust direction moving forward. Using the vignette's language, if the homeowner still *feels* hot after the thermostat *senses* an ambient temperature of 72 degrees, they could give direction to cool the house to 70 degrees. Alternatively, the homeowner could *feel* cold and direct the thermostat to heat the house to 75 degrees. Otherwise, the homeowner could *feel* content and decide to keep the temperature at 72 degrees.

In the scenario, the homeowner weighs two sources of feedback while making decisions to give intent or change direction. The first mechanism is the hot and cold receptors of the human body that tell the homeowner how the environmental conditions are making them feel. The second mechanism is the thermostat's ambient temperature reading. If the homeowner reads that the ambient temperature is 72 degrees yet still *feels* hot, he could lower the desired temperature or decide to repair or replace the thermostat itself.

Military command and control is similar in many ways to the home air conditioning example. The role of the command function is to establish and communicate intent, assess the situation as it develops, and issue changes to previous intent or guidance if desired.[8] The control function is typically a combination of organizations and processes that oversee and manage the execution of the commander's intent. Military members cannot expect successful operational outcomes with only command or control. The two functions must operate in harmony. This inseparability of command from control may be the reason why military members so often assume that command and control is one function.

Principles of Command and Control

If understanding the definitions of command and control is not difficult enough, implementing an effective C2 framework is even more challenging. Military doctrine provides several principles for C2 that

[8] Alberts and Hayes, 57.

serve as guidelines for creating effective structures to manage the complexity of modern warfare. Doctrinal principles are authoritative, but they require judgment in application.[9] Therefore, most C2 frameworks are unique to the specific operational context of a given environment or mission.

The first principle for effective command and control is the concept of unity of command. JP 1 *Doctrine for the Armed Forces of the United States* notes that "unity of command means all forces operate under a single commander with the requisite authority to direct all forces employed in pursuit of a common purpose."[10] Using the air conditioning vignette, unity of command implies that only one member of the household can issue commands to the thermostat. If two people were setting the target temperature, one hot and one cold, the environment would meet the specific needs of neither person or only the needs of whomever last set the thermostat.

Unity of effort is perhaps the most important doctrinal concept relating to command and control. JP 1 describes unity of effort as required for:

> Coordination and cooperation among all forces toward a commonly recognized objective, although they are not necessarily part of the same command structure. During multinational operations and interagency coordination, unity of command may not be possible, but the requirement for unity of effort becomes paramount. Unity of effort—coordination through cooperation and common interests—is an essential complement to unity of command. Unity of command requires that two commanders may not exercise the same command relationship over the same force at any one time.[11]

[9] Chairman of the Joint Chiefs of Staff, Joint Doctrine Development System, A-1.
[10] Joint Chiefs of Staff, Doctrine for the Armed Forces of the United States, V–1.
[11] Joint Chiefs of Staff, V–1.

Unity of effort is the key to success in joint operations.[12] As force structures in the DoD shrink, unity of effort assures mission accomplishment through synchronization at all levels and provides clean lines of communication with focused and coordinated objectives.[13]

Building upon unity of effort is the concept of unified action. While unity of effort focuses on synchronizing the joint fight, unified action ties together the actions of military organizations with non-DoD government entities and multinational partners. JP 1 describes unified action as a concept that:

> Synchronizes, coordinates, and/or integrates joint, single-Service, and multinational operations with the operations of other USG departments and agencies, NGOs, IGOs (e.g., the United Nations), and the private sector to achieve unity of effort. Unity of command within the military instrument of national power supports the national strategic direction through close coordination with the other instruments of national power.[14]

The key to both unity of effort and unified action is synchronization. While agreeing with Boyd's hypothesis of superior decision making, Alberts points out that the ability to "act in concert in a timely manner often separates the victor from the vanquished."[15] Through command and control relationships, DoD doctrine defines synchronization as "the arrangement of military actions in time, space, and purpose to produce maximum actions in time, space, and purpose to produce maximum relative combat power at the decisive place and time."[16] Multi-domain warfare is leading many to believe, however, that the need to mass forces should be replaced by the imperative to mass effects at the appropriate place and time.[17] Synchronization of effort and

[12] Lawrence, "Joint C2 Through Unity of Command," 110.
[13] Lawrence, 110.
[14] Joint Chiefs of Staff, Doctrine for the Armed Forces of the United States, II–8.
[15] Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*, 104.
[16] Joint Chiefs of Staff, DOD Dictionary of Military and Associated Terms, 223.
[17] Alberts and Hayes, *Power to the Edge: Command and Control in the Information Age*, 104.

action, whether at the joint or multinational level, is underpinned by the ability to effectively collaborate. Commanders establish the conditions for collaboration which, in turn, sets patterns of behavior for the organization.[18] A fully synchronized C2 framework exhibits collaboration in the form of inclusive participation, unconstrained communication, and rich multimedia or face-to-face interaction.[19]

Command and Control Models

The first step to determining the appropriate C2 framework is to identify the mission and conditions for the operation.[20] The various service doctrine of the U.S. armed forces differ in the overall approach to C2 due to unique characteristics of their respective domains.[21] Speaking in generalities, the U.S. Army favors decentralization to maintain initiative and speed. The U.S. Navy leans toward mission-type orders to facilitate unity of command in the semi-autonomous circumstances of the maritime domain. Marines focus on tight coordination and flexibility in order to synchronize the air, land, and maritime domains. Finally, the Air Force leverages centralized control and decentralized execution to mass strategic effects while also supporting the tactical requirements of land force commanders.[22]

Determining the appropriate C2 framework for a given mission and operational conditions can be challenging. Real-world implementations of command and control often differ from what doctrine recommends due to the unique demands of the operational environment.[23] After conducting a study that consulted senior leaders from NATO nations, Alberts defined the operational environment by the rate of change, the

[18] Alberts and Hayes, *Understanding Command and Control*, 40.
[19] Alberts and Hayes, 152.
[20] Vassiliou, "How C2 Goes Wrong," 40.
[21] Weems, "Command and Control in the Anti-Access/Area Denial Environment," 17.
[22] Weems, "Command and Control in the Anti-Access/Area Denial Environment."
[23] Alberts and Hayes, *Understanding Command and Control*, 75.

degree of familiarity, and the strength of information position.[24] The first characteristic, rate of change, describes the situation itself. Static problems are more open to centralized decision making, where organizational efforts are optimized, preplanned, and tightly controlled. Dynamic situations involve rapid change and the controls present in static problem sets are often impediments to successful command and control. Degree of familiarity describes the nature of the problem.[25] If the problem is well understood, the degree of familiarity is likely high. This does not, however, mean that a dynamic situation is less understood. The final characteristic, strength of information position, refers to the degree to which an organization is able to fulfill its information requirements.[26]

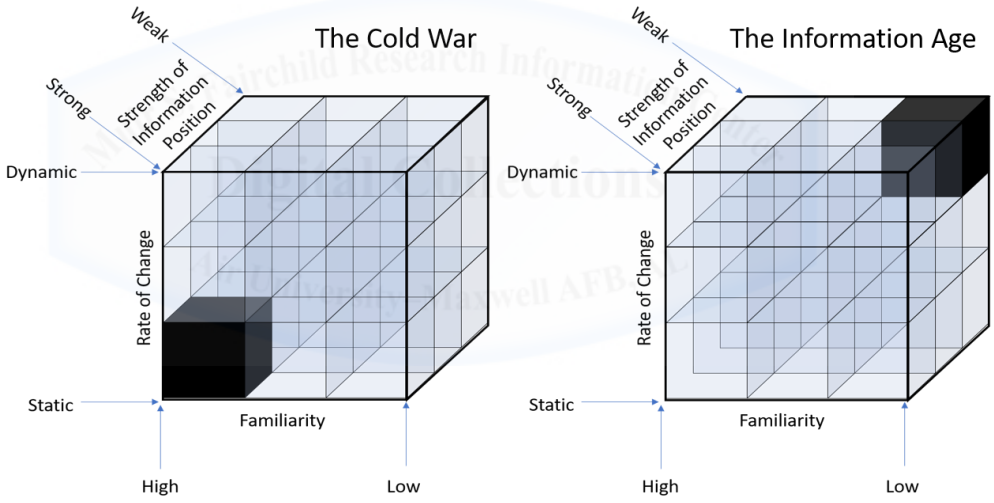

Figure 2: The Spectrum of Operational Environments
Source: Adapted from Alberts and Hayes, Understanding Command and Control

Figure 2 illustrates the difference between Cold War and Information Age operational environments. The Cold War represented a static situation with a high degree of familiarity between competitors and exquisite knowledge about not only friendly but adversary capabilities, as

[24] Alberts and Hayes, 78–79.
[25] Alberts and Hayes, 78.
[26] Alberts and Hayes, 79.

well.[27] On the other hand, information age warfare takes place in a volatile, uncertain, complex, and ambiguous (VUCA) environment against an unknown or unfamiliar adversary. Therefore, information age warfare presents a dynamic situation, with low familiarity of the adversary, and an unquenching thirst for information with a modest ability to fulfill the information requirement.

After determining the operational environment, it is possible to create a command and control framework that enables the force to achieve its objectives. Alberts builds upon his description of the operational environment by identifying that the critical dimensions of a C2 framework are the allocation of decision rights, the patterns of interaction, and the distribution of information.[28] The allocation of decision rights describes how the command function will operate within the framework. It determines who can choose among the existing alternatives and how the authority for those decisions is either centralized or distributed through the organization. The patterns of interaction entail the number and variety of participants, the quality of the contents for the interaction, and the means through which the interaction occurs. Patterns of interaction range from a tightly controlled hierarchical exchange of information to a highly networked and collaborative engagement toward a common purpose.[29] The last dimension, distribution of information, describes how collaboration is enabled through the access to information. At one extreme, information is centrally stored and access is tightly controlled. On the other extreme, information is available to all participants in the organization and stored in a distributed and redundant manner.[30] The three dimensions of a C2 framework are interdependent. The allocation of decisions helps to

[27] Alberts and Hayes, 79.
[28] Alberts and Hayes, 81–102.
[29] Alberts and Hayes, 96.
[30] Alberts and Hayes, 109.

determine the patterns of interaction necessary for collaboration and shared situational awareness. Finally, the requirement for situational awareness and collaboration determines the desired distribution of information within the organization.[31]

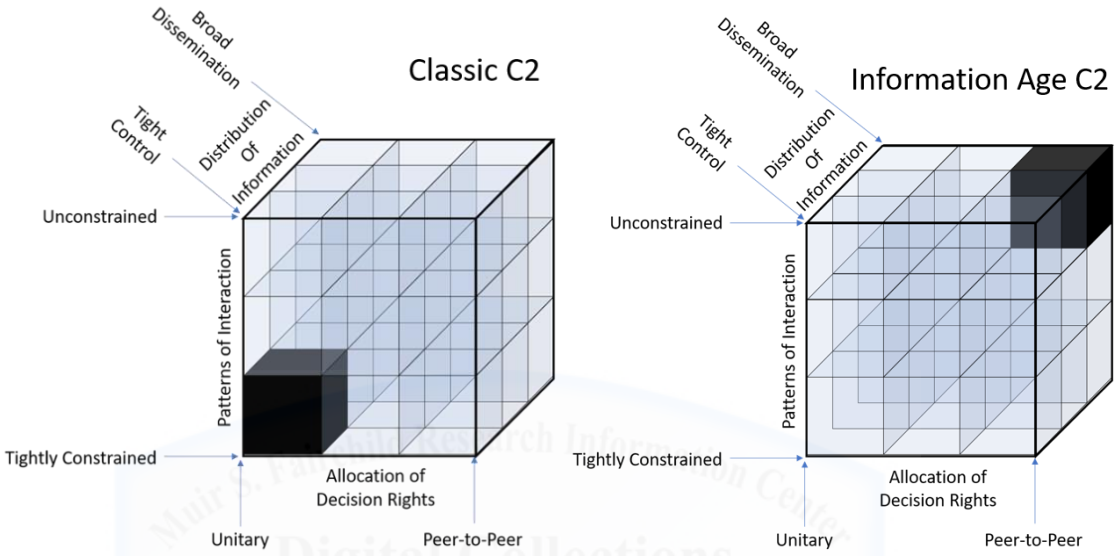

Figure 3: The Spectrum of C2 Frameworks
Source: Adapted from Alberts and Hayes, Understanding Command and Control

Figure 3 illustrates the difference between classic and Information Age C2 frameworks. Classic C2 involves rigid hierarchical frameworks ideal for top-down decision making where only senior staff levels engage in cross-functional collaboration and information is tightly controlled by decision makers.[32] Information Age C2 exhibits flattened organizational structures, unconstrained vertical and horizontal cross-functional collaboration, ubiquitous access to information, and loose controls for information sharing. Empowering the lower echelons through this model

[31] Alberts and Hayes, 82.
[32] Alberts and Hayes, 79.

promotes the ability to capitalize on fleeting opportunities as an asymmetric advantage.[33]

Command Relationships

It is important to restate that there is not a one-size-fits-all framework for the command and control of military operations. Military leaders must carefully weigh the mission and operational context against the costs and benefits of agile or static C2 methodologies. To assist in this process, the military created mechanisms to promote unity of command, flexibility, and interoperability between organizations in a manner that is relatively easy to comprehend.

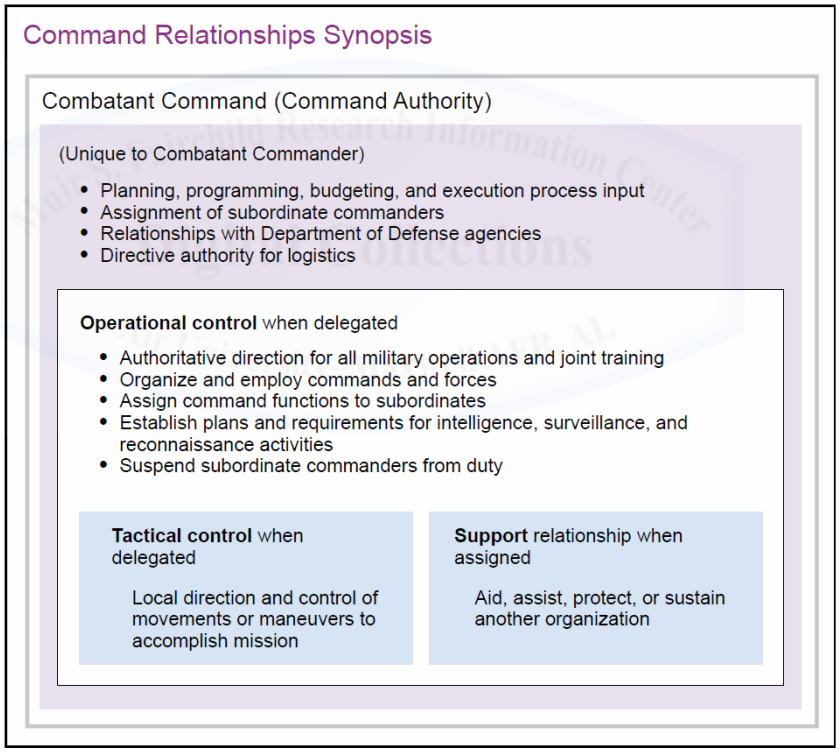

Figure 4: Overview of Command Relationships
Source: Joint Chiefs of Staff, JP 3-0 Joint Operations

Joint Force Commanders (JFCs) exercise various command authorities over assigned or attached forces, as described in Figure 4.[34]

[33] Weems, "Command and Control in the Anti-Access/Area Denial Environment," 22.
[34] Joint Chiefs of Staff, Joint Operations, III–3.

JP 3-0 *Joint Operations* explicitly outlines the functions of combatant command authority, operational control, and tactical control:

> COCOM, which cannot be delegated, is the authority of a CCDR to perform those functions of command over assigned forces involving organizing and employing commands and forces; assigning tasks; designating objectives; and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command.[35]
>
> OPCON is inherent in COCOM and may be delegated within the command. OPCON is command authority that may be exercised by commanders at any echelon at or below the level of CCMD to perform those functions of command over subordinate forces. It involves organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. OPCON includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command.[36]
>
> TACON is inherent in OPCON. TACON is an authority over assigned or attached forces or commands, or military capability or forces, made available for tasking. It is limited to the detailed direction and control of movements or maneuvers within the OA necessary to accomplish assigned missions or tasks assigned by the commander exercising OPCON or TACON of the attached force. TACON may be delegated to, and exercised at, any level at or below the level of CCMD. TACON provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task.[37]

Additionally, Joint Force Commanders can establish support relationships among functional and Service component commanders for complex operations that involve participation by more than one component.[38] Figure 5, below, outlines the categories of support.

[35] Joint Chiefs of Staff, III–3.
[36] Joint Chiefs of Staff, III–4.
[37] Joint Chiefs of Staff, III–5.
[38] Joint Chiefs of Staff, III–6.

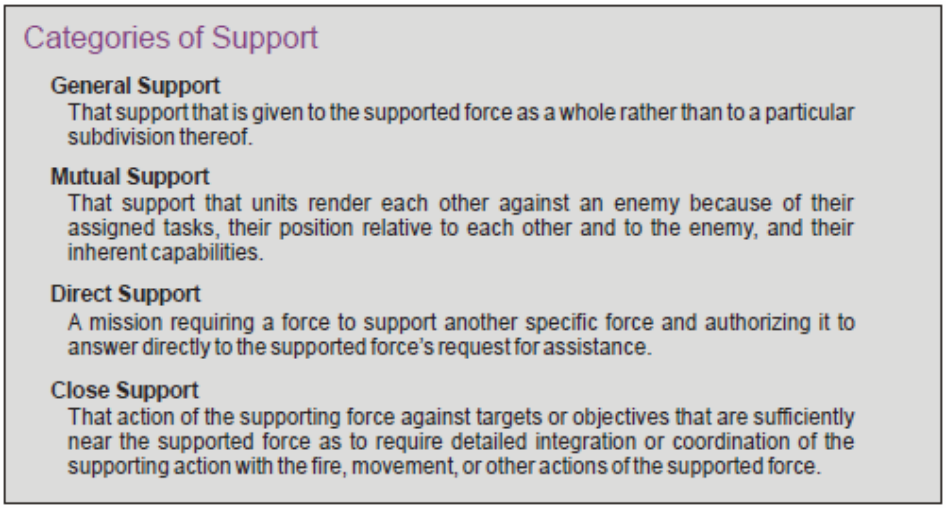

Figure 5: Categories of Support Relationships
Source: Joint Chiefs of Staff, JP 3-0 Joint Operations

The nomenclature and challenges of command and control can appear daunting for even the most experienced military professional. The imperative for military organizations is to design and implement a C2 framework that enables effective management and synchronization of effort in the operational environment. Command relationships and the various categories of support should facilitate the allocation of decision rights, patterns of interaction, and distribution of information that is appropriate for the mission. As the environment evolves, so too should the C2 framework that aims to control the effort affecting it. The case studies that follow will explore several operating environments and associated C2 framework while assessing their effectiveness in achieving the desired military objectives.

Chapter 3

Command and Control of Air Power

On 21 July 1943, the United States War Department published FM 100-20 *Command and Employment of Air Power* with the opening statement "Land power and air power are co-equal and interdependent forces; neither is an auxiliary of the other."[1] FM 100-20 was a monumental step forward for the effective command and control of air power capabilities. Since the introduction of military aviation in the early 1900's, air power advocates have pushed for an independently controlled air service. A few sentences later, the War Department underwrote the potential of American air power:

> The inherent flexibility of air power is its greatest asset. This flexibility makes it possible to employ the whole weight of the available air power against selected areas. Such concentrated use of the air striking force is a battle winning factor of the first importance. Control of available air power must be centralized and command must be exercised through the Air Force Commander if this inherent flexibility and ability to deliver a decisive blow are to be fully exploited.[2]

As evident in the words of the War Department, early airpower advocates understood that the flexibility of air power presented great opportunity if centrally controlled and employed en masse against strategic objectives.

The Air Force's organic system for controlling air operations is known as the Theater Air Control System.[3] The concept of the TACS is not an American creation. Instead, it is an adaptation of the Royal Air Force Fighter Command's air defense system employed during the Battle of Britain in 1940.[4] The RAF integrated its Fighter Groups with its radar,

[1] War Department, Command and Employment of Air Power, 4.
[2] War Department, 4.
[3] Joint Chiefs of Staff, Command and Control of Joint Air Operations, II–9.
[4] Franks, *Battle of Britain*, 11.

anti-aircraft, and observer capabilities to defend against surprise attacks of the Luftwaffe.[5]

FM 100-20 laid the foundation for many significant aspects of the USAF TACS[6]. Building on the concept of centralized control, FM 100-20 suggests that there will only be one air force in a given theater of operations.[7] Furthermore, the War Department prohibited Army Air Force units from attaching to ground force units except when operating independently or isolated by distance or lack of communications.[8] Even in this rare exception, higher headquarters directed their task force commanders to command their air forces through an air commander.[9]

In the present day, tightly controlled planning and supervision of geographically dispersed aviation assets almost always occur at the very highest levels of a theater.[10] This approach, known in Air Force C2 doctrine as centralized control and decentralized execution, exploits air power's unique capabilities of speed, range, versatility, and battlespace perspective.[11] Despite the foresight and direction of the War Department, the TACS incrementally matured over a period of decades to provide a mechanism to command and control air power. In the skies of Vietnam, the foundational tenant of centralized control and decentralized execution served as the focal point for a high-stakes internal struggle between the Air Force and the Marine Corps.

C2 of Tactical Strike Aircraft in Vietnam

From 20 January to 18 March 1968, two divisions of the North Vietnamese Army (NVA) surrounded a regiment of U.S. Marines on a mountain plateau in northwest Vietnam called Khe Sanh.[12] The 6,000

[5] Franks, 12.
[6] Liepman, "TACS and Air Battle Management: The Search for Operational Doctrine," 68.
[7] War Department, Command and Employment of Air Power, 5.
[8] War Department, 4.
[9] War Department, 8.
[10] Smith, "USAF Theater Air Control System: Where Do We Go From Here?," 3.
[11] Hukill et al., "Air Force Command and Control: The Need for Increased Adaptability," 10.
[12] Callahan, *Close Air Support and the Battle for Khe Sanh*, 9.

Marines at Khe Sanh faced an NVA force nearly three times as large.[13] In many ways, the American conditions at Khe Sanh paralleled those of the French military at Dien Bien Phu some 14 years earlier.[14] The North Vietnamese recognized this analogy and sought a similar strategic outcome.

Unlike Dien Bien Phu, the meeting at Khe Sanh was not a matter of fate. Instead, it was a carefully orchestrated encounter that both sides treated as a strategic opportunity to crush the opposing will.[15] General William C. Westmoreland, commander of U.S. Military Assistance Command Vietnam (USMACV), aimed to lure the massive NVA force into the remote countryside and annihilate them with superior air power.[16] To accomplish this objective, he ordered centralized coordination and direction for all Air Force tactical air, Strategic Air Command bombers, Marine fixed-wing aviation, and diverted strikes from outside of the country.[17] Figure 6, below, identifies the aviation units that GEN Westmoreland included in the centralized control structure for the battle.

[13] Nalty, *Air Power and the Fight for Khe Sanh*, iii.
[14] Callahan, *Close Air Support and the Battle for Khe Sanh*, 9.
[15] Nalty, *Air Power and the Fight for Khe Sanh*, iii.
[16] Callahan, *Close Air Support and the Battle for Khe Sanh*, 9.
[17] Nalty, *Air Power and the Fight for Khe Sanh*, 68.

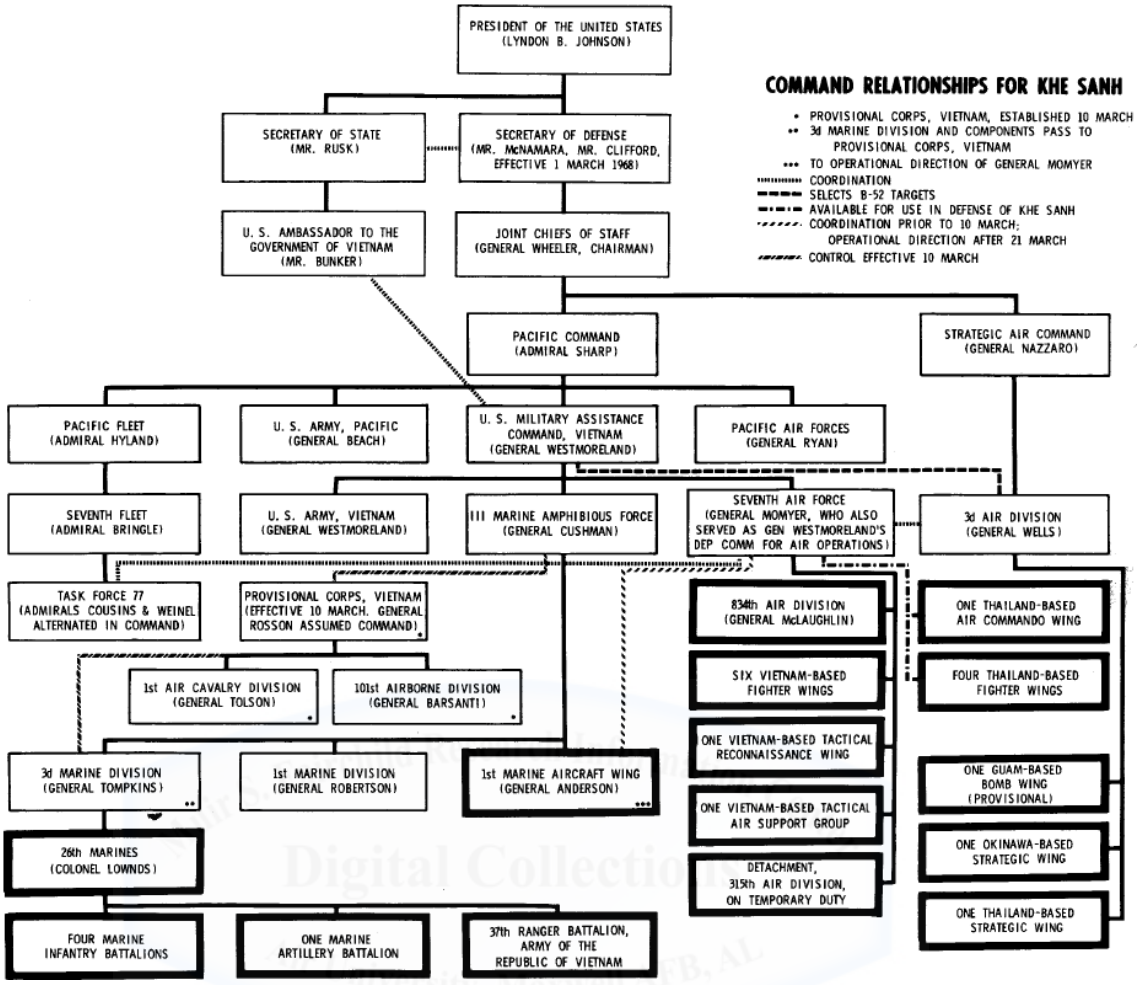

Figure 6: Command Relationships for the Battle of Khe Sanh
Source: Nalty, Air Power and the Fight for Khe Sanh

The III Marine Amphibious Force (MAF) Commander, General Robert Cushman, fought to retain fixed wing Marine aviation to provide close air support to its infantry units at Khe Sanh. Gen Cushman defended this position through the Marine Corps' establishment of the MAF, a combined arms team with a ground combat element dependent on an integrated air combat element.[18] The existing Marine Air Wing (MAW) in Vietnam was doctrinally insufficient to support the number of Marines in-country. Therefore, Gen Cushman had no appetite to

[18] Callahan, *Close Air Support and the Battle for Khe Sanh*, 92.

surrender to the Air Force what little fixed-wing aviation remained under his control.[19]

Air Force Lt Gen William Momyer, MACV Deputy Commander for Air and 7th Air Force Commander, supported GEN Westmoreland's plan for centralized command and control. As an advocate for the centralized control of air power, Lt Gen Momyer felt that the Marines put too much emphasis on geographical considerations.[20] Staying consistent with long-standing Air Force doctrine, he asserted that air power should be free to pursue the highest priority targets, regardless of geographic boundaries.[21]

Historical grievances and cultural differences drove the opposing views of the Marine Corps and Air Force. The Air Force had maintained unified control of fixed aviation during WWII and Korea. From the Airman's perspective, dual management of air power in Vietnam inefficiently applied the air power principles of mass and deep interdiction.[22] The Air Force's Close Air Support plan involved using sensors to locate NVA targets before they could reach the Marines' fixed defensive positions.[23] Once detected, the Air Force sought to mass SAC bombers and multi-service tactical air to attrite the enemy.[24]

The Marines' version of the past, and its vision for the future, varied dramatically from the Air Force. Marine leaders recalled unified management of airpower in Korea as depriving the 1st Marine Division of adequate air support.[25] By maintaining control of organic airpower at Khe Sanh, the Marine Corps sought to destroy forces threatening their maneuver capabilities or defensive posture.[26] In the view of the Marines,

[19] Callahan, 93.
[20] Nalty, *Air Power and the Fight for Khe Sanh*, 74.
[21] Nalty, 74.
[22] Nalty, 69.
[23] Callahan, *Close Air Support and the Battle for Khe Sanh*, 9.
[24] Callahan, 10.
[25] Nalty, *Air Power and the Fight for Khe Sanh*, 69.
[26] Callahan, *Close Air Support and the Battle for Khe Sanh*, 10.

"Deep Air Support" interested the Air Force more than the highly integrated air-ground effort of Close Air Support.[27]

The clash between the Air Force and Marine opposing views required intervention by Admiral Grant Sharp, Commander of U.S. Pacific Command. ADM Sharp endorsed Lt Gen Momyer's authority to oversee centralized control of air power for Khe Sanh.[28] He allowed an exception for the Marine Direct Air Support Center (DASC), Horn DASC, to launch any reserve aircraft for emergency alerts and time-sensitive targets.[29] In effect, ADM Sharp supported a centralized control structure with a caveat for localized direction and control if real-time ground conditions warranted such an approach.

The centralized control system went live on 21 March, lasting just nine days until the Marines appealed to Deputy Secretary of Defense Paul Nitze. The Marines felt the system was unresponsive and instead often used the emergency alert caveat to cover down on most of their needs. DEPSECDEF Nitze delivered a compromise decision, upholding the centralized control system until the tactical situation permitted OPCON of Marine fixed-wing aviation to revert to Gen Cushman.[30]

The introduction of three Army divisions interspersed between the two Marine Divisions in Vietnam made anything other than centralized control untenable. For the duration of the conflict, 7th Air Force retained C2 of air power in Vietnam. General Keith McCutcheon, Deputy Commanding General of III MAF, reflected on the centralized control debate in 1970:

> The system worked. Both the Air Force and Marines saw to that. But the way it was made to work evolved over a period of time, and a lot of it was due to gentlemen's agreements between on-the-scene commanders.[31]

---

[27] Callahan, 9–10.
[28] Nalty, *Air Power and the Fight for Khe Sanh*, 77.
[29] Callahan, *Close Air Support and the Battle for Khe Sanh*, 79.
[30] Nalty, *Air Power and the Fight for Khe Sanh*, 80.
[31] Nalty, 81.

Gen McCutcheon's reflection provides clarity to a pertinent point about the centralized control structure. Although the TACS was a C2 system that should have been personality agnostic, it could not properly function without trust and cooperation between the services. In the case of the Vietnam TACS, cooperation enabled the system rather than the system enabling cooperation.

In a post-war analysis on Fire Support Coordination, MACV personnel lauded the TACS for its flexibility to fit any tactical situation.[32] The TACS utilized an extensive array of C2 nodes to direct the employment of 7AF, VNAF, USMC, USN and SAC air power in the theater.[33] The Tactical Air Control Center (TACC) was the senior C2 element that aligned with the MACV headquarters and coordinated with the Army's Tactical Air Support Element (TASE) at the theater level. Below the TACC, a DASC performed tactical regional C2 and liaised with the Corps Tactical Operations Center (TOC). A Tactical Air Control Party (TACP) attached to each division TOC or brigade Fire Support Coordination Center (FSCC) to facilitate the pre-planned or immediate request for air support.[34]

The MACV TACS, depicted in Figure 7 below, standardized the coordination process for pre-planned strikes. A request for air support usually started at the battalion level.[35] The battalion commander, in conjunction with the attached TACP, derived requirements based on the following day's scheme of maneuver. The FSCC would route the request to the division TOC. There, the division commander would prioritize them by working with the attached TACP. This process would repeat

[32] United States Military Assistance Command Vietnam, "Vietnam Lessons Learned No. 77: Fire Support Coordination in the Republic of Vietnam," C–3.
[33] United States Military Assistance Command Vietnam, C–3.
[34] United States Military Assistance Command Vietnam, C–12.
[35] United States Military Assistance Command Vietnam, C–13.

until it reached the TASE. The TASE worked with TACC to task available aircraft, or source support from SAC, for the next day's order.[36]

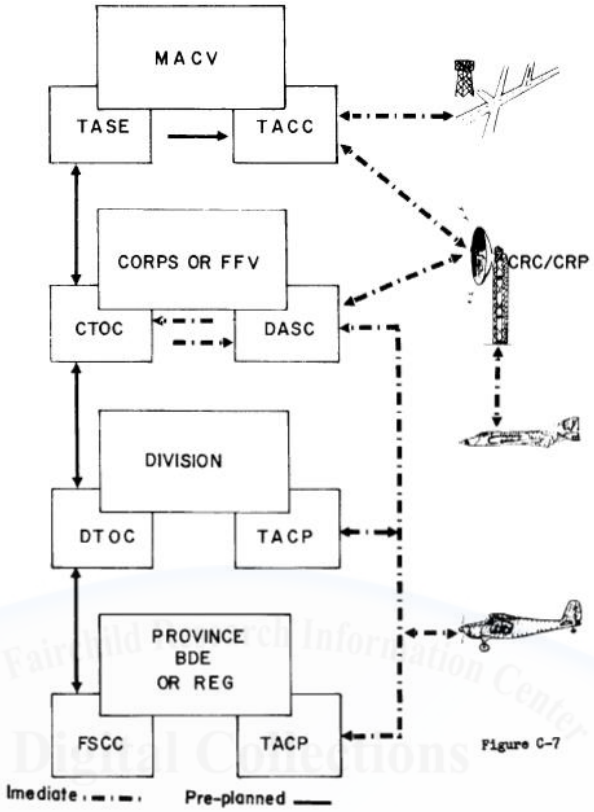

Figure 7: Air Support Coordination in Vietnam
Source: USMACV Vietnam Lessons Learned No. 77

Overall, MACV admitted the TACS implemented greater centralized control than initially intended. The MACV staff recognized that the theater's formidable tactical aviation capability paired with an extensive communications network allowed for such an arrangement.[37] Air superiority in the region permitted the use of an airborne Forward Air Controller (FAC) to identify friendly or enemy positions and relay general observations to ground forces. The airborne FAC, in conjunction with the Airborne Battlefield Command and Control Center (ABCCC) and TACPs, added a tactical C2 layer to the TACS that enabled rich

[36] United States Military Assistance Command Vietnam, C-14.
[37] United States Military Assistance Command Vietnam, C–43.

situational awareness for both the air and ground commanders, making it far superior to the available C2 frameworks of the other services.[38]

Air Power Case Study Analysis

The centralized control debate represents a struggle between two views of the same classic C2 framework. Both the Marine Corps and Air Force pursued courses of action that leveraged unity of command and unity of effort. The Marines sought unity of command for the air-ground task force to create unity of effort within the III MAF area of operations. The Air Force preferred unity of command for the fixed-wing aviation function while fostering unity of effort for the more substantial theater.

In command and control terms, the debate boils down to a difference in desired categories of support for the fixed-wing aviation to the ground component. The Marines preferred close support, where enemy targets near the supported force require detailed integration and coordination of fires and maneuver.[39] The Air Force preferred general support, where support is provided to an entire force rather than to a particular subdivision. [40] In this case, the Air Force sought to support the theater while prioritizing the Khe Sanh area of operations above other missions.

Both the Marine Corps and Air Force courses of action came with strengths and weaknesses. The Marine view benefited from the ability of both the command and the control functions to receive real-time feedback from the environment. Based upon either positive or negative feedback, the III MAF Air Component could change command outputs by issuing a new intent to the Marine Air Wing that loosened the rules of engagement or shifted from CAS to air interdiction. They could also change the control outputs by increasing sortie production, reconfiguring aircraft standard configuration loads, or streamlining weapons

[38] United States Military Assistance Command Vietnam, C–44.
[39] Joint Chiefs of Staff, Doctrine for the Armed Forces of the United States, V–10.
[40] Joint Chiefs of Staff, V–10.

employment procedures. In this light, authority rather than trust underpinned the Marine model of utilizing the MACS to control Marine aviation.

On the other hand, the Marine view suffered from a limited view of the battlefield. If Marine fixed-wing aviation only supported the air-ground task force, it would be unavailable to the broader military effort in the Republic of Vietnam. Presenting a less unified approach toward theater campaign objectives could have negative strategic implications where U.S. forces could win individual battles yet lose the broader war. Furthermore, bifurcating the TACS and Marine Air Control System (MACS) complicated the external synchronization and integration of non-organic fixed-wing aviation from 7th Air Force and SAC. In a close air support scenario, responsiveness is a crucial component to effectiveness. Maintaining parallel C2 structures for air power would create situational awareness deficiencies in both systems, raising the potential for miscues and delaying mutual support between organizations.

The Air Force view accentuated the desire to synchronize the theater's air efforts. The 7th Air Force Commander's OPCON of Marine fixed-wing aviation presented an opportunity to mass both organic and non-organic air in support of the Khe Sanh ground commander. By leveraging the speed and flexibility of airpower, excess capacity from Khe Sanh could reflow to support priority theater strategic objectives. Additionally, the TACS simplified the coordination process by providing a universal C2 system for the request and synchronization of both organic and non-organic air support. The decision to leverage the TACS simplified air power command and control at the theater level, focusing on efficient use of strike assets to achieve MACV objectives.

Conversely, the Air Force's theater-wide perspective complicated the localized employment of air power for Khe Sanh. First, combining the TACS and MACS increased the complexity of communications requirements within the system. Instead of only requesting air support

from DASC Horn in the MACS, the Marines coordinated with a series of operational and tactical C2 elements to receive air support. Second, as a theater-wide entity, the TACS presented a C2 framework built on trust. Marine ground commanders did not have the authority to *direct* fixed-wing support.

Instead, it had to *trust* a parallel organization could provide the appropriate level of air support when needed. The events at Khe Sanh demonstrated that trust was not present at first. Instead, cooperation and mutual understanding fostered trust over time. Finally, the Air Force view had a limited mechanism for environmental feedback. The 7th Air Force Commander depended on battlefield information from the III MAF ground force to drive decisions on changing command or control outputs.

The second-hand feedback required a higher level of judgment from the Air Force and likely slowed the TACS' responsiveness to III MAF needs. By implementing the TACS, MACV demonstrated that it favored the stability of a standing C2 process rather than betting on organizational relationships and personalities to accomplish the mission.

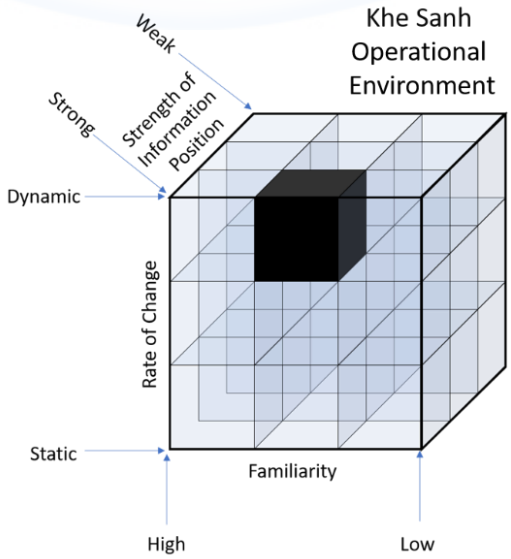

Figure 8: The Operational Environment at Khe Sanh
Source: Adapted from Alberts and Hayes, Understanding Command and Control

Did the centralized control structure fit the operational environment? Alberts' models, previously described in the C2 chapter, can help illuminate this subject. The character of the operational environment for the Battle of Khe Sanh, as depicted in Figure 8 above, is one of moderate familiarity, dynamic rate of change, and strong information position. The enemy is moderately familiar because the North Vietnamese Army rarely presented itself in a regular manner. Most of the battlefield skirmishes to this point were guerrilla warfare efforts led by the Viet Cong. Given the geographic and force size advantages of the NVA, the American forces could anticipate a dynamically changing and chaotic battlefield. Finally, the American advantage in intelligence, surveillance, and reconnaissance capabilities paired with a strong mechanism for intelligence distribution created a strong information position for the U.S. force. An appropriately aligned C2 framework would sit in the same place on the cube as the representation of the operational environment.

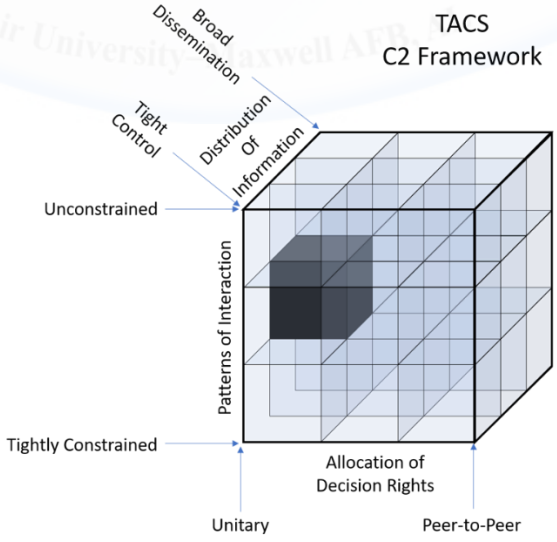

Figure 9: The TACS C2 Framework
Source: Adapted from Alberts and Hayes, Understanding Command and Control

The MACV TACS, as depicted in Figure 9 above, displayed unitary decision rights, moderately constrained patterns of interaction, and

moderately distributed information. The TACS has unitary decision rights due to the requirement for lower echelons to elevate issues to the highest level of the system before any non-emergency deviation beyond the original scope of the intent can occur. The patterns of interaction are numerous, but they happened according to tightly constructed procedures between ground units, C2 nodes, and supporting aircraft. Information within the MACV TACS varied in quality dependent upon the location in the structure. Some tactical nodes, such as TACPs or the ABCCC, may have had better awareness of the combat situation than the TACC. Limitations on information technology capabilities hindered real-time information sharing throughout the various levels of the TACS, however. This combination of characteristics places the MACV TACS C2 framework on the left face of the cube, representing a mismatch with the operational environment.

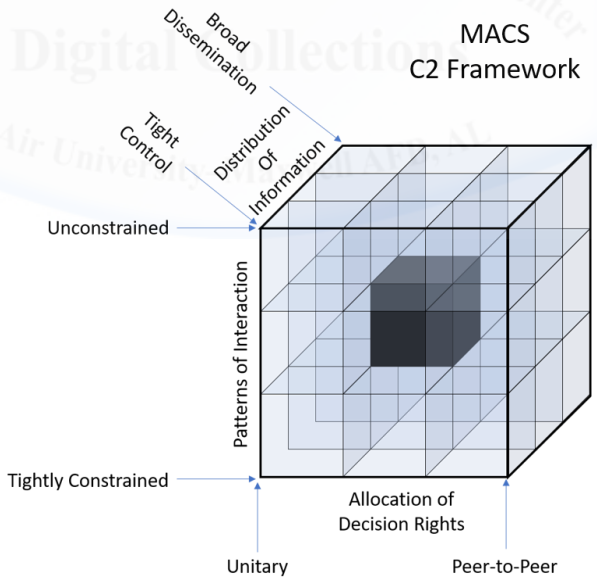

Figure 10: The MACS C2 Framework

Source: Adapted from Alberts and Hayes, Understanding Command and Control

Would the Marine Corps position have aligned any better by retaining OPCON of its fixed-wing aviation? Conceivably, the tight integration of the MACS at Khe Sanh would have displayed moderate

allocation of decision rights, moderately constrained patterns of interaction, and moderate distribution of information. The MACS model only varies from the TACS in the allocation of decision rights. The MACS structure would allow the ground commander to make decisions about fixed-wing aviation within his geographic location. However, 7th Air Force and SAC required the Marines to coordinate with them for any additional air power that was not organic to III MAF. This blend of attributes places the MACS model in the center of the cube.

In summary, neither the TACS nor the MACS were entirely appropriate for commanding and controlling fixed-wing aviation in the Battle of Khe Sanh. The eventual cooperation between the two Services led to a system that served both the needs of Khe Sanh ground commander and those of the larger theater.

Conclusion

The Air Force's doctrine of centralized control and decentralized execution exploits air power's unique capabilities of speed, range, versatility, and battlespace perspective. Its use of integrated air liaison elements such as TACPs, and other modern variants, fosters a highly integrated system to coordinate air support. Additionally, the employment of embedded or airborne tactical C2 elements is an elegant solution for knitting together tactical ground forces with operational air commanders in a complex operational environment.

The inflexibility of the TACS to tailor its structure and processes to unique mission demands is a weakness given the spectrum of operational environments in the present day. The centralization of information and decision rights at the senior element of the TACS is a limiting factor for distributed operations in more complex and rapidly changing environments. The next chapter will examine C2 considerations in such an environment, that of U.S. Special Operations.

Chapter 4

Command and Control of Special Operations

If the Air Force designed the TACS to emphasize standardized and repeatable processes to enable centralized control and decentralized execution, how does the military conduct C2 for distributed operations in a dynamically changing environment? Such an environment and operational approach is the trademark of special operations forces. SOF personnel pursue a unique approach to the problems of complexity, uncertainty, and change by investing in support relationships and agile organizational constructs designed to enhance the effectiveness of small teams. The unique cultural identity of the special operator developed over time with the involvement of policymakers responding to early failures for SOF integration.

On 24 April 1980, the U.S. military conducted a mission to rescue 53 Americans held in Tehran, Iran. Code-named Operation EAGLE CLAW, the mission not only failed to free the Americans but ended with the death of eight U.S. servicemembers.[1] The failure culminated a period of decline for Special Operations in the 1970s marked by significant funding cuts and distrust between Special Operations Forces (SOF) and the conventional military.[2] The failure of Operation EAGLE CLAW foreshadowed multi-service integration issues in 1983 for Operation URGENT FURY in Grenada. Although successful at the strategic level, U.S. military forces displayed a misuse of special operations, a lack of appropriate resources, and an inability to command and control joint operations.[3]

[1] Locher, "Defense Organization: The Need for Change," 359.
[2] United States Special Operations Command, "USSOCOM History: 20th Anniversary Edition," 5.
[3] Thornton, "How Setbacks and DoD Reform Led to the Creation of SOCOM," 1.

A Congressionally-directed investigation cited numerous causes for the interoperability issues within the Department of Defense. Policymakers cited poor operational planning, bureaucratic acquisitions processes, disconnected strategy and long-range policy, and inadequate inter-Service coordination as the primary sources for the Department of Defense's organizational deficiencies.[4] In response, Congress passed the Goldwater-Nichols act of 1986 in part to force the DoD to improve joint force integration and cooperation.

Later that year, Congress passed the Nunn-Cohen Amendment to the Goldwater-Nichols Act to correct perceived problems with inter-service rivalries and mismanagement of United States Special Operations Forces. As a result of the amendment, United States Special Operations Command (USSOCOM) activated on 1 June 1987 as a Functional Unified Combatant Command.[5] USSOCOM assumed the role of the DoD's advocate for Special Operations Forces that focused on improving operational continuity for both the indirect approach, foreign internal defense, and counterterrorism.[6] Congress hoped that a unified SOF command could tie the lessons from the past to a strong vision for the future:

> Retention of successful tactics from the past requires an effective institutional memory. Mechanisms to prevent the loss of valuable experience can preclude falling into preventable errors. Experience and trust go together. In a complex operation, the chain is only as strong as the weakest link.[7]

Congress believed that creating an organization focused solely on special operations would help retain lessons of the past and reduce the potential for operational breakdowns in the future. From the very beginning, policymakers worked to ensure that the vitality of

[4] Locher, "Defense Organization: The Need for Change," 15.
[5] United States Special Operations Command, "USSOCOM History: 20th Anniversary Edition," 7.
[6] McCombie, "Options for Command and Control of Special Operations," 5.
[7] Locher, "Defense Organization: The Need for Change," 362.

special operations was resident in its people and organizations rather than its processes and systems.

USSOCOM and the joint forces under its command grew into the world's premier special operations organization in the 31 years since the Nunn-Cohen Amendment.[8] Its relative separation from the conventional side of the DoD has created a strong, independent SOF identity that exhibits many characteristics of a separate service. As such, special operations personnel tend to have little experience with conventional forces outside of directed integration for combat missions.[9] The case study in the next section examines the successes and challenges of SOF and conventional integration in Afghanistan.

Special Operations C2 in Afghanistan

Shortly after the September 11th terrorist attacks, United States Central Command (USCENTCOM) tasked its Joint Force Special Operations Component Command (JFSOCC) to establish an unconventional warfare Joint Special Operations Task Forces (JSOTF) in Afghanistan.[10] The JSOTF, formed with personnel from Task Force (TF) DAGGER at Karshi-Khanabad (K2) Air Base in Uzbekistan, and its tactical forces and select factions of the Northern Alliance to defeat the governing Taliban and resident Al Qaeda forces.[11] The SOF-dominant team, paired with U.S. intelligence personnel and air support from the U.S. Air Force, facilitated Northern Alliance victories at Mazar-e-Sharif, Kabul, and Kunduz within two months.[12]

Despite its tactical success against the Taliban, TF DAGGER lacked the planning, joint fires, and logistics personnel to either sustain

[8] Bright, "Operational Seam: The Command and Control of Conventional and Special Operations Forces," 2.
[9] Martin, "Special Operations and Conventional Forces: How to Improve Unity of Effort Using Afghanistan as a Case Study," 30.
[10] United States Special Operations Command, "USSOCOM History: 20th Anniversary Edition," 104.
[11] Jackson, "Tactical Integration of Special Operations and Conventional Forces Command and Control Functions," 23.
[12] Jackson, 24.

current operations or plan future operations.[13] The Taliban's demise ushered in a new phase of Operation ENDURING FREEDOM that focused on conventional force operations to stabilize Afghanistan. A conventional force headquarters of the 10th Mountain Division, known as Combined Joint Task Force (CJTF) Mountain, succeeded TF DAGGER to lead the U.S. effort in late 2001.[14]

Special Operations Command Central (SOCCENT) maintained OPCON of SOF forces until November 2001.[15] At that point, CENTCOM re-tasked SOCCENT to lead the SOF planning effort for the U.S. invasion of Iraq and transferred OPCON of the JSOTF to the theater Combined Forces Land Component Command (CFLCC) in Kuwait.[16] The CFLCC delegated TACON of the JSOTF to CJTF-Mountain.[17] The JSOTF moved from K2 to Bagram Airfield to collocate with CJTF-Mountain and facilitate battlefield coordination.

Special operations personnel conducted reconnaissance, direct action, and unconventional warfare missions in Afghanistan, but without an official command relationship with SOCCENT, SOF personnel relied on conventional support for intelligence, communications, and planning.[18] This interdependence signaled a growing trend toward SOF and conventional force integration at the operational and tactical level.[19] In February 2002, CJTF-Mountain and the JSOTF began integrated

[13] United States Special Operations Command, "USSOCOM History: 20th Anniversary Edition," 104.
[14] Martin, "Special Operations and Conventional Forces: How to Improve Unity of Effort Using Afghanistan as a Case Study," 1.
[15] Jackson, "Tactical Integration of Special Operations and Conventional Forces Command and Control Functions," 31.
[16] Martin, "Special Operations and Conventional Forces: How to Improve Unity of Effort Using Afghanistan as a Case Study," 1.
[17] Jackson, "Tactical Integration of Special Operations and Conventional Forces Command and Control Functions," 31.
[18] Jackson, 28; Martin, "Special Operations and Conventional Forces: How to Improve Unity of Effort Using Afghanistan as a Case Study," 21.
[19] Jackson, "Tactical Integration of Special Operations and Conventional Forces Command and Control Functions," 35.

planning for a massive operation to crush Al Qaeda in Paktia Province of eastern Afghanistan.[20]

Operation ANACONDA was the first significant test for the operational and tactical integration of SOF and conventional forces in Afghanistan. The operation aimed to isolate and encircle the Shah-i-Khot Valley, followed by converging attacks against Al Qaeda forces.[21] The 10th Mountain and elements of the 101st Airborne Division comprised the mission's nearly 1,000-member conventional force. The SOF elements included six Operational Detachment-Alpha (ODA) teams, three SOF C2 elements, and a brigade of U.S.-trained Afghan Military Forces.

Preparation for the battle uncovered a lack of intelligence data on the enemy disposition. Despite significant U.S. capabilities in human intelligence, signals intelligence, and overhead ISR, the rugged and inaccessible terrain, poor weather, and enemy concealment created uncertainty in the planning process. The U.S. estimated that 200-300 Taliban and Al Qaeda forces were in the area when there were likely closer to 700-1,000 enemy fighters in the area. [22] Intelligence analysis also underestimated the presence of heavy armaments including rocket-propelled grenades, mortars, and artillery pieces.[23] Most importantly, the U.S. mistakenly believed that Al Qaeda and Taliban fighters lacked the resolve to make a stand in the Shah-i-Khot Valley. In reality, the enemy fighters declared "jihad" with no intention of ceding the valley without significant resistance.[24]

Another shortfall of the planning process was the failure to involve the Combined Forces Air Component Commander (CFACC) staff to coordinate tactical air support. CJTF Mountain planners considered

[20] United States Special Operations Command, "USSOCOM History: 20th Anniversary Edition," 98.
[21] United States Special Operations Command, 98.
[22] Kugler, "Operation Anaconda in Afghanistan: A Case Study of Adaptation in Battle," 5.
[23] Kugler, 6.
[24] Kugler, 7.

Operation ANACONDA as a ground assault in which Air Force assets would only play a minor supporting role and, therefore, did not notify the CAOC of the impending operation until the CJTF issued the initial OPORD on February 20.[25] CAOC planners proposed intense saturation bombing to prep the environment for a ground assault but were denied by CJTF Mountain to maintain the element of surprise.[26] The CFACC's assigned role, instead, was to provide airlift resupply, limited deliberate strikes on the first day, and on-call close air support. The limited intelligence preparation combined with minimal CFACC involvement limited the coalition's ability to manage and mitigate risk for the operation.

Operation ANACONDA was a complex and ambitious mission even without the planning shortfalls.[27] On 1 March, about 600 SOF-led AMF would move into position along the routes of retreat. CJTF Mountain would air assault into an inner ring of blocking positions along the eastern face of the valley. Finally, the main force of ODAs and AMF would assault the valley, forcing the elimination of the exposed Al Qaeda elements. Both conventional and special operations forces worked in close proximity while pursuing the same tactical objective, Objective REMINGTON.[28] In this case, the conventional force served as the supporting effort to the SOF and Afghan main body.

In war, however, missions rarely go as planned. Three SOF teams experienced heavy fire while validating the landing zones and high-value targets during the reconnaissance phase of the mission. A separate SOF convoy experienced difficulties navigating the unimproved Afghan roads, forcing several trucks to slide off or break down. While several vehicles left the formation to secure a blocking position, they came under fire

[25] Kugler, 13.
[26] Kugler, 13.
[27] United States Special Operations Command, "USSOCOM History: 20th Anniversary Edition," 98.
[28] Jackson, "Tactical Integration of Special Operations and Conventional Forces Command and Control Functions," 32.

from a U.S. AC-130 gunship, killing a U.S. SOF operator and two Afghan troops and wounding more than a dozen others.[29] As the battle intensified on 2 March, the enemy force shot down a helicopter carrying a SEAL team en route to secure an observation post. Three hours later, a rocket-propelled grenade struck one of the two helicopters in the quick reaction force sent to rescue the SEALs.

The late involvement of the CFACC's planners led to ineffective or misunderstood command relationships for the control of air power. Requests for non-emergency strike sorties had to go to the CAOC for approval. In such a case, the approval process took up to 45 minutes due to the standardized procedures of the TACS[30]. In some instances, the CAOC denied requests for non-emergency CAS due to their determination that it did not meet the authorization criteria. As the battle progressed, the CAOC and CJTF cleared up misunderstandings about the rules of engagement, virtually permitting strikes against all enemy targets at the ground commander's discretion.[31]

On 4 March, the conventional forces continued the fight by conducting an air assault to assume battle positions. The Afghan military, accompanied by an ODA element, launched a reconnaissance team to observe enemy movements in the valley and coordinate air strikes against fortified positions. After an operational hold of several days to await further Afghan militia reinforcements, the combined SOF and conventional force cleared Objective REMINGTON of enemy resistance.[32]

The tragic loss of eight U.S. personnel combined with bad weather, difficult terrain, and poor air-ground coordination overshadowed the tactical success of Operation ANACONDA.[33] Coalition conventional and

[29] Kugler, "Operation Anaconda in Afghanistan: A Case Study of Adaptation in Battle," 15.
[30] Kugler, 18–19.
[31] Kugler, 19.
[32] United States Special Operations Command, "USSOCOM History: 20th Anniversary Edition," 103.
[33] Franks, *American Soldier*, 379.

SOF forces killed more than 800 Al Qaeda operatives, however, and cleared the last refuge for the terror cell in Afghanistan. Coalition forces would not face similar concentrations of Al Qaeda or Taliban adversaries again until 2006.

Special Operations Case Study Analysis

The accomplishments of SOF in the aftermath of 9/11 represented the determination of the United States to seek out and eliminate terrorist safe havens across the globe. The special operators demonstrated the ability to adapt to rapidly changing battlefield conditions to bring the full weight of the American military instrument of power to bear. As the conditions changed, SOF personnel leveraged an agile C2 structure to synchronize U.S. government and coalition military efforts toward a common objective.

The SOF C2 framework in Afghanistan had numerous sources of strength. First, the special operations model is rapidly scalable to support distributed operations. Special operations campaigns typically operate with a small footprint to maintain a posture of low-visibility. As either mission complexity or the number of teams in the battlespace increases, the SOF framework allows for a nearly limitless number of tactical C2 nodes to synchronize the fight. In the first year of OEF, the U.S. and its coalition partners employed a variety of CFSOCCs, JFSOCCs, JSOTFs, and SOTFs to provide oversight of special operations missions and assist with integrating SOF efforts with conventional headquarters and missions.

Second, the scalability of the SOF C2 structure allows for continuous integration with conventional fires support. As demonstrated in Operation ANACONDA, special operations forces have embedded mechanisms such as JTACs, combat controllers, and JSOTF fires teams that understand the TACS and Army Fires Support system. By integrating on-demand conventional fires, SOF teams can remain small while still maintaining adequate firepower when required.

Third, having a scalable and integrated framework fosters the ability to tailor the C2 structure to the characteristics of each unique mission.[34] In the initial entry phase of OEF, TF DAGGER leveraged a SOF-centric model that emphasized the low-visibility, yet strategically focused, nature of special operations missions.[35] As missions became more complex and required in-depth planning and support, TF DAGGER evolved into a JSOTF that was TACON to a much larger conventional force. If TF DAGGER and its SOF missions were the main effort, why was the conventional force not TACON to TF DAGGER? Having special operators lead the SOF mission would have been a better solution in this instance. One of the shortfalls with dynamic command relationships is that the U.S. military sometimes misapplies importance to the entity with the most resources instead of that is with appropriate expertise and mission focus.

Finally, the success of U.S. special operations leveraged unified action through a whole-of-government approach.[36] The SOF C2 framework includes LNOs or touchpoints from the U.S. State Department, the intelligence agencies, and foreign partners.[37] Beyond the C2 nodes themselves, the intelligence community and foreign militaries are frequent contributors at the tactical unit level. Thus, SOF's mutually supporting relationship with its mission partners fosters unified action on the battlefield.

In addition to its numerous strengths, the SOF C2 model demonstrated several weaknesses. The first weakness of the distributed C2 model is that it often relies on informal or unofficial support relationships that are personality based and not repeatable for enduring campaigns. In the Army counterinsurgency manual, former

[34] Department of the Army, Special Forces Operations, 1–17.
[35] Lehman, "Command and Control in the Gray Zone: The Advantage of SOC-FWDs," 31.
[36] Lehman, 33.
[37] Tisdel, Taske, and Fleser, "Theater Special Operations Commands Realignment," 11.

USCENTCOM Commander GEN Anthony Zinni describes SOF relationships as "Hand Shake Con":

> [There is] no memoranda of agreement or memoranda of understanding. The relationships are worked out on the scene, and they aren't pretty. And you don't want to try to capture them or distill them. As you go off in the future, [you might not] have this sort of command relationship. It is Hand Shake Con and that's the way it works. It is consultative. It is behind-the-scenes.[38]

GEN Zinni highlights the weakness of the SOF C2 framework when compared with the TACS. The SOF method is an organizational approach that relies on individual personalities and relationships for success. The TACS is a standardized system that relies on process over personality. While not abandoning its organizational model, perhaps the SOF method could emphasize processes that foster collaboration with conventional forces instead of purely relying on either official or back-door support relationships.

Although a strength of the SOF C2 framework is its flexibility, that same characteristic causes interoperability problems with the conventional force. As the SOF C2 nodes continuously adapt to the operational environment, communication and coordination can break down with conventional forces in the shared or adjacent battlespace.[39] The tendency for special operations to employ strict operational security measures exacerbates the lack of communication.[40] It is imperative that both SOF and conventional forces mitigate the issue by exchanging LNOs to foster effective integration.[41]

Finally, the SOF operational model is a thoroughly human endeavor and its C2 structure requires a significant investment in

---

[38] Department of the Army, Counterinsurgency, 2–3.

[39] Martin, "Special Operations and Conventional Forces: How to Improve Unity of Effort Using Afghanistan as a Case Study," 11.

[40] Martin, 20.

[41] Jackson, "Tactical Integration of Special Operations and Conventional Forces Command and Control Functions," 35.

human capital.[42] With the focus oriented on the tactical fight, many Theater Special Operations Commands (TSOCs) cannot support the operational-level planning and execution of Geographic Combatant Command priorities.[43] This problem played out in the Operation ANACONDA scenario and frequently manifests itself in an over-reliance on support relationships with conventional forces.

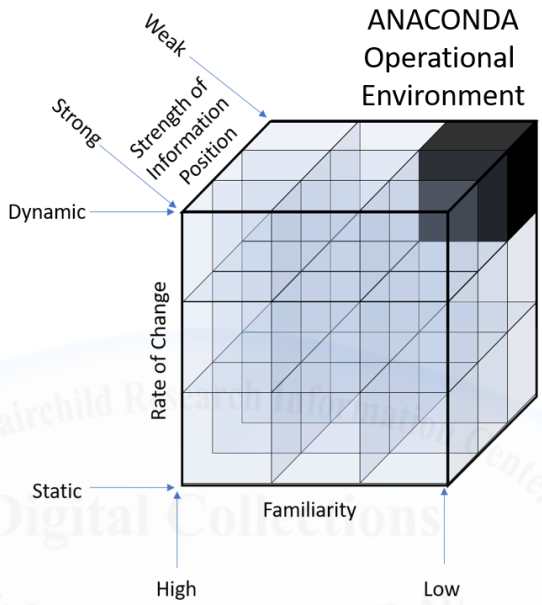

Figure 11: The ANACONDA Operational Environment
Source: Adapted from Alberts and Hayes, Understanding Command and Control

Did the Special Operations model in the early stages of OEF fit the operational environment? The operational environment for Operation ANACONDA, as depicted in Figure 11 above, was one of low familiarity, a dynamic rate of change, and a weak strength of information position. The U.S. was unfamiliar to both its Taliban and Al Qaeda adversaries and the harsh Afghanistan terrain. The nature of the response to the 9/11 terrorist attacks created a unique circumstance that permitted little pre-deployment training or intelligence preparation of the operational environment (IPOE). The lack of a well-developed IPOE left those on the

[42] Lehman, "Command and Control in the Gray Zone: The Advantage of SOC-FWDs," 33.
[43] Tisdel, Taske, and Fleser, "Theater Special Operations Commands Realignment," 11.

ground with limited appreciation of the dynamic environment of the battlespace. A highly developed battlefield can help create stability by illuminating the risks and uncertainty to friendly forces. Without such clarity, the U.S. forces had an unquenchable appetite for intelligence information with only a modest ability to fulfill those requirements. An appropriately aligned C2 framework for Operation ANACONDA would sit in the same place on the cube as the representation of the operational environment.

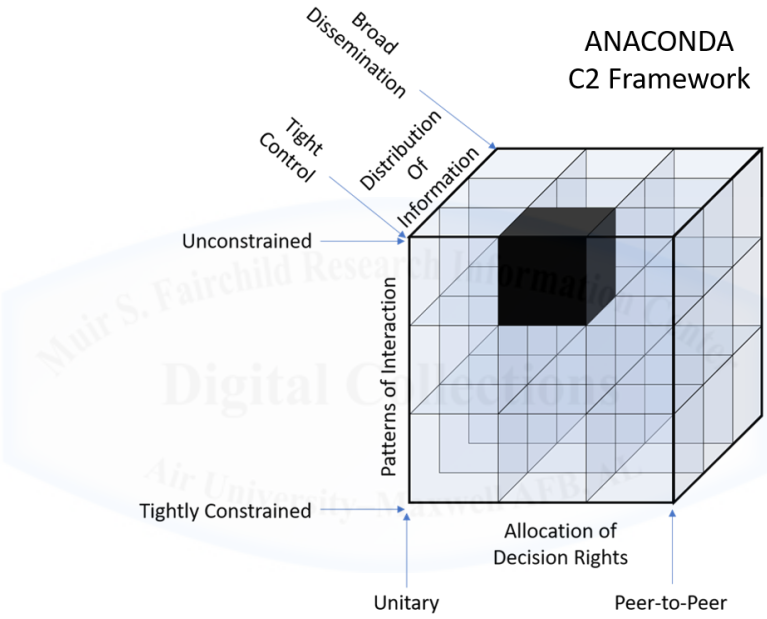

Figure 12: The ANACONDA C2 Framework
Source: Adapted from Alberts and Hayes, Understanding Command and Control

Operation ACACONDA's C2 model, as depicted in Figure 12, displayed moderately allocated decision rights, unconstrained patterns of interaction, and tightly controlled information distribution. CJTF Mountain's TACON relationship over SOF forces de-emphasized the special operations nature of the mission. This conventional force led relationship contributed to insufficient coordination with mission partners, such as the CFACC's CAOC, and created unity of command issues for the effective employment of air power. Interaction and

collaboration for the mission were unconstrained, but the CJTF failed to involve all the participants required for a successful operation. Finally, the SOF reliance on secrecy and OPSEC as a means of surprise created a moderate distribution of information between friendly forces on the battlespace. This combination of characteristics places the C2 framework at the top and center of the front face of the cube.

Therefore, a mismatch exists between the operational environment of Operation ANACONDA and the SOF C2 framework. The appropriate utilization of LNOs and employment of embedded tactical unit enablers mitigated some of the effects of the mismatch. A more carefully considered support relationship between SOF forces and their larger conventional counterparts may have corrected the planning and execution deficiencies of the battle.

Special Operations C2 Conclusion

The Special Operations Forces' model of distributed operations exploits its unique ability to leverage unified action and flexibility to deliver strategic effects at the tactical level in a dynamically changing environment. While it is tailorable to the mission, SOF C2 nodes and tactical maneuver units integrate well with existing conventional fires frameworks, such as the Air Force's TACS.

The SOF C2 model requires extensive human capital and relies on informal and sometimes misaligned support relationships to thrive in a shared battlespace. In such an environment, the cultural secrecy that fuels SOF success hinders its coordination and integration with conventional forces.

Building on the lessons learned from the air power and special operations command and control models, the next chapter will examine the unique considerations of nonlethal operations in the cyberspace domain.

Chapter 5

Command and Control of Cyberspace Operations

The air power and SOF case studies show that command and control structures often emphasize the strengths of a domain or mission while minimizing its weaknesses. How, then, does the DoD command and control cyber warfare when the cyberspace domain's advantages are also its weakness?

Cyberspace-enabled capabilities provide the means for the U.S. military and its allies to gain and maintain a strategic advantage in the joint operational environment.[1] Joint Publication 3-12 *Cyberspace Operations* points to a self-imposed security paradox of a highly connected society by noting that "the prosperity and security of our Nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and critical dependence on cyberspace."[2] Balancing and mitigating the adverse effects of the military's reliance on cyberspace capabilities is a primary role of cyberspace professionals.

The DoD's earliest attempts at conducting cyberspace operations involved ad-hoc technical specialists loaned from disparate organizations executing underdeveloped tactical concepts.[3] The increasing dependence of both the American public and the U.S. military on information technology capabilities drove the need for a different approach. The Department of Defense established United States Cyber Command (USCYBERCOM) in 2009 as a subordinate unified command under United States Strategic Command with an initial charge to protect the

[1] Joint Chiefs of Staff, Cyberspace Operations, v.
[2] Joint Chiefs of Staff, v.
[3] Nakasone, Opening Remarks for Lieutenant General Paul Nakasone, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 1.

"dot-mil" network.[4] Since its conception, USCYBERCOM has matured and evolved into a highly-potent force capable of conducting daily operations against adversaries around the globe. The command's mission now involves directing, synchronizing, and coordinating cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.[5]

The DoD categorized cyberspace operations missions into three distinct lines of effort to pursue military objectives while balancing the availability and security of information.[6] Offensive cyberspace operations (OCO) project power by the application of force in and through the domain.[7] Defensive cyberspace operations (DCO) aim to defend the department's interests in cyberspace. Finally, DoD information network operations (DoDIN Ops) include actions that "design, build, configure, secure, operate, maintain, and sustain DoD communications systems and networks in a way that creates and preserves data availability, integrity, and confidentiality."[8]

The combined effects of OCO, DCO and DoDIN Ops missions represent the tactical cyberspace actions supporting USCYBERCOM and Geographic Combatant Commander objectives. In an acknowledgment of cyber warfare's role in the changing character of the battlefield, CJCS Gen Joseph Dunford stated:

> Advancements in space, information systems, cyberspace, electronic warfare, and missile technology have accelerated the speed and complexity of war. As a result, decision space has collapsed, and we can assume that any future conflict will involve all domains and cut across multiple geographic regions.[9]

---

[4] Gibney, "Centralized Offense, Decentralized Defense: Command and Control of Cyberspace," 54.
[5] Nakasone, Advance Policy Questions for Lieutenant General Paul Nakasone, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 10.
[6] Lundgren, "Examining Command and Control Constructs for Offensive Cyberspace Operations," 17.
[7] Joint Chiefs of Staff, Cyberspace Operations, vii.
[8] Joint Chiefs of Staff, vii.
[9] Dunford, "From the Chairman: The Character of War and Strategic Landscape Have Changed," 2.

While Gen Dunford correctly identifies the impact of IT and cyber warfare capabilities on modern conflict, the thinking that guides their employment is not different from that of the traditional warfighting domains. There are unique and nuanced aspects of cyber warfare and the cyberspace domain, however. Understanding those differences is imperative to an effective multi-domain fight.

Cyberspace Operational Environment

Cyber warfare broadly uses or considers many traditional warfighting concepts such as terrain, mass, objective, maneuver, and surprise.[10] While cyber warfare has similarities with its traditional counterparts, there are a few fundamental differences that planners must understand. The three main categories of cyber-specific considerations include the nature of the domain, nuances of operating *in* the domain, and the physical infrastructure that creates the domain.

The nature of the cyberspace domain is its most unique consideration. Today's hyperconnected society gives single individuals access to billions of people and limitless information, making the massive cyberspace domain can feel exceptionally small. That same open and connected nature has implications for cyber warfare. One of the most famous malicious computer worms, known as NIMDA, took less than 22 minutes from its introduction to the Internet to become the most widespread virus in the world.[11] In both theory and practice, the cyberspace domain does not subscribe to the geographic boundaries of the physical world. State and non-state actors, therefore, can use networked capabilities that do not reside in their physical territory to carry out attacks.[12] On the other hand, it is exceptionally challenging to confine the impact of an attack, and its secondary or tertiary effects, to a

[10] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 84–120.
[11] Rodriguez, "USCYBERCOM: A Centralized Command of Cyberspace," 11.
[12] Wood, "USCYBERCOM: Right Solution, Wrong C2 Structure," 10–11.

specific target or geographical area.[13] This limitation could cause an adversary to perceive a targeting error as an intentional escalation, thereby giving strategic implications to tactical operations.

In addition to cyberspace's unique nature, there are nuances involved in operating within the domain itself. Planning and executing an OCO mission is quite often a deliberate and time-consuming process that requires intense intelligence preparation, mission-tailored techniques, tactics, procedures (TTPs), customized weapons, national command authority permissions.[14] Even after carefully constructing the IPOE and TTPs, a weapon may work once, twice, or not at all.[15] Cyber warfare personnel operate with the assumption that once used, attack methods are a part of the public domain and competent adversaries will eliminate that vulnerability or avenue of approach to render the weapon effectively useless in the future.[16] The uncertainty of OCO capabilities and effects is a foreign concept to military personnel accustomed to the predictability and repeatability of kinetic attacks.[17]

Many planners believe the cyber warfare barriers to entry are low; however, this common belief is misleading. Any skilled actor with a computer and access to the Internet can theoretically conduct a cyber-attack. Operating consistently, effectively, and in a disciplined manner, however, takes a considerable amount of physical infrastructure.[18] Cyber warfare and its associated support mechanisms require specialized network infrastructure, data analysis capabilities, isolated training ranges, and situational awareness tools to plan, execute, and C2 missions in the domain.[19] Organizing for cyber warfare, therefore,

---

[13] Connary, "Computer Network Operations Command and Control: A New Perspective," 13.
[14] Gibney, "Centralized Offense, Decentralized Defense: Command and Control of Cyberspace," 86.
[15] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 47.
[16] Gibney, "Centralized Offense, Decentralized Defense: Command and Control of Cyberspace," 87.
[17] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 47.
[18] Lundgren, "Examining Command and Control Constructs for Offensive Cyberspace Operations," 25.
[19] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 121–39.

requires a thoughtful and deliberate approach to create the infrastructures that will enable the capability and capacity of the desired force.

The nature of the domain, nuances of operating *in* the domain, and the physical infrastructure that creates the domain are driving factors for why traditional military members misunderstand cyber warfare. These three considerations have also driven USYCBERCOM to construct its command and control framework in a manner vastly different from other DoD organizations.

Cyberspace Operations Command and Control

Since its inception, USCYBERCOM has leveraged the unique characteristics of the cyberspace domain to command and control its forces. Internet connectivity and information technology systems allow commanders to control operations from extreme distances.[20] While building its capabilities and processes, USCYBERCOM exercised centralized command and control of cyberspace operations.

The cyberspace C2 organizational construct, illustrated in Figure 13 below, was the DoD's first attempt to standardize the command and control architecture across the department by balancing regional and global cyber priorities.[21] The Commander of USCYBERCOM controlled the day-to-day management of cyberspace operations while its parent organization, U.S. Strategic Command, retained COCOM authority.[22] The GCCs were the supported commanders for cyberspace operations with first order effects within their AORs. Except for USCYBERCOM's role as a subordinate unified functional command providing direct support to the GCCs, these command relationships were nothing new as they closely mirrored the frameworks of other functional commands.

[20] Smail, "Designed to Win: An Agile Approach to Air Force Command and Control of Cyberspace," 10.
[21] Office of the Secretary of Defense, Cyberspace Command and Control Execution Order, 1.
[22] Joint Chiefs of Staff, Cyberspace Operations, IV–6.

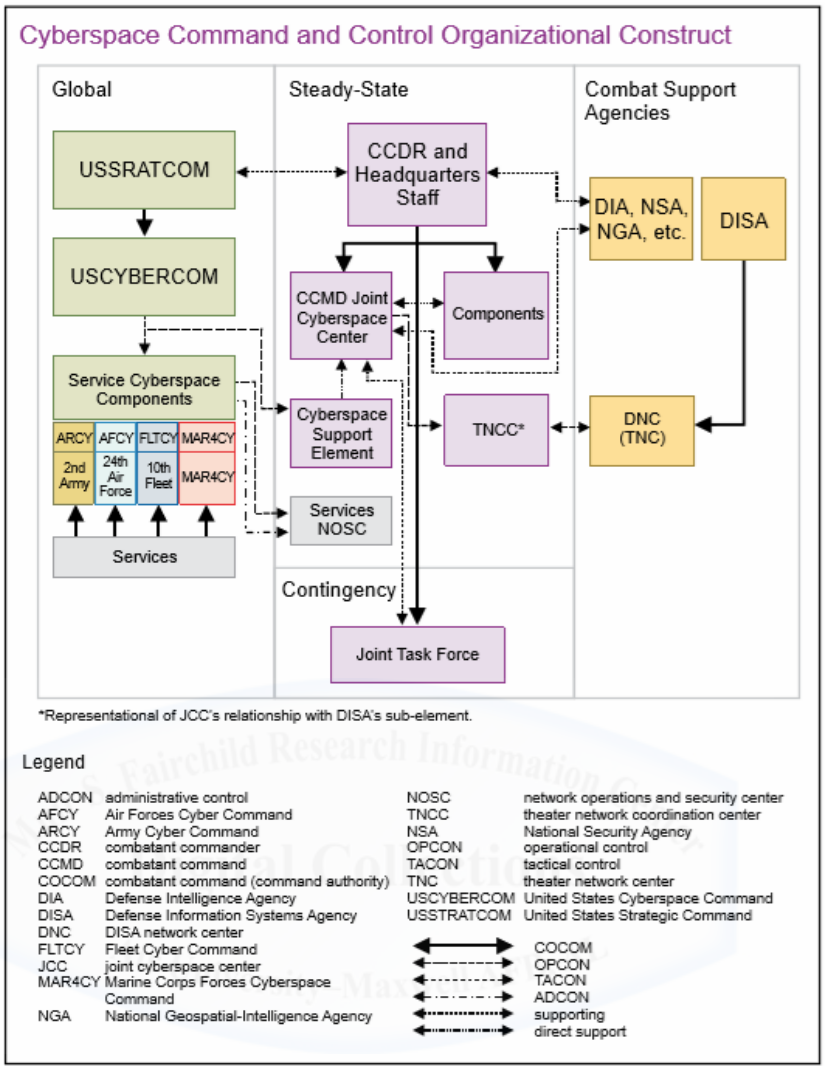

Figure 13: Cyberspace C2 Organizational Construct (Circa 2013)
Source: Joint Chiefs of Staff, JP 3-12 Cyberspace Operations

Coordination of cyber operations between USCYBERCOM and the GCCs occurred through the deliberate employment of liaison elements. In 2012, each GCC established a Joint Cyber Center (JCC) to integrate and synchronize cyber operations within their respective area of responsibility (AOR).[23] USCYBERCOM, in turn, deployed cyberspace support elements (CSEs) to the JCC to facilitate, coordinate, integrate, and deconflict cyberspace operations requirements within the GCC's

[23] Joint Chiefs of Staff, IV–7.

planning process, when necessary.[24] The CSE remained under OPCON of USCYBERCOM and provided direct support to the JCC.[25]

The cyberspace C2 organizational construct fell short in some key areas. First, collaboration between USCYBERCOM and the GCCs was event-driven and sporadic. As the CSE was only a temporarily deployed contingent, USCYBERCOM did not maintain a persistent and integrated relationship with the JCC or GCC staffs. Second, the service cyber components did not have a standardized method to present forces and capabilities to the GCCs. Gen Keith Alexander, USCYBERCOM's first commander, noted that both issues were the result of "not having the capacity to do everything."[26] The lack of capacity forced USCYBERCOM to choose between building tactical capabilities at the team level or fostering improved integration at the GCCs.

As the DoD struggled to integrate cyber warfare into its operational plans, USCYBERCOM shifted its focus to building a standardized force presentation model. In late 2012, the Deputy's Management Action Group (DMAG) endorsed the first cyberspace presentation model, effectively establishing the DoD Cyber Mission Force (CMF).[27] The CMF built upon existing units and contained three distinct elements: the cyber national mission force (CNMF), the combat mission force, and the cyber protection force. The combat mission force and cyber protection force directly support CCMDs through OCO-oriented combat mission teams (CMT), DCO-oriented cyber protection teams (CPTs), and cyber-intel cyber support teams (CSTs). The introduction of CMTs, CPTs, and CSTs actualized USCYBERCOM's desire to standardize its force presentation to the CCMDs.

[24] Joint Chiefs of Staff, III–6.
[25] Joint Chiefs of Staff, III–7.
[26] Rodriguez, "USCYBERCOM: A Centralized Command of Cyberspace," 13.
[27] Office of the Secretary of Defense, Cyberspace Command and Control Execution Order, 1.

As the Cyber Mission Forces matured, it became evident that Joint Force Commanders needed a more robust cyber command and control structure to better support their requirements. The DoD approved the creation of a Joint Force Headquarters-Cyber (JFHQ-C) within each service cyber component to provide operational-level C2 for the CCMDs.[28] In practice, the JFHQ-C Commander is a "dual-hat" responsibility for the service component commander. Adding to the traditional service roles of organize, train, and equip, the service component commanders' portfolio expanded to include warfighting authorities in support of multiple CCMDs.

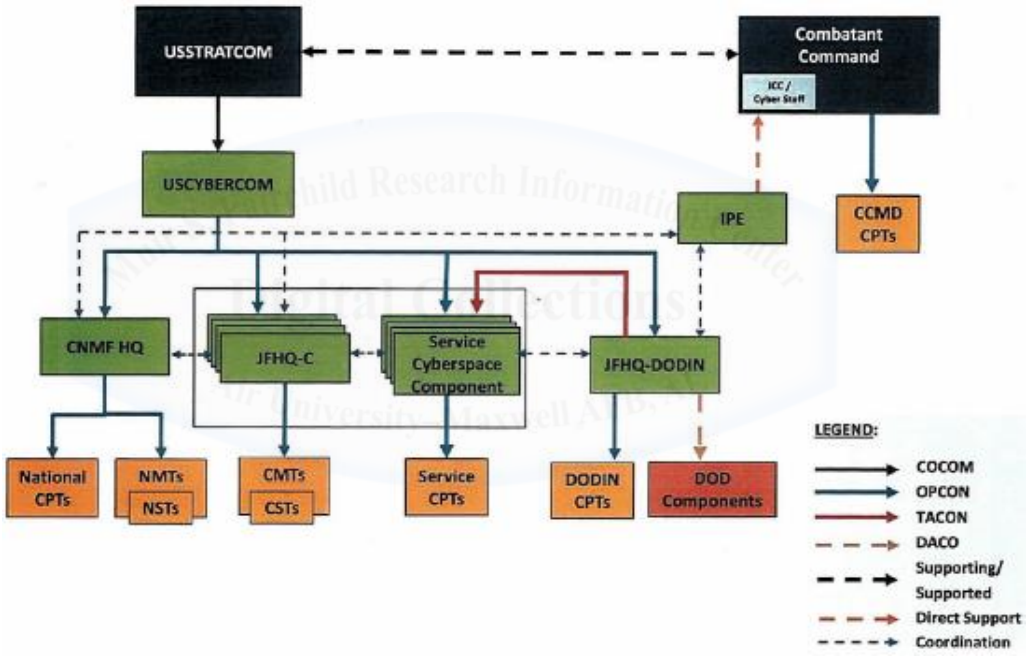

Figure 14: Cyberspace C2 Organizational Construct (Circa 2017)
Source: Office of the Secretary of Defense, Cyberspace Command and Control Execution Order, 10

In the 2017 iteration of the cyberspace command and control organizational construct, depicted in Figure 14, the DoD looked to codify the relationships between the CMF, JFHQ-Cs, and CCMDs. In the new structure, CCMDs exercise OPCON of their assigned DCO-oriented CPTs.

[28] Nakasone, Advance Policy Questions for Lieutenant General Paul Nakasone, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 11.

USCYBERCOM, however, retains OPCON of all other CMF forces. The dual-hatted service cyber components and JFHQ-Cs exercise OPCON on behalf of USCYBERCOM for all CMTs, CSTs, and service-retained CPTs.[29] USCYBERCOM located the JFHQ-Cs in proximity to elements of the National Security Agency at NSA-Washington, NSA-Texas, NSA-Georgia, and NSA-Hawaii to foster unified action and mutual support for national security objectives.[30]

Collaboration and integration with the CCMDs continued to challenge the fledgling cyber force. In a February 2018 testimony to the Senate Armed Services Committee, USCYBERCOM Commander ADM Mike Rogers reinforced the notion of treating the command as "a high-demand, low-density resource, where we have to acknowledge there's not enough capacity to do everything we want."[31] To address the problem, the DoD directed USCYBERCOM to stand up a Cyber Operations – Integrated Planning Element (CO-IPE) at each CCMD.[32] While the CO-IPE performs planning and integration liaison functions similar to the now-defunct CSE, it differs in a couple of ways. Once fully stood up, USCYBERCOM will permanently integrate and collocate the CO-IPE with the CCMD as opposed to the CSE's event-driven deployment model. Whereas the CSE was an extension of USCYBERCOM, the CO-IPE is a forward extension of the JFHQ-C.[33] The new C2 structure for cyber forces is USCYBERCOM's attempt to prioritize national level guidance with adversary activity, employing its low-density, high-demand force in

[29] Gargan, "The Joint Force Air Component Commander and the Integration of Offensive Cyberspace Effects," 89.
[30] Office of the Secretary of Defense, Cyberspace Command and Control Execution Order, 2.
[31] Rogers, Hearing to Receive Testimony on United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2019 and the Future Years Defense Program, 46.
[32] Office of the Secretary of Defense, Cyberspace Command and Control Execution Order, 4.
[33] Pomerleau, "Cyber Command Stands up Planning Cells at Combatant Commands," 3.

a manner that supports both national and Combatant Commander objectives.[34]

Cyberspace Operations C2 Analysis

USCYBERCOM made significant progress in building the capacity of its tactical forces while continuing to pursue better integration with the combatant commands. For a command that is less than a decade old, that is a significant achievement that is lauded by policymakers and combatant commanders alike.[35] Is the latest cyberspace command and control organizational construct the ideal design for cyber warfare joint force integration? The challenge for USCYBERCOM is to operate within a C2 framework that leverages the beneficial aspects and mitigates the negative features of the cyberspace domain while balancing the low-density and high-demand character of cyber warfare capabilities.

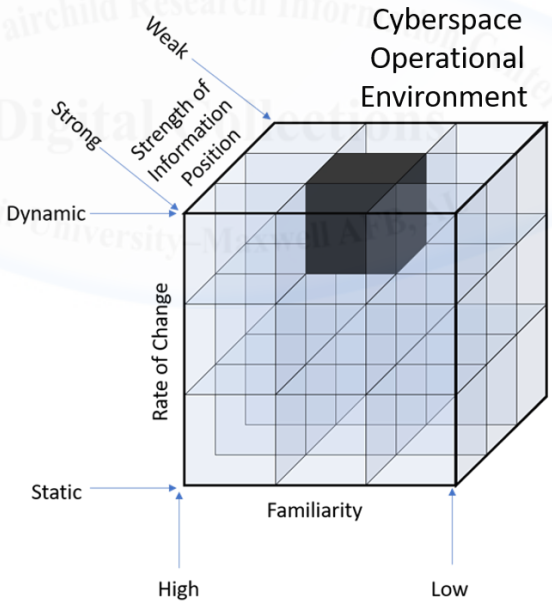

Figure 15: The Cyberspace Operational Environment
Source: Adapted from Alberts and Hayes, Understanding Command and Control

[34] Nakasone, Advance Policy Questions for Lieutenant General Paul Nakasone, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 17.
[35] Rogers, Hearing to Receive Testimony on United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2019 and the Future Years Defense Program, 79.

The cyberspace operational environment, depicted in Figure 14 above, is one of moderate familiarity, dynamic rate of change, and moderate strength of information position. The actors and potential adversaries in the cyberspace domain are vast, driving the moderate degree of familiarity. It is not only possible but likely that the DoD will have a high level of familiarity against a known and operationally prioritized adversary. It is virtually impossible, however, for the DoD to have a rich familiarity with all actors in cyberspace. The rate of change in the operational environment is extremely dynamic. Information networks are constantly changing and expanding, regularly applied security patches eliminate vulnerabilities, and the mix of humans interacting with the domain changes frequently as well. Finally, the strength of information position is moderate due to the character of both the familiarity of adversaries and the rate of change. The continuously changing environment drives an insatiable demand for intelligence. If properly prioritized and deliberately planned, it is possible to have a strong information position for a specified window of time. The continual improvement of cyber intelligence capabilities can strengthen the enduring information position as USCYBERCOM and the CMF mature. An appropriately aligned cyber C2 framework would sit in the same place on the cube as the representation of the operational environment.

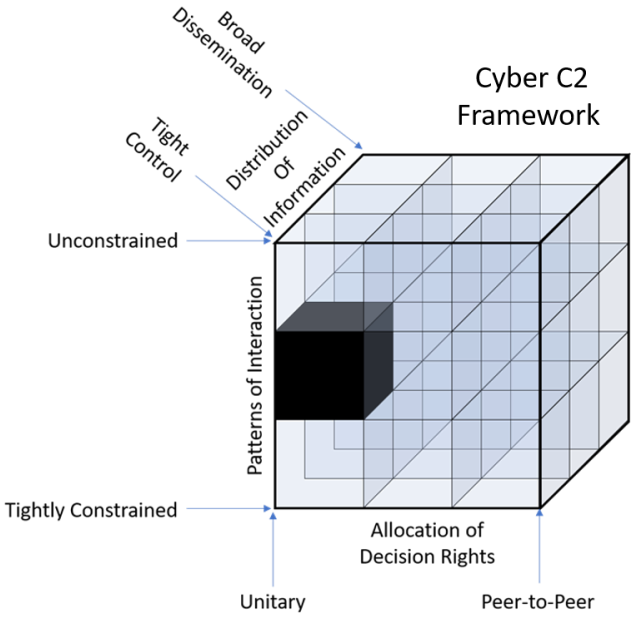

Figure 16: The Cyberspace C2 Framework

Source: Adapted from Alberts and Hayes, Understanding Command and Control

Creating an effective means to command and control cyber operations with significant personnel and infrastructure constraints is a challenge. The 2017 cyberspace C2 framework exhibited unitary decision rights, moderately constrained patterns of interaction, and tightly controlled information distribution. The C2 framework, therefore, is a mismatch with the cyberspace operational environment.

One of the significant challenges in the C2 framework is the allocation of decision rights. The cyberspace domain is not well understood by traditional military professionals. Policy makers and military leaders, therefore, are still working to figure out how cyber warfare fits into traditional military operations. Many tactical actions require Presidential or SECDEF approval to tightly control the risk and uncertainty of cyber warfare.[36] USCYBERCOM utilizes cyberspace capabilities to direct operations from extreme distances, thus eliminating

[36] Gibney, "Centralized Offense, Decentralized Defense: Command and Control of Cyberspace," 104.

layers of hierarchical command between the "trigger puller" and the decision maker.[37]

The 2017 C2 framework decentralizes control to an extent by allowing the JFHQ-C to exercise OPCON of CMF OCO missions. That control, however, is still highly centralized within the JFHQ-C. Describing the JFHQ-C AFCYBER structure illustrates this point. JFHQ-C AFCYBER is responsible for supporting USEUCOM, USTRANSCOM, and USSTRATCOM cyber operations missions. The Cyber Mission Force construct does not include team-level commanders by design. The most *junior* cyber warfare commander supporting USEUCOM is, therefore, the two-star general JFHQ-C AFCYBER Commander who works day-to-day in San Antonio, Texas. That same commander is the most *junior* cyber warfare commander for USTRANSCOM and USSTRATCOM missions. The breadth of responsibility and the high retention of command authority creates a centralized command and control model that underpins the entire cyber C2 framework.

The patterns of interaction for the 2017 C2 framework are moderately constrained yet improving. The decision to integrate the CO-IPE into the staff of the CCMD on a permanent basis is the right decision. As noted in the air power and SOF cases, liaison elements are critical enablers to effective command and control because they facilitate trust, shared awareness, and meaningful collaboration. The C2 framework does not integrate far enough, however. Limiting formally recognized liaison efforts to the CCMD staff creates a void between the non-cyber tactical forces at the battalion or squadron level and the highest level of command in the AOR.

The current framework does facilitate positive collaboration between the various cyber forces, however. The collocation of JFHQ-C organizations with elements of the NSA enables rich interaction between

[37] Smail, "Designed to Win: An Agile Approach to Air Force Command and Control of Cyberspace," 10.

Title 10 DoD forces and Title 50 Intelligence Community enablers, supporting unified action in cyberspace. The DoD benefits from this mutual dependency as USCYBERCOM and the JFHQ-Cs currently rely on NSA infrastructure and capabilities to perform its mission.[38]

Tight controls on information distribution due to the nature of the cyber domain limit the 2017 C2 framework. In a dynamically changing environment with mission-tailored weapons, it is an operational imperative to closely guard information and secrets about cyber warfare missions. Operational and technical information, therefore, is highly classified and only shared with a validated justification.[39] Tightly controlled information in a congested operational environment could reasonably create a scenario where multiple government agencies or foreign partners pursue the same target, for different purposes, and none of them know enough to deconflict their actions. In this respect, USCYBERCOM's role as global command authority for U.S. cyber operations is not just mission enhancing but mission critical.

Cyberspace Operations C2 Conclusion

The DoD's cyber C2 framework emphasizes centralized command and control to synchronize tactical missions around the globe with limited personnel and infrastructure resources. In carrying out that task, USCYBERCOM leverages neither the processes similar to air power nor the agile organizational construct similar to SOF to link the tactical level of war with strategic objectives. Limiting the C2 framework to the combatant command level decreases the likelihood of standardization across the department and hinders USCYBERCOM's goal of integrating cyber effects into joint operations.

The demand for cyber warfare will only increase in the future. As USCYBERCOM grows into its new role of Functional Combatant

[38] Rogers, Hearing to Receive Testimony on United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2019 and the Future Years Defense Program, 88.
[39] Rogers, 20.

Command, the cyber C2 framework must evolve to better align with the operational environment and more effectively integrate cyber warfare capabilities across the battlefield. Recommendations for doing so are the focus of the next, and final, chapter.

Conclusion and Recommendations

The complexity of military operations is increasing as information technologies begin to merge the strategic, operational, and tactical levels of warfare. In addition to an increased emphasis on coalition warfare, the introduction of new warfighting domains such as space and cyberspace complicate an already complex array of organizational relationships. As the operating environment evolves, so too must the C2 frameworks that synchronize military efforts on the battlefield.

This thesis examined various operational environments and the C2 structures used to conduct military actions within them. Through a comparative case study analysis, the paper sought to answer the research question: How can USCYBERCOM best organize its forces to both leverage its budding operational capabilities and integrate the unique characteristics of cyber warfare with the objectives of Joint Force Commanders?

The first case study examined the command and control of air power during the battle of Khe Sanh in Vietnam. The Marines argued for control air power at Khe Sanh and to request for additional support from the Air Force and Navy, as needed. The Air Force looked to control all air power in the theater while prioritizing effort to specific regions based upon the joint force commander's objectives. The Air Force won the argument after a series of heated debates between senior military leaders and used the Theater Air Control System to synchronize theater air effects while placing Khe Sanh as the main effort. The TACS controlled air power in Vietnam through a *process-oriented framework* underpinned by the Air Force doctrine of centralized control and decentralized execution.

The TACS has significant strengths as a process-oriented framework. Its use of integrated air liaison elements to the tactical level fosters a highly structured system to coordinate planning requirements

for air support. Additionally, the employment of embedded or airborne tactical C2 elements presents an elegant solution for knitting together tactical ground forces with operational air commanders to synchronize battlefield execution.

The process-oriented strengths of the TACS also present potential weaknesses. The standardization of the TACS limits its flexibility to unique mission demands across the spectrum of conflict. For example, the centralization of information and decision rights at the senior element of the TACS is a limiting factor for distributed operations in complex and rapidly changing environments.

The second case study analyzed the command and control of Special Operations Forces' during Operation ANACONDA in Afghanistan. SOF personnel achieved success in the early stages of Operation ENDURING FREEDOM when working solely with their traditional intelligence agency and local national partners. Integration with the conventional force for ANACONDA, however, led to significant deficiencies in mission planning and execution. Improperly aligned command relationships, inadequate intelligence preparation of the operational environment, and poor air-ground coordination doomed the ground assault from the start.

The Special Operations Forces' distributed operations model has significant strengths as an agile organization-oriented framework. The model exploits SOF's unique ability to leverage unified action and flexibility to deliver strategic effects at the tactical level in a dynamically changing environment. The SOF model is tailorable to the mission while requiring that its C2 nodes and tactical maneuver units integrate with existing conventional fires frameworks, such as the Air Force's TACS, to increase combat power.

The distributed operations model, however, has its weaknesses. The model requires extensive human capital and relies on informal and sometimes misaligned support relationships to thrive in a shared

battlespace. In such an environment, the cultural secrecy that fuels SOF success hinders its coordination and integration with conventional forces.

The final case study examined the command and control of cyber operations. The nature of the cyberspace domain, nuances of operating *in* the domain, and the physical infrastructure that creates the domain are driving factors for why traditional military members misunderstand cyber warfare. These three considerations have also driven USYCBERCOM to construct its command and control framework in a manner vastly different from other DoD organizations.

The DoD's cyber C2 framework emphasizes centralized command and control to synchronize tactical missions around the globe with limited personnel and infrastructure resources. In carrying out that task, the DoD leverages neither the processes-oriented approach of air power nor the agile organization-oriented approach of SOF to link the tactical level of war with strategic objectives. Limiting the cyber C2 framework to the combatant command level decreases the likelihood of standardization across the department and hinders USCYBERCOM's goal of integrating cyber effects into joint operations.

The demand for cyber warfare will only increase in the future. As USCYBERCOM grows into its new role of Functional Combatant Command, the cyber C2 framework must evolve to align with the operational environment and more effectively integrate cyber warfare capabilities across the battlefield.

Recommendations

Recommendation 1 – DoD must stand up theater-level cyber components, under USCYBERCOM COCOM, that are collocated with the supported GCC and FCCs.

In his testimony to the Senate Armed Services Committee, Admiral Rogers stated that USCYBERCOM needs to get "integrated structures

and organizations at the execution level" to enable speed and agility.[1] If tactical integration is the key to USCYBERCOM's future success, the command must take thoughtful and deliberate action to modify its C2 structure to facilitate speed and agility in the domain.

First, as a Unified Combatant Command, USCYBERCOM should focus on global synchronization and standards for cyber operations, advocating for cyber operations to the national command authority, and pursuing unified action with interagency partners.[2] USCYBERCOM and its supported CCMDs can no longer afford to adhere to the centralized control and centralized execution model that it espoused during the years of fledgling cyber capabilities.

Second, the DoD must stand up regionally aligned subordinate unified commands, under USCYBERCOM COCOM authority, and collocated with the supported GCCs. This model relationship mirrors the ties between USSOCOM and its TSOCs.[3] The theater cyber commands should have General Officer or Flag Officer representation, with the associated authorities to plan and execute cyber operations with first-order effects in the supported AOR. Due to proximity, increased rank, and expanded authorities, a cyber Commanding General and his or her staff have a greater ability to influence theater planning efforts and fully integrate with the daily battle rhythm of the GCC.

The new theater command should also be the primary office charged with building partner capacity for cyber operations. Expanding, strengthening, and operationalizing partnerships with allies is one of USCYBERCOM's top-five future imperatives.[4] By maintaining persistent and meaningful engagement with regional allies, the theater command is

[1] Rogers, 16.
[2] Nakasone, Advance Policy Questions for Lieutenant General Paul Nakasone, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 11.
[3] Tisdel, Taske, and Fleser, "Theater Special Operations Commands Realignment," 2.
[4] Rogers, "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," 9.

best postured to shape the operational environment to prepare for great power competition in the cyber domain.[5]

The theater cyber command should also have robust capabilities that enable USCYBERCOM continuity of operations and build resiliency into the exquisite infrastructures that enable cyber warfare. This concept satisfies part of the command's vision for enabling persistent operations in a dynamic and globally contested domain.[6]

Third, the DoD must abolish the JFHQ-C structure and allow the service components to focus on their traditional mission of organizing, training, and equipping cyber forces. The DoD and its services already face significant challenges with readiness across the cyber mission force.[7] Alleviating the service component commanders of the responsibility of operational C2 across multiple combatant commands will enable them to focus on presenting ready and capable forces to the theater cyber commands and their supported commanders.

Recommendation 2 – USCYBERCOM must create command positions for each Cyber Mission Force team.

The Cyber Mission Force construct does not include team-level commanders by the original design. The most *junior* cyber warfare commander supporting USEUCOM is the two-star general JFHQ-C AFCYBER Commander who works day-to-day in San Antonio, Texas. That same commander is the most *junior* cyber warfare commander for USTRANSCOM and USSTRATCOM missions. The breadth of responsibility and the high retention of command authority creates a

[5] Rogers, 10.
[6] Rogers, 4.
[7] Nakasone, Advance Policy Questions for Lieutenant General Paul Nakasone, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, 7.

centralized command and centralized control model that hinders the C2 framework by eliminating tactical C2.

The new CMF team commanders would serve two important roles. The team commander should be responsible and accountable to the service cyber component for developing personnel and maintaining team readiness. When assigned to a theater cyber component, the CMF team commander would serve as the lowest level of tactical C2 for executing cyber operations.

Recommendation 3 – USYCBERCOM and the supported CCMDs should leverage existing non-organic fires processes to plan cyber warfare operations and synchronize timing and tempo.

The current cyber C2 organizational framework lacks a coordinating framework that integrates and connects the tactical and operational levels of warfare. Considering USCYBERCOM's low-density and high-demand nature, it should not create a duplicative or stand-alone process. Instead, it should leverage existing non-organic fires processes during major combat operations, such as the Theater Air-Ground System (TAGS), to synchronize timing and tempo of cyber warfare effects.

To accomplish this objective, fully-qualified graduates of CMF assignments should imbed as liaisons with key nodes of the TAGS throughout the TACS, MACS, Army Air-Ground System, Navy Tactical Air Control System, and Special Operations Air-Ground System. These liaison elements would gain a better understanding of the tactical scheme of maneuver than the current elements located at the GCC. By leveraging a close relationship with maneuver units and understanding their objectives, the TAGS LNOs could forecast requirements for

battlefield cyber effects and synchronize timing and tempo during execution.[8]

Final Thoughts

The DoD made significant progress in maturing the capabilities of its cyber force during USCYBERCOM's first nine years. To take cyber warfare to the next level, it must shift its attention to forecasting and building a C2 structure that effectively and efficiently links tactical level efforts with strategic objectives. USCYBERCOM's goal must be to focus on globally synchronizing the fight that occurs below the level of the Geographic Combatant Commands. The recommended change should follow a deliberate and thoughtful process that occurs as a part of a strategic roadmap for cyber C2 capabilities. This five to ten-year plan should address investment in infrastructure and capabilities, codifying roles and responsibilities between organizations, and developing qualified and capable personnel. Successfully integrating cyber warfare effects on the battlefield through effective operational C2 will prepare the DoD for information-age warfare and better posture the U.S. for great power competition.

[8] Conti and Raymond, *On Cyber: Towards an Operational Art for Cyber Conflict*, 227.

Bibliography

Alberts, David S., and Richard E. Hayes. *Power to the Edge: Command and Control in the Information Age*. Washington, D.C.: Command and Control Research Program Publications, 2003.

———. *Understanding Command and Control*. Command and Control Research Program Publications, 2006.

Bright, James M. "Operational Seam: The Command and Control of Conventional and Special Operations Forces." Naval War College, 2007.

Callahan, Shawn P. *Close Air Support and the Battle for Khe Sanh*. Quantico, Virginia: History Division United States Marine Corps, 2009.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5120.02D. *Joint Doctrine Development System*, 5 January 2015.

Connary, Shane M. "Computer Network Operations Command and Control: A New Perspective." Naval War College, 2009.

Conti, Gregory, and Gregory Raymond. *On Cyber: Towards an Operational Art for Cyber Conflict*. Kopidion Press, 2017.

Department of Defense. *DOD Dictionary of Military and Associated Terms*, March 2018.

Department of the Army Field Manual (FM) 3-24. *Counterinsurgency*, December 2006.

Department of the Army Field Manual (FM) 3-05.20. *Special Forces Operations*, June 2001.

Dunford, Joseph F. Jr. "From the Chairman: The Character of War and Strategic Landscape Have Changed." *Joint Forces Quarterly* 89, no. 2nd Quarter (2018): 2–3.

Franks, Norman. *Battle of Britain*. New York: Bison Books Limited, 1981.

Franks, Tommy R. *American Soldier*. Regan Books, 2004.

Gargan, Jason M. "The Joint Force Air Component Commander and the Integration of Offensive Cyberspace Effects." *Air & Space Power Journal* Spring 2016 (n.d.): 86–93.

Gibney, Aaron M. “Centralized Offense, Decentralized Defense: Command and Control of Cyberspace.” School of Advanced Air and Space Studies, 2012.

Hammond, Grant T. *The Mind of War: John Boyd and American Security*. Washington, D.C.: Smithsonian Books, 2001.

Hukill, Jeffrey, Larry Carter, Scott Johnson, Jennifer Lizzol, Edward Redman, and Panayotis Yannakogeorgos. “Air Force Command and Control: The Need for Increased Adaptability.” *Air Force Research Institute Papers*, July 2012, 135.

Jackson, Scott A. “Tactical Integration of Special Operations and Conventional Forces Command and Control Functions.” School of Advanced Military Studies, 2003.

Joint Pub 1. *Doctrine for the Armed Forces of the United States*, 12 July 2017.

Joint Pub 3-0. *Joint Operations*, 12 January 2017.

Joint Pub 3-12. *Cyberspace Operations*, 5 February 2013.

Joint Pub 3-30. *Command and Control of Joint Air Operations*, 12 January 2010.

Kugler, Richard. “Operation Anaconda in Afghanistan: A Case Study of Adaptation in Battle.” Center for Technology and National Security Policy, February 2007.

Lawrence, Scott K. “Joint C2 Through Unity of Command.” *Joint Forces Quarterly* 1994–1995, no. Autumn/Winter (1995): 4.

Lehman, Joshua O. “Command and Control in the Gray Zone: The Advantage of SOC-FWDs.” *Special Warfare* April-June 2017 (2017): 30–33.

Liepman, James M. “TACS and Air Battle Management: The Search for Operational Doctrine.” *Airpower Journal* Spring 1999 (1999): 61–75.

Locher, James R. III. “Defense Organization: The Need for Change.” Staff Report. Washington, D.C.: Senate Armed Services Committee, October 16, 1985.

Lundgren, John M. Jr. “Examining Command and Control Constructs for Offensive Cyberspace Operations.” Naval Postgraduate School, 2014.

Martin, Grant M. “Special Operations and Conventional Forces: How to Improve Unity of Effort Using Afghanistan as a Case Study.” School of Advanced Military Studies, 2009.

McCombie, Ryan J. “Options for Command and Control of Special Operations.” National War College, 1986.

Nakasone, Paul. Advance Policy Questions for Lieutenant General Paul Nakasone, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, Senate Armed Services Committee (2018).

———. Opening Remarks for Lieutenant General Paul Nakasone, Nominee for Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service, Senate Armed Services Committee (2018).

Nalty, Bernard C. *Air Power and the Fight for Khe Sanh*. Washington, D.C.: Office of Air Force History, 2005.

Office of the Secretary of Defense. Cyberspace Command and Control Execution Order (2017).

Pomerleau, Mark. “Cyber Command Stands up Planning Cells at Combatant Commands.” *C4ISRNet*, October 11, 2017.

Ramsey, Ryan. “C2 - Less Is More.” Newport, Rhode Island, 2007.

Rodriguez, Stephen M. “USCYBERCOM: A Centralized Command of Cyberspace.” Naval War College, 2011.

Rogers, Michael. “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.” United States Cyber Command, March 23, 2018.

———. Hearing to Receive Testimony on United States Cyber Command in Review of the Defense Authorization Request for Fiscal Year 2019 and the Future Years Defense Program, U.S. Senate Committee on Armed Services (2018).

Smail, John P. “Designed to Win: An Agile Approach to Air Force Command and Control of Cyberspace.” School of Advanced Air and Space Studies, 2010.

Smith, James K. “USAF Theater Air Control System: Where Do We Go From Here?” United States Marine Corps Command and Staff College, 2002.

Thornton, David. “How Setbacks and DoD Reform Led to the Creation of SOCOM.” Federal News Radio, April 6, 2018. https://federalnewsradio.com/socom/2018/04/how-setbacks-and-dod-reform-led-to-the-creation-of-socom/.

Tisdel, Michael D., Ken D. Taske, and William C. Fleser. “Theater Special Operations Commands Realignment.” Alexandria, Virginia, 2014.

United States Military Assistance Command Vietnam. “Vietnam Lessons Learned No. 77: Fire Support Coordination in the Republic of Vietnam.” San Francisco, California, May 1970.

United States Special Operations Command. “USSOCOM History: 20th Anniversary Edition.” MacDill AFB, Florida: USSOCOM/SOCS-HO, 2007.

Vassiliou, Marius S. “How C2 Goes Wrong,” 46. Alexandria, Virginia, 2014.

War Department Field Manual (FM) 100-20. *Command and Employment of Air Power*, 21 July 1943.

Weems, Max C. “Command and Control in the Anti-Access/Area Denial Environment.” Air War College, 2014.

Wood, Daniel C. II. “USCYBERCOM: Right Solution, Wrong C2 Structure.” Naval War College, 2012.