Cyberspace in War

BY

Alphanso Adams

A Thesis Presented to the Faculty of
the School of Advanced Air and Space Studies
for completion of graduation requirements

Air University
Maxwell Air Force Base, Alabama
June 2020

APPROVAL

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

_____

Nathaniel R. Huston (Date)

_____

David Benson (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

Lieutenant Colonel Adams was a graduate of and commissioned at Baylor University in 2004, where he majored in Information Systems and Operations Management. In various leadership roles at the 39th Communications Squadron, Incirlik Air Base, Turkey; 52nd Combat Communications Squadron and 5th Combat Communications Support Squadron, Robins Air Force Base, Georgia; 318th Operations Group and 90th Information Operations Squadron, Joint Base San Antonio-Lackland, Texas; Air Force Personnel Center, Joint Base San Antonio-Randolph, Texas; and Headquarters Air Force Special Operations Command, Hurlburt Field, Florida. Additionally, Lt Col Adams has deployed in support of Operation IRAQI FREEDOM and Joint Task Force-Bravo. He served as the Defense Fellow for Senator Bill Nelson of Florida during the 115th Congress-2nd Session. Prior to his assignment to the School for Advanced Air and Space Studies, he was the Chief of Cyber Programs, Secretary of the Air Force Legislative Liaison, Washington, District of Columbia.

ACKNOWLEDGEMENTS

This has been an amazing year of growth rendered possible by the support of many. I offer my sincere appreciation to my fantastic thesis advisor, Dr. Nate Huston. His willingness to donate extraordinary amounts of time, paper, and ink helped me tremendously as I wrestled with the research and writing process. I owe him a significant debt of gratitude I can only hope to repay. To my thesis reader, Dr. David Benson, thank you for your insight and for helping me remove the gargoyles.

Each of my SAASS professors were instrumental in developing my writing skills and I am truly grateful for their commitment to the education of Airmen. I particularly want to thank Dr. James Kiras and Dr. Sarah Bakthiari for their investment in me professionally. To Ms. Sheila McKitt, thank you for your personal attention and perspective.

Researching this topic would not have been possible without the support of Colonel Anthony Thomas, Colonel Douglas Shahan, and Lieutenant Colonel Jennifer Law who provided me unprecedented access to the right people, places, and documents. Additionally, I would like to thank each of the authors cited in the case studies for capturing the challenges of their time. I remain optimistic such stories and reports from recent wars are not lost to the digital ether.

My year has been marked by the presence of great classmates of which I am proud to call great leaders. Thank you for your encouragement, selflessness, and friendship. To the commanders, jefes, officers, non-commissioned officers, and airmen who have mentored me along the way – thank you for your guidance and trust.

Finally, to my family. I am blessed to have a bride who encompasses strength, courage, and wisdom in every way. I would be a shadow of myself without her by my side. I can never find the words to express how much I love you. Thank you for marrying me. To my sons, you are my greatest accomplishments. I am forever proud of you.

ABSTRACT

Strategies for cyberspace have focused primarily on the consequences of operations “in” and “with” cyberspace. These discussions, typically centered on cyber war or cyberwarfare, presume access to cyberspace to be present, resilient, and adequate for military operations. However, the physical infrastructure which provides access to cyberspace is an avenue to exert control over the domain. Because the U.S. Air Force and U.S. Space Force will need to operate in access-constrained environments, it is imperative to explore how the U.S. Air Force has operated with similar constraints in the past. In this historical analysis, the author analyses the challenges and impacts of communications infrastructure on military operations from the Vietnam War and the Gulf War. Extrapolated from these past experiences are lessons that can apply to the physical components of cyberspace in order to help shape military strategies for the future.

CONTENTS

Illustrations

Figures

Chapter 1
Introduction

Additionally, questions such as "Is cyber intel?" or "Is cyber comm?" are counterproductive as they encourage legacy stovepiped views of cyberspace operations.

Major General Brett T. Williams
Director of Operations, U.S. Cyber Command

In 1942, the United States established an air route within the China-Burma-India Theater to supply materiel and people into Japanese occupied China. The Army's Signal Corps and Army Airways Communications Service were responsible for establishing communications across the theater and quickly discovered significant obstacles. India, the hub of the air route, lacked an extensive and reliable network to support the modern foreign air force of the United States.[1] Aircraft and administrative message transmission became heavily reliant on radio communications, which overloaded the ad hoc network.[2] When wired infrastructure was installed, it fell victim to a range of climatic, biological, and human interferences.[3] Yet the air-to-ground and base communications capabilities were critical to conduct of operations for what was the most dangerous air route in the world.[4]

Today's military strategist might be forgiven for perceiving cyberspace as a completely virtual domain, built solely on computer-coded logic and human interactions. Yet, cyberspace is not far beyond the wires and radio frequencies of battlefields 80 years prior. Analyses of the threats within cyberspace often grapple with the consequences of cyber weapons against populations, governments, militaries, and industries.[5] Fear of an

[1] James F. Brewer et al., eds., *China Airlift--the Hump*, vol. 1 (Poplar Bluff, Mo: China-Burma-India Hump Pilots Association, 1980), 125.

[2] Brewer et al., 1:126.

[3] Brewer et al., 1:125.

[4] James F. Brewer et al., eds., *China Airlift--the Hump*, vol. 2 (Poplar Bluff, Mo: China-Burma-India Hump Pilots Association, 1983), 257–59. Of note, because of its superior reliability over the War Departments signal facilities, the China-Burma-India communications network established by the Army Airways Communications Services was used to transmit terms of surrender to the Japanese on 15 August 1945. Amidst the confusion of the atomic attack on Nagasaki, the China-Burma-India communications network became the official channel between Imperial Japan and the United States.

[5] Defined by Thomas Rid as, "computer code capable of threatening or causing harm, on populations, governments, militaries, and industries." Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013), 37.

unsuspecting attack capable of crippling power grids, banking institutions, or military aircraft have contributed to a public consciousness of an impending cyberwar in scale and shock as the Japanese attack on Pearl Harbor.[6] This perception, however, overlooks a key commonality with those decades-old battlefield challenges. Just as air forces of World War II relied heavily on physical components to transmit information, so too do today's military forces require physical infrastructure in order to access cyberspace.

The U.S. military, particularly the U.S. Air Force and U.S. Space Force, will need to operate in constrained environments without the level of access to cyberspace it has enjoyed when fighting against technologically inferior military forces. The U.S. Air Force has operated with similar constraints in the past, and I will demonstrate how a combination of transmission technologies were employed to account for physical circumstances on the ground overcome these constraints to accomplish military objectives. Specifically, I will examine how the U.S. Air Force addressed the physical challenges of the communications architecture in the Vietnam and Gulf Wars. From these past experiences, I will extrapolate lessons that can apply to cyberspace in order to help shape military strategies for the future.

Although I have no intention of perpetuating a stovepiped view of cyberspace, I argue the strategist must wrestle to control physical access to cyberspace first before considering operations "in" or "with" cyberspace. Given the gravity of this claim, how can the strategist gain a better understanding of the physical challenges of cyberspace? The first requirement is to understand exactly what is meant by the term, "cyberspace."

BACKGROUND

Defining cyberspace and exploring its relevance is critical to understanding why it is important in war. The following paragraphs discuss why cyberspace matters as a source of power for states, both politically and economically. Building on this discussion, the work turns then to an explanation of why cyberspace matters to militaries in war.

No universal definition of cyberspace exists, but the most useful in understanding the physical characteristics is:

[6] Leon Panetta, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City" (Business Executives for National Security, New York City, NY, October 11, 2012), https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

> *A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.*[7]

This definition provides three key insights into the nature of cyberspace. First, unlike other domains, cyberspace is only accessible through electronic means by leveraging the electromagnetic spectrum. Unlike the land, sea, and air domains, cyberspace is not everywhere waiting to be tapped into. Cyberspace is created by man-made equipment which exploits a scientific phenomenon. Second, cyberspace is a critical component of the information environment. The origin of information and the intensity of interactions between physical, virtual, and cognitive dimensions characterizes the cyberspace contribution to the information environment.[8] Third, cyberspace is formed through interconnected networks across a distance using information-communication technologies. As Colin Gray puts parsimoniously, "cyber[space] is information and the communication of this information."[9]

This information and its exchange has become a resource driving modern economies. An inability or delay in connecting to the digital commons has an impact on overall economic growth. The United Nations estimates that digital services exports accounted for 50% of all global service exports.[10] Other analysis measures the digital economy at nearly 15.5% of world Global Domestic Product.[11] Additionally, because cyberspace is interconnected, both private and state-owned companies can benefit from first-movers advantage by leveraging information to compound their market position. Similar to compound interest, digital economies benefit from information on

[7] Daniel Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," in *Cyberpower and National Security*, ed. Franklin Kramer, Stuart Starr, and Larry Wentz, 1st edition (Dulles, Virginia: Potomac Books, 2009), 28.

[8] Robert Axelrod and Michael Cohen, *Harnessing Complexity: Organizational Implications of a Scientific Frontier* (New York, N.Y.: Basic Books, 2000), 26; United Stated Department of Defense, Joint Staff, "Joint Publication 3-13, Information Operations" (United States Department of Defense, Joint Chiefs of Staff, November 20, 2014), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

[9] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), 34.

[10] United Nations Conference on Trade and Development, "Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries" (United Nations Publications, 2019), 6, https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf.

[11] United Nations Conference on Trade and Development, 6.

information.[12] Because information has become a wealth-generating resource, efforts to exert sovereignty on cyberspace have been pursued by states. Government regulations and laws restricting the location of physical infrastructure needed to mine, store, and process digital information have been adopted in both democratic and communist governments.[13]

Additionally, cyberspace has provided a global venue for political discourse. Globalization and the reach of information has altered the idea of societal community by undermining the nation-state as the principle means of engagement.[14] By exchanging information beyond the control of governments, cyberspace has the potential to subvert national identity, disrupt trade, and replace the role of governments as intermediaries between people.[15] In response, nation-state leaders have often attempted to restrict the flow of information within their national boundaries with, at times, catastrophic results.[16]

Beyond economics and politics, cyberspace has become critical in war. The military force unable to connect to cyberspace is at an information disadvantage, which could have decisive consequences on the battlefield.[17] Modern military forces have become more highly integrated and dependent on the information environment to create asymmetrical advantages in combat power. From Russian General Gareev's perspective, Operation DESERT STORM was such a pairing of, "war with the application of ultra-modern multinational forces; and war using outdated weapons on the part of Iraq."[18] Against modern forces, Gareev stipulated war could not be won by targeting a fraction of fielded combat forces. Instead, he stated destruction of the enemy's, "common

[12] This is explained in detail through a short case study of Google. See: Shawn M. Powers and Michael Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom*, History of Communication (Urbana: University of Illinois Press, 2015), 79–88.

[13] Yuxi Wei, "Chinese Data Localization Law: Comprehensive but Ambiguous," The Henry M. Jackson School of International Studies, University of Washington, February 7, 2018, https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.

[14] Powers and Jablonski, *The Real Cyber War*, 162.

[15] David Aucsmith, "Disintermediation, Counterinsurgency, and Cyber Defense," in *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Washington D.C.: The Brookings Institution, 2018), 343.

[16] David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (Oxford University Press (2015), Edition: Reprint, 352 pages, 2015); Powers and Jablonski, *The Real Cyber War*, 164.

[17] Makhmut Gareev, *If War Comes Tomorrow? The Contours of Future Armed Conflict*, ed. Jacob Kipp (London, United Kingdom: Routledge, 1998), 49.

[18] Gareev, 66.

information space," where intelligence, orientation, command, control, and targeting reside, would be more effective.[19] A natural evolution of this thought is the targeting of cyberspace where information exists and digital interactions occur. Attacks directed at cyberspace could become a means to remove an adversary's asymmetrical information advantage on the battlefield.

Military utility, economic growth, and domestic political order have new dynamics which must be addressed due to the growth of information, the information environment, and cyberspace. Nation states and militaries are now exploring avenues to regain sovereign control of the information environment and cyberspace. Additionally, the interdependent and interconnected nature of cyberspace has stoked fears of cyber war. Although literature on the practicality of cyber war and cyberwarfare is plentiful, it typically favors an analysis from a virtual perspective. Deficient is an analysis of the physical nature and geographic location of the equipment necessary to connect to cyberspace, how nation-states exercise control of this aspect of cyberspace, and how physical control impacts the conduct of military operations.

RESEARCH QUESTION

Given the impact of physical layer of cyberspace and relative paucity of rigorous examination of history, it behooves the 21st century strategist to explore the past in order to acutely ascertain the future. This research examines the relationship between the control of access to cyberspace and that control's impact on military operations. Specifically, I ask *how could the physical components of cyberspace impact the conduct of military operations?* Additionally, I explore why some forces have better access to cyberspace than others and how access is distributed over a geographic area of operations. Ultimately, I attempt to invigorate a discussion on the notion of communications as a support function instead of a cyberspace operations element.

Three issues guided the research of this topic. First, it appeared that communications in most major U.S. conflicts of the past were either haphazardly planned or executed. Military professionals pride themselves on the ability to conquer the odds and ensure the mission gets done. However, this chapter's opening story describing communications challenges during air operations over the Himalayas in World War II is

[19] Gareev, 49.

not the exception. Why do communications always seem inadequate? Second, the U.S. Air Force studies ad nauseum the history of its enemy and their unidentified vulnerabilities. However, rarely is there a comprehensive assessment of its own historical vulnerabilities which were, luckily or deliberately, overlooked by the enemy.

Third, if the conduct of cyberspace in war follows the same trajectory as the analog communications era, what potential challenges and historical solutions can the strategist expect to counter in the future? The current dependence on digital information for war is particularly important to the U.S. Air Force which has little historical experience operating in a non-connected and information deprived battlespace.[20] By comparison, the U.S. Space Force, the newest military service established in 2020, has no experience operating disconnected from a digital information space. The physical portions of cyberspace are intrinsically linked to all space operations. Exercising control over the ability to access cyberspace in war may become the more important task for cyberspace forces in a contested environment, as opposed to attacking and defending virtual spaces and information.

LIMITATIONS

This research ambitiously aims to highlight an aspect of cyberspace which has garnered little attention. However, it is not without limitations which deserve to be addressed up front. Attempting to synthesize the interaction of military operations and cyberspace from a physical perspective is a daunting task. This is evident in the lack of research on this matter. Additionally, some unit history from the communications squadrons of the timeframe studied are classified as of this writing. Unclassified documents, unfortunately, captured only generalized information on the number of phone calls received and teletype messages transmitted instead of the number of aircraft crash-line calls made or supply data transmitted. To compensate for these limitations, some

[20] Kennett's superb historical account of air forces during World War I provide a unique perspective on the relationship between airpower and communications. What becomes evident is how little experience was gained by air forces operating without air-to-ground or airfield communications. Early rudimentary procedures of communications included landing near available telephones in order to pass observed enemy movements. By 1915, one year since the start of the war, wireless telegraphy was installed in some aircraft enabling constant air-to-ground communications. Significant advantages were afforded to those military's capable of installing communications within their aircraft later in the war. This also became a precursor of events for successful air force employment in World War II. Lee Kennett, *The First Air War: 1914-1918* (New York, N.Y.: Free Press, 1999), 33-34.

simplification is necessary at the risk of over-correlation between disparate actions. However, given the dearth of literature on this matter, particularly for military strategists, my intent is to introduce a view of cyberspace which may elude typical consideration.

METHODOLOGY

This research begins by discussing the impact of national sovereignty and international relations on the employment of information communication technologies in nation-states in Chapter 2. This chapter aims to dispel the oft quoted myth of low barriers of entry to cyberspace. From a physical perspective, geography and politics create high barriers to entry and provide avenues for states to exert control over access to cyberspace. Next, a historical assessment of the Vietnam and Gulf Wars follows in Chapters 3 and 4.

This work employs a case-study methodology to compare how the physical artifacts of communications architectures impacted operations in the Vietnam and Gulf Wars. These wars were selected for their historical proximity to the current Information Age and the availability of unclassified documentation . The introduction of computing devices during the Vietnam war can provide an understanding of how new information technology influences communications architectures. The Gulf War is generally referred to as the first information war because of the confluence of information-technologies, space systems, and the Internet. As such, each provides insights into the future of cyberspace in war.

Building on this foundation, in chapters 3 and 4, I explore the two case studies from the vantage point of U.S. Air Force operations, its reliance on information, and its ability to exchange that information outside the United States. In each case, the analysis compares assumptions of connectivity pre-conflict. In chapter 5, I conclude with an analysis of the impacts of communications architectures in both wars and discuss the potential implications for controlling the physical layer of cyberspace.

Chapter 2

Access

Discussions regarding the role of cyberspace in war have tended to focus on virtual activities and have often resulted in strategies which overlook the physical layer of the cyberspace domain. However, insufficient consideration of physical cyberspace will have significant impact on a military's ability to meet operational objectives in the information age. In this chapter, I argue that physical cyberspace must become a more important factor in the development of strategy. I begin by reviewing how access to cyberspace is a source of power. Next, I discuss why cyberspace in war warrants a position of more importance and urgency in strategy.

THE DOMAIN

Colin Gray reminds us that information and its exchange lie at the heart of cyberspace.[1] Without information, cyberspace serves no purpose. Therefore, all strategies for cyberspace seek to control information or the exchange of information. This is observable in various economic and diplomatic strategies for cyberspace. Because of the rapid spread of the Internet, a component of cyberspace, information has become a resource to fuel business growth and national Gross Domestic Product. [2] Within the economic environment, corporations seek to control as many portions of the information resource market as possible. For example, Google's strategy of integrating its cyberspace products, services, and applications allows it to control how information from its platform is monetized.[3] Diplomatically, nation states seek to control the use of information through laws regulating its access and distribution. The European Union's General Data Protection Regulation, aimed at protecting the privacy of European Union citizens, exerts state control over data, information, and its exchange throughout cyberspace.

Modern militaries must also pursue control of information and information exchange in war. Due to the speed and range of modern weapons systems, information is an operational prerequisite. For example, the speed and efficiency of close air support is

[1] Gray, *Making Strategic Sense of Cyber Power*, 34.
[2] Powers and Jablonski, *The Real Cyber War*, 108.
[3] Powers and Jablonski, 75–77.

dependent on the proliferation of information from sensors blanketing the battlespace; this is a significant evolution from the low-level dive attack requirements of 1926.[4] Other advancements in navigation, intelligence, logistics, and command and control are dependent on information resident in and exchanged through cyberspace. It is the harnessing of information as a weapon which makes cyberspace important in conflict and why militaries must develop strategies for cyberspace.[5]

CONTROL THE DOMAIN

According to Dolman, a former professor at the U.S. Air Force's School of Advanced Air and Space Studies, strategies to control a domain depend first on the ability to operate from and within the domain.[6] It is a prerequisite for violence. Without an ability to impact the domain, strategy is of zero value.[7] The utility of a strategy for cyberspace can thus be judged by its ability to control access to cyberspace. Webster's dictionary defines access as, "permission, liberty, or ability to enter, approach, or pass to and from a place."[8] However, defining access to cyberspace has become blurred by attempts to characterize the domain.

Fanelli and Conti, developers of a cyber operations methodology from U.S. Cyber Command and the U.S. Military Academy respectively, attempt to describe attributes of cyberspace in relation to four features or planes: physical, logical, cyber persona, and supervisory.[9] A second perspective from Sean Kern, an Air Force Officer who at the time was assigned to U.S. Cyber Command, argues control is determined by the level of access to key cyber terrain described as three layers: the physical, logical, and persona.[10]

---

[4] Benjamin Franklin Cooling, *Case Studies in the Development of Close Air Support* (Washington D.C.: Office of Air Force History, 1990), 49.

[5] Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age*, Cass Series--Strategy and History 6 (London, United Kingdom: Frank Cass, 2005), 39.

[6] Dolman, 34.

[7] Colin S. Gray, *The Strategy Bridge: Theory for Practice* (Oxford, UK: Oxford University Press, 2010), 171.

[8] *Merriam Webster's Collegiate Dictionary*, 11th ed. (Springfield, MA, USA: Merriam Webster, Incorporated, 2003).

[9] Robert Fanelli and Gregory Conti, "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict" (2012 4th International Conference on Cyber Conflict, Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, 2012), 325, https://westpoint.edu/sites/default/files/inline-images/centers_research/cyber_research_center/PDFs/201206_fanelli.pdf.

[10] Sean Kern, "Expanding Combat Power Through Military Cyber Power Theory," *Joint Force Quarterly*, no. 79 (October 1, 2015): 89.

In both methodologies, control of cyberspace is achieved by targeting these planes or terrain. However, neither answers which feature, plane, or layer defines the ability to access cyberspace.

Scholars and theorists most commonly place the digital layers, the logical and persona, as the key to the ability to access cyberspace. This is typically contextualized as a conflict *in* cyberspace or "cyberwarfare." Cyberwarfare attempts to create adverse consequences through human-to-human, human-to-machine, or machine-to-machine interactions with and through digital-code in the logical and persona layers. But these consequences are only abstract and have not been definitively observed or proven.[11] The ability to digitally attack trustworthy information may or may not be a form of social manipulation,[12] deterrence,[13] or violence.[14] Assuring access to truthful information through digital defenses is also a proposition some scholars have approached with conflicting views.[15]

Despite a lack of consensus on the ability to wage conflict in cyberspace, military strategists continue to develop cyberspace strategies primarily within the context of cyberwarfare, paying little to no attention to the physical aspect of cyberspace itself. The 2018 Department of Defense Cyber Strategy emphasizes the maliciousness of computer-code, both as an advantage and threat, within the context of war and warfare.[16] "Defending forward," one of the strategy's primary objectives, aims to disrupt malicious cyber activity by conducting offensive cyber-attacks, yet these offensive attacks are susceptible to the very debates which have, thus far, failed to advance the theory of cyberwarfare.[17] As a result, defining access primarily through the logical and persona layers diverts attention away from a more enduring truth. Access to cyberspace is

[11] Gray, *Making Strategic Sense of Cyber Power*, 10.

[12] Peter W. Singer and Emerson Brooking T, *LikeWar, The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt, 2018).

[13] Herbert Lin and Amy Zegart, *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington D.C.: The Brookings Institution, 2018), 173–94.

[14] Rid, *Cyber War Will Not Take Place*.

[15] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, 1st Ecco pbk. ed (New York: Ecco, 2012).

[16] United States Department of Defense, "Department of Defense Cyber Strategy 2018" (United States Department of Defense, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[17] Josephine Wolff, "Trump's Reckless Cybersecurity Strategy," *The New York Times*, October 2, 2018, New York edition, sec. A.

determined, or more appropriately defined, by the level of control exercised over the physical layer.

Cyberspace is inherently physical. The use of electronics in the form of information-communications technologies is required to operate from or within cyberspace.[18] Whereas the maritime and air domains do not require ships and airplanes to exist, cyberspace requires physical artifacts such computers, servers, routers, cables, and antennas to exist. A strategy to control physical access to a computer or a connection between computers subsequently controls access to the information resident or exchanged between computers. This is frequently ignored in the development of strategies for cyberspace. I surmise this is for two reasons.

First, physical access to cyberspace is often misperceived as ubiquitous. Global penetration of the Internet, however, is only 53 percent.[19] When developing strategies for cyberspace, military strategists may fall victim to the availability heuristic, a condition where the individual determines the frequency of an event by the ease at which they can recall its occurrence, thereby failing to recall any instance when physical access to cyberspace did not exist.[20] A more common memory may be the inability to access information due to a problem with computer-code. As an example, an inability to visit a website is more likely to be perceived as an issue with a piece of software than the severing of a cable outside. This perpetuates the idea of cyberwarfare and controlling access at the logical and persona layer as more probable than controlling access at the physical layer.

Second, physical access to cyberspace is codified in doctrine as a communications function instead of a cyberspace operations mission. Commercial and private industry own and operate the vast majority of the physical layer of cyberspace. This makes the U.S. military reliant on non-military organizations and business contracts for services and architectures in order to access cyberspace across the globe.[21] However, assessments of

[18] Kuehl, "From Cyberspace to Cyber Power: Defining the Problem," 28.

[19] Nathan McDonald, "Digital in 2018: World's Internet Users Pass the 4 Billion Mark," Global Digital Report 2018, January 30, 2018, https://wearesocial.com/us/blog/2018/01/global-digital-report-2018.

[20] For more information on the availability heuristic, see Daniel Kahneman, *Thinking, Fast and Slow*, 1st edition (New York: Farrar, Straus and Giroux, 2013), 129.

[21] United Stated Department of Defense, Joint Staff, "Joint Publication 3-12, Cyber Operations" (United States Department of Defense, Joint Chiefs of Staff, June 8, 2018), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

the expected performance of these contracts in conflict is not considered a part of operations, which could place military urgency in competition with corporate interests.[22]

CYBERSPACE IN WAR

The majority of the military's physical access to cyberspace is divorced from its contextual view of cyberwarfare.[23] Continued misperceptions and misalignments have the potential to place the U.S. military in a position tactically prepared for cyberwarfare but operationally unprepared for cyberspace in war. Military strategies for cyberspace which do not seek to control access at the physical layer of cyberspace are particularly susceptible to failure due to two factors: geography and politics.

Colin Gray dubbed geography inescapable because of its influence on the conduct of strategy. Specifically, geography drives choices.[24] Integral to the Air Force's Command and Control doctrine is the execution of reachback, distributed, or split operations. Each can be generalized as the geographic dispersion of combat support or operational decision-making efforts and each, arguably, requires substantial access to cyberspace.[25] Depending on location, the geography of cyberspace may not be capable of supporting these types of operations.

Viewing the physical layer of cyberspace on a map reveals what Erik Kreifeldt describes as, "a lateral band around the world along the core transoceanic transport routes."[26] Submarine fiber optic cables, which account for over 95% of international cyberspace traffic,[27] disproportionately span the North Atlantic and North Pacific Oceans

[22] United Stated Department of Defense, Joint Staff, "Joint Publication 6-0, Joint Communications System" (United States Department of Defense, Joint Chiefs of Staff, October 4, 2019), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0ch1.pdf?ver=2019-10-15-172254-827.

[23] This is perplexing because Joint Doctrine on Cyber Operations discusses the dependency of cyber operations on commercial and private industry. Additionally, it highlights the lack of military authority and oversight over the conduct of these entities. However, the implications the commercial and private industry can have on physical access to cyberspace is ignored in favor of repeating tropes on the implications this can have with cyberwarfare. See: United

[24] Colin S. Gray, "Inescapable Geography," *Journal of Strategic Studies* 22, no. 2–3 (June 1999): 165, https://doi.org/10.1080/01402399908437759.

[25] Curtis E. Lemay Center for Doctrine Development and Education, "Annex 3-30 Command and Control," January 7, 2020, 18–19, https://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-30-Command-and-Control/.

[26] Jayne Miller, "Where the Internet Is (And Why)," *TeleGeography Blog* (blog), July 12, 2017, https://blog.telegeography.com/where-the-internet-is-and-why.

[27] The Office of General Counsel, National Oceanic and Atmospheric Administration, "Submarine Cables," Submarine Cables, accessed April 1, 2020, https://www.gc.noaa.gov/gcil_submarine_cables.html.

before spreading vertically into smaller branches.[28] Many of these smaller branches are also heavily concentrated in the South China Sea, Mediterranean Sea, Red Sea, and Arabian Sea. Topographically, the western coast of England; northeastern, southeastern, and the west coast of the United States; eastern Japan; and numerous sea straights are decisive strategic points for cyberspace. Geographically, reachback, distributed, and split operations conducted further away from this lateral band or without control of these strategic points are more susceptible to cyberspace disruption, denial, or degradation. A report from 2003 provides some evidence to this potential.

In 2003, the National Research Council, a conglomerate of U.S. based non-profits, published a detailed analysis on the performance of the internet following the September 11 terror attacks in New York City. By analyzing two years of data regarding the attacks impact on digital traffic, the report determined the global internet demonstrated substantial resilience. However, the concentration of key physical infrastructure on the island of Manhattan created cascading local and regional Internet outages.[29] Additionally, Italy, Romania, and South Africa, the furthest away from the lateral band of cyberspace, experienced disruptions for days due to dependencies on physical connections in New York City.[30] In the case of South Africa, the severed connection denied access to websites located within the country because local Domain Name Servers, which act as a records office for Internet addresses, required periodic access to master Domain Name Servers in the United States.[31]

In addition to geography, the physical layer of cyberspace is also influenced by politics. P.W. Singer and Allan Friedman challenge the notion of cyberspace as a global commons because "it relies on physical infrastructure and human users who are tied to geography, and thus is also subject to our human notions like sovereignty, nationality, and property."[32] Physical devices such as the previously mentioned Domain Name Service servers, which underpin the daily work of cyberspace, are located within the

[28] TeleGeography, "Submarine Cable Map," Submarine Cable Map, accessed April 1, 2020, https://www.submarinecablemap.com/#/.

[29] National Research Council 2003, *Internet Under Crisis Conditions: Learning from September 11* (Washington, DC: NATIONAL ACADEMIES Press, 2003), 23.

[30] National Research Council 2003, 27.

[31] National Research Council 2003, 32.

[32] Peter W. Singer and Allan Friedman, *Cybersecurity: What Everyone Needs to Know* (OUP USA, 2014), 14.

sovereign border of states with domestic and international goals. Supervision of root, or master, Domain Name Servers is performed by the non-profit Internet Corporation for Assigned Name and Numbers, or ICANN, which, until 2016, was overseen by the U.S. government. Through this relationship, the U.S. had the ability to issue binding direction on the management of access to the internet.

Since the Obama Administration's announcement to, "transition key Internet domain name functions to the global multi-stakeholder community," other states have postured to influence the rules of internet access.[33] In 2019, China leveraged its growing Internet population to gain its first ICANN controlled root Domain Name Server in Shanghai.[34] By May 2020, this number grew to five. China's history of domestic censorship and growing tension with its neighbors has increased concerns of a larger conflict over physical access to cyberspace.[35] Japan and Taiwan could exercise a substantial control over China's Internet access with their combined 21 root Domain Name Servers and strategic position along the lateral band of the North Pacific Ocean.[36]

Globalization is also increasing the potential for state-controlled corporations to serve as political instruments of conflict. Through a process called "peering," corporate and public entities contractually agree to join disparate networks in order to allow information to physically flow from one place to another.[37] Physical peering choke points in some networks, either in close-proximity or higher-up in complex contractual relationships, are exploitable to devastating effect. In 2008, a business disagreement led Sprint Corporation to stop carrying traffic for Cogent Communications. As two large Internet Service Providers, this "de-peering" partitioned the Internet for three days and

[33] "NTIA Announces Intent to Transition Key Internet Domain Name Functions" (National Telecommunications and Information Administration, March 14, 2014), https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

[34] "First ICANN Managed Root Server Instance Installed in Shanghai," ICANN, September 3, 2019, https://www.icann.org/news/announcement-2-2019-09-03-en.

[35] Robert K. Knake, "2019: The Beginning of the End of the Open Internet Era," Council on Foreign Relations, *Digital and Cyberspace Policy Program and Net Politics* (blog), January 6, 2020, https://www.cfr.org/blog/2019-beginning-end-open-internet-era.

[36] Internet Assigned Numbers Authority, *Domain Name System Root Servers*, January 30, 2020, January 30, 2020, https://root-servers.org.

[37] Andrew Blum, *Tubes: A Journey to the Center of the Internet*, 1st ed (New York: Ecco, 2012), 119.

held some Internet traffic hostage in Canada, India, Colombia, and others.[38] It is not impossible to imagine a deployed military force similarly partitioned from cyberspace. According to James Cowie, Russian Internet Service Providers provide over 90% of the access to cyberspace in Central Asia, 73% in Latvia, and 50% in Armenia.[39]

Summary

Cyberspace is important because it is where information exists and is exchanged. Cyberwarfare, fighting within the virtual domain, is certainly worthy of attention, but the physical component of cyberspace is equally, if not more, important. While preparation for digital cyberwarfare is debated, it should not preclude operational inspection of the physical attributes of cyberspace in war. Strategists must consider how geography and politics will influence the computers, cables, servers, and antennas which are required in order for a strategy for cyberspace to be viable. If not, operational plans and processes which require cyberspace may be executed at great known or unknown risk. The end result could be catastrophic.

Given the importance of the physical layer of cyberspace, where should one look for insights? B.H. Liddell Hart encourages the strategist to turn to history because "indirect practical experience may be the more valuable because [it is] infinitely wider."[40] The challenges of cyberspace in war are similar to previous challenges of analog information and its exchange. The case studies that follow were chosen due to their historical proximity to the current information age. As such, they may illuminate a more nuanced understanding of the expectations of cyberspace in future conflict and war.

[38] Martin A. Brown, Clint Hepner, and Alin C. Popescu, "Internet Captivity and the De-Peering Menace, Peering Wars: Episode 1239.174" (NANOG 45, Santo Domingo, Dominican Republic, January 2009), https://archive.nanog.org/meetings/nanog45/presentations/Tuesday/Brown_Internet_Peering_N45.pdf.

[39] *James Cowie on the Geopolitics of Internet Infrastructure* (Harvard University: The Berkmen Klein Center for Internet & Society, 2011), https://www.youtube.com/watch?v=xx13GO2kJU0&feature=emb_title.

[40] Basil Henry Liddell Hart, *Strategy*, 2nd rev. ed (New York, N.Y.: Meridian, 1991), 3.

Chapter 3
Access in Vietnam

This chapter covers the history of U.S. communications in Vietnam from 1961 to 1964. This period is of particular relevance to this study because of the establishment of Military Assistance Command, Vietnam (MACV) in 1962. MACV's predecessor, the Military Assistance Advisory Group, Vietnam (MAAG-V), was originally sent to Vietnam by President Truman in 1950. However, the growing threat posed by the Communist Party in North Vietnam to the democratic government in the South led to a drastic increase in forces and equipment in South Vietnam. This offers an example of how the U.S. military addressed the need to improve physical access to cyberspace due to an influx of forces, equipment, and missions.

Additionally, the early stages of any conflict are a critical period for access. As more forces and equipment flow into theater, the requirements for information and networks become driving factors for communications. Furthermore, this period offers insight into all three military requirements for physical access: inter-theater, intra-theater, and worldwide. Each challenge had to be addressed concurrently in order to meet the mission requirements for forces in Vietnam.

Most historical studies of military communications in Vietnam begin in 1965 and coincide with the Johnson Administration's expansion of military force in the country. For our purposes, however, the period from 1961 to 1964 offers a richer understanding of the challenges of access in war. These early years set the foundation for access as hostilities grew. By 1965, as the number of forces in Vietnam grew, the U.S. Air Force in particular found itself without the access needed in war because of planning decisions made in the years prior.

There are several questions important to understanding access in Vietnam. What were the communications plans? How were these plans executed? Who were the key players? What physical or geographic restraints and constraints existed impacting communications? Why did the communications plan evolve? The answers to these questions offer lessons that might be applied to future challenges to access cyberspace in war.

This chapter is divided in three sections. It begins in 1961 with the communications architecture and geography in Vietnam as used by MAAG-V. Next is an analysis on the growth of communication from 1962 to 1963 due to the activation of MACV and the growth of combat capabilities in the theater. Afterward, a final analysis beginning in 1964 assesses the major communications impacts as combat actions increased leading into and after the Gulf of Tonkin incident.

1961 to 1962 – Initial communications architecture and geography

South Vietnam's geography presented significant challenges to military forces. A combination of meteorological factors created hot, humid, and often wet conditions. Competition existed with local populations for hospitable dry land, especially around the Mekong Delta, west of Saigon, where flooding occurred during the rainy season.[1] Throughout the war, communications sites were often selected due to terrain and security considerations rather than technical requirements, which led to suboptimal results.[2] This could include the location of communications equipment in areas maximizing security at the expense of coverage and efficiency. Additionally, access to commercial capabilities were extremely limited. The national telephone system was built using antiquated French equipment left over from the French-Indochina War.[3] Because of these limitations, South Vietnamese military forces and their U.S. military advisors, overwhelmingly from the U.S Army, relied heavily on High-Frequency radio networks for Command and Control. Army Signal Corps and advisory forces painstakingly built the rudimentary network required to support 400 personnel across the 500-mile South Vietnamese countryside.[4] A small number U.S. Air Force personnel advised the South Vietnamese air force from an air control center at Tan Son Nhut, Air Base near Saigon.[5] Activated in January 1961, the bare-bones air control center relied heavily on the High-Frequency network to coordinate

[1] Rienzi, Thomas Matthew, *Vietnam Studies: Communications-Electronics 1962-1970*, 1st ed. (Washington, D.C., 2002: Department of the Army, 1972), 5.

[2] 1070803002, Logistics Support in the Vietnam Era - Monograph 5: Communications" (Joint Logistics Review Board, n.d.), 9, Glenn Helm Collection, The Vietnam Center and Sam Johnson Vietnam Archive, Texas Tech University.

[3] John D. Bergen, *Military Communications: A Test for Technology*, vol. 91 (Washington, D.C.: Center of Military History, United States Army, 1986), 367.

[4] Rienzi, Thomas Matthew, *Vietnam Studies: Communications-Electronics 1962-1970*, 6.

[5] John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, vol. I, The Air War in Indochina (Maxwell Air Force Base, Alabama: Air University, 1981), 73.

tactical airpower but capacity and reliability problems became exacerbated as operations increased.[6]

In mid-1961, South Vietnam requested urgent help from the Kennedy Administration to combat the Viet Cong insurgency. In response, the advisory mission increased by over 2,700 personnel. [7] Part of this increase included support to the South Vietnamese air force in two areas: air operations and air control. U.S. Airmen and aircraft from the 4400th Combat Crew Training Squadron deployed in August 1961 to Bien Hoa airfield in South Vietnam under the code-name "Farm Gate" to train and assist the South Vietnamese air force in interdiction and close air support.[8] In October 1961, elements of the 507th Tactical Control Group deployed to Tan Son Nhut Air Base near Saigon in order to create a limited Tactical Control System with initial communications capabilities for the South Vietnamese air force.[9]

No clear communications plan existed in 1961. In-country communications capabilities were ad hoc in nature and driven primarily by U.S. Army needs due to the number of soldiers deployed throughout the country. Requirements for tactical air control and aerial transport compounded communications requirements for airpower. The Tactical Air Control System required robust communications capabilities at major South Vietnamese and Army Corps operations centers at Da Nang Air Base, Pleiku Air Base, Can Tho, and Saigon.[10] Tan Son Nhut Air Base and Bien Hoa Air Base, both near Saigon, were critical locations for the coordination and employment of tactical airpower within South Vietnam.[11] Additionally, Pleiku, Da Nang, and Nha Trang Air Bases were major aerial port facilities for military airlift.[12]

Communications capabilities, reliant on nascent High-Frequency radio networks, were rapidly saturated and insufficient for the amount of information needed for air

---

[6] John J. Lane, Jr, I:108.

[7] Rienzi, Thomas Matthew, *Vietnam Studies: Communications-Electronics 1962-1970*, 6.

[8] James S. Corum and Wray R. Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists* (Lawrence, KS: University Press of Kansas, 2003), 246.

[9] Corum and Johnson, 245.

[10] John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, I:74.

[11] Corum and Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists*, 245–46.

[12] Carl O. Clever, "F031100450859, Project CHECO Southeast Asia Report #62 - Part VI - Support Activities" (Office of Air Force History, October 1961), 31, Sam Johnson Vietnam Archive Collection, The Vietnam Center and Sam Johnson Vietnam Archive, Texas Tech University.

operations. Some of these problems were self-inflicted. The detachment of Airmen from the 4400th Squadron, for example, who were supporting Operation Farm Gate from Bien Hoa Air Base, communicated often with squadron leadership back in Florida using the High-Frequency network.[13] This undoubtedly consumed available capacity; communicating directly with the chain of command at Tan San Nhut Air Base, approximately 17 miles away, may have been more effective and conserved precious bandwidth. However, the challenge of communications in South Vietnam could not be resolved through simple process improvements. Before the end of 1961, the Commander-in-Chief, Pacific Command identified long-line communications in Vietnam as an urgent requirement in order to expedite, "military reaction to Viet Cong operations."[14]

1962 to 1963 – The First Plan

Growth of the advisory mission in Vietnam led to the activation of the Military Assistance Command, Vietnam (MACV) in 1962. One of the most urgent challenges for the new command was the lack of communications capability to conduct military support operations. In an effort to mitigate the communications challenge, the Secretary of Defense approved four major projects to address communications requirements in-theater: Barn Door I, Barn Door II, Back Porch, and Wet Wash.

Barn Door I and Barn Door II

The first two projects, Barn Door I and Barn Door II, sought to improve the Tactical Control System in-theater by expanding capabilities in South Vietnam and creating a new capability at Ubon Air Base, Thailand. [15] The need for air control intensified in 1962, which led to another expansion of the Tactical Control System. Operation Farm Gate increased the number of air sorties as U.S. and South Vietnamese air forces began conducting joint operations. Communications personnel and equipment from the 5th Tactical Control Group deployed to Tan Son Nhut Air Base and established the Tactical Air Coordination Center for all joint operations in South Vietnam.[16] Additionally, in March 1962, a tactical air control element in Pleiku observed periodic

[13] Corum and Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists*, 246.

[14] Carl O. Clever, "F031100450859, Project CHECO Southeast Asia Report #62 - Part VI - Support Activities," 44–45.

[15] Carl O. Clever, 45–46.

[16] Corum and Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists*, 251; John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, I:99.

but unverifiable aircraft flying through southern Laos towards North Vietnam creating an air route and defense vulnerability .[17] In order to respond to potential aerial resupply routes into and from Northern Vietnam, additional air control and warning facilities were deployed to Ubon Air Base, Thailand.[18]

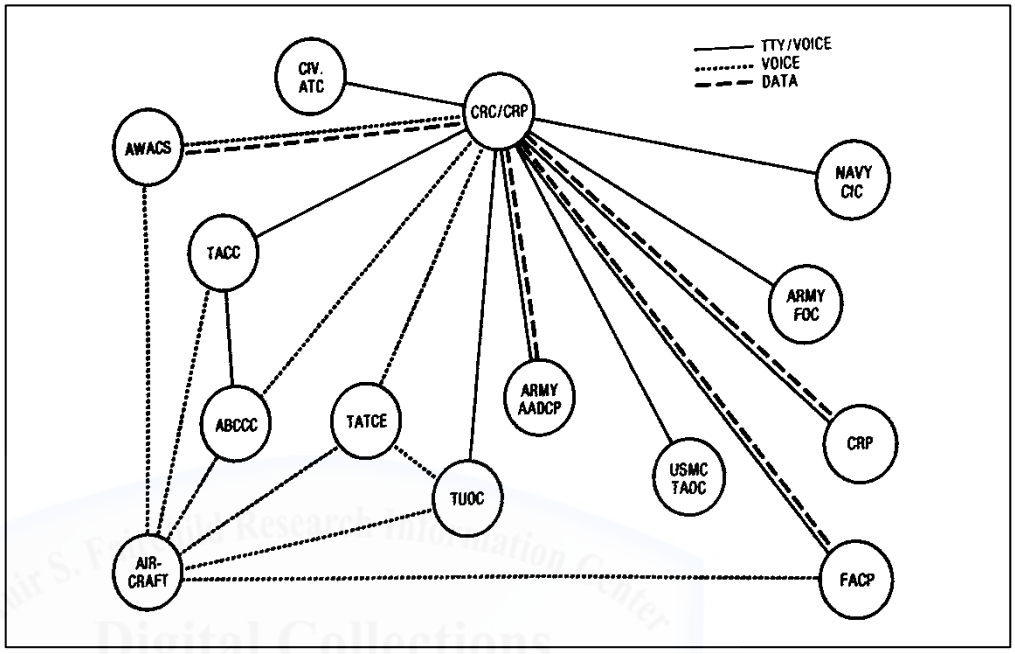

Figure 1. Logical diagram of communications network for airspace control (reprinted from Command and Control and Communications Structures in Southeast Asia).

An effective Tactical Control System required 11 operational elements in order to coordinate air interdiction, close-air support, airlift, airspace control, and reconnaissance operations.[19] Central to the system was the Tactical Air Control Center, which served as the central information node. Voice, teletype, and sensor-data were the three types of information required for the Tactical Control System. Logical diagrams, an example of which can be seen in Figure 1, depicted the flow of information but made no mention of the often-times significant physical challenges of access in the jungles of Vietnam.

Due to the vast geography of Vietnam, wired access was limited to small local areas. Tropospheric scatter, line-of-sight, and High-Frequency radio systems were each

[17] John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, I:74.

[18] Carl O. Clever, "F031100450859, Project CHECO Southeast Asia Report #62 - Part VI - Support Activities," 46.

[19] John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, I:27–31.

capable of providing voice, teletype, and sensor-data, but each had inherit limitations.[20] Tropospheric scatter radio provided the highest number of voice circuits which, when combined with multiplex equipment, could provide teletype and data transmission over distances up to 320 kilometers. In comparison, line-of-sight and High-Frequency radio had lower voice and teletype circuit capacity, requiring an increase in the amount of equipment and personnel to meet information requirements. Improper communications architecture could become rapidly saturated, creating bottlenecks which could only be overcome through re-design. Expanding the Tactical Control System across Vietnam and Thailand required an out-of-country, high-capacity communications path for the transmission of data and voice between various operating locations. In early 1962, no such capability existed.

Back Porch

After the Barn Door I and II projects, the third major communications effort, and by far the largest in scope, began. Back Porch was a joint initiative between the Defense Communications Agency, U.S. Air Force, and U.S. Army, Operation Back Porch established a long-line communications capability in Vietnam between the major operational locations in Vietnam as well as Thailand.[21] Using Tropospheric Scatter Radio, Operation Back Porch was envisioned as a 200-mile beyond-line-of-sight communications capability.[22] Funded and contracted by the Air Force, Back Porch would be operated and maintained by the U.S. Army Signal corps; command and control of the Back Porch network was the responsibility of MACV in Saigon.[23]

[20] Joint Logistics Review Board, "1070803002, Logistics Support in the Vietnam Era - Monograph 5: Communications." f3-f8.

[21] Carl O. Clever, "F031100450859, Project CHECO Southeast Asia Report #62 - Part VI - Support Activities," 46.

[22] Rienzi, Thomas Matthew, *Vietnam Studies: Communications-Electronics 1962-1970*, 8.

[23] Rienzi, Thomas Matthew, 15.

Figure 2. Back Porch System in 1964 (reprinted from Vietnam Studies: Communications-Electronics 1962-1970)

The system became operational in September 1962.[24] The physical design of Back Porch (Figure 2) highlights more clearly its limitations. Phu Lam, the Army's primary signal facility in Saigon, Nha Trang Air Base, Vietnam and Pleiku Air Base, Vietnam were critical strategic points within the system architecture. Phu Lam connected forces south of the Mekong Delta through a combination of smaller Tropospheric radio and microwave relays. Nha Trang Air Base was both the northern communications route to Bien Hoa, Qui Nhon, and Da Nang as well as the single-point of failure for communications north of Saigon. Pleiku Air Base provided access to Ubon Air Base, Thailand and was the only high-capacity military communications route out-of-country until 1965. The U.S. Army resolved the Nha Trang Air Base single point of failure by deploying additional mobile tropospheric radio equipment to meet their operational requirements.[25] This would have benefits for communications between the Tactical Air Control Center and other elements of air control in Vietnam and Thailand.

[24] Rienzi, Thomas Matthew, 10.
[25] Rienzi, Thomas Matthew, 13.

Using tactical equipment, Operation Back Porch became the initial Southeast Asia Wideband System by providing high throughput communications into the theater; yet, it was designed with two constraints.[26] First, the system only had to meet the needs of the South Vietnamese military. Second, the system provided only minimal excess capacity to support additional U.S. forces. Because of these limitations, Back Porch was both modest in scope and reliability. Doctrinally, airpower required dedicated communications to be effective.[27] Because of the small footprint of Air Force tactical communications units, air force operations were forced to compete with ground operations for access. Air support missions, if they were not cancelled, were sometimes executed with limited coordination because the Back Porch system failed to provide access to the Tactical Air Control System.[28] Weather forecasts from Tan Son Nhut Air Base frequently failed to arrive at Army processing facilities on Qui Nhon.[29] Concerns over reliability led to the creation of additional High-Frequency networks for tactical air control by the 1st Mobile Communications Group deployed from Clark Air Base, Philippines.[30] However, even this additional capability did not fully meet the need for high capacity and reliable communications dedicated to airpower in Vietnam.

Wet Wash

The fourth project, named Wet Wash, was designed to provide an inter-theater connection between South Vietnam and Clark Air Force Base in the Philippines.[31] The proliferation and use of low-capacity High-Frequency networks caused voice and data traffic to stall during transmission; the implementation of a precedence system, intended to ensure time sensitive information was communicated over lower priority messages, effectively denied administrative and logistics information from leaving South Vietnam in a timely manner. By connecting South Vietnam to the Philippines through a reliable physical capability, this information bottleneck could be reduced while also creating

[26] Rienzi, Thomas Matthew, 6–7.

[27] John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, I:143.

[28] John J. Lane, Jr, I:109.

[29] Carl O. Clever, "F031100450859, Project CHECO Southeast Asia Report #62 - Part VI - Support Activities," 48.

[30] John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, I:109.

[31] Rienzi, Thomas Matthew, *Vietnam Studies: Communications-Electronics 1962-1970*, 15.

redundant paths into the military's worldwide communications network (Figure 3). Responsibility for the system was given to the Air Force. It consisted of multiple line-of-sight radio networks and the establishment of an 800-mile submarine cable across the South China Sea. The system was not completed until 1965 and, despite its overall effectiveness, remained susceptible to cuts from maritime vessels.[32] High-Frequency networks continued to proliferate as an alternate inter-theater communications capability.

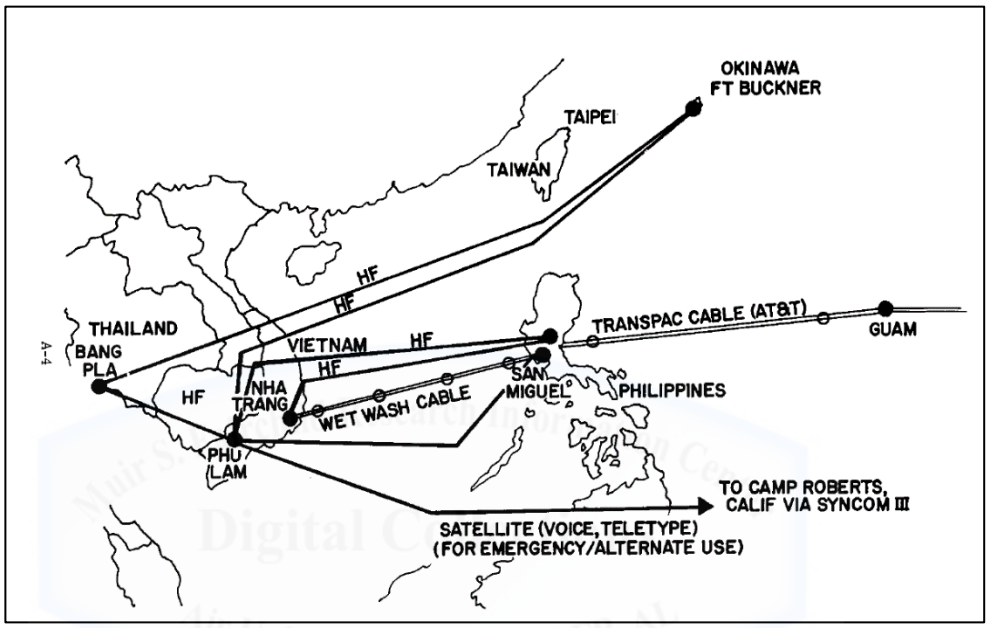

Figure 3. Major communications links into Vietnam on 1 January 1965 (reprinted from Logistics Support in the Vietnam Era - Monograph 5: Communications)

1964 to 1965 – Increased Operational Demand

With four major projects nearing completion, demands on Air Force tactical communications still outstripped available supply. Establishment of an initial wideband system in Vietnam with connections to Thailand, though an improvement, remained unreliable and had little excess capacity to handle a surge in information. High-Frequency radio networks remained the only means of inter-theater communications from Vietnam. he inadequacy of communications across Vietnam became apparent in 1964.

Activation of the 1964th Communications Squadron in May 1962, followed shortly by its growth and designation as a group in October 1962, was an early effort to

[32] Joint Logistics Review Board, "1070803002, Logistics Support in the Vietnam Era - Monograph 5: Communications," 14.

relieve pressure on the tactical forces and equipment. [33] Responsible for all radio, teletype, voice, and base communications at the five major air bases in Vietnam and two air bases in Thailand, the group struggled to provide garrison-level support in a tactically equipped environment. Operational scope and fluidity challenged the concept of fixed versus tactical communications support. The 1964th Communications Group was required to maintain and expand upon the communication architecture as air missions evolved, but it lacked expertise and equipment for the tactical environment.

After action reports in 1963 highlighted a further problem for communications maintenance activities: that of limited airlift support.[34] Lead times for new communications infrastructure were too long for the rapid pace of change as the counterinsurgency mission grew.[35] Airmen deployed to the 1964th Communications Group were on 12-month rotations with little experience operating in tactical environments. By 1963, the 1964th Communications Group was inundated with requirements it could not meet with the resources available. The Commander, capturing lessons learned, noted that, with the exception of inter-theater fixed communications facilities, all communications for the counterinsurgency mission in South Vietnam should be handled by tactical communications units.[36]

In August 1964, North Vietnam took offensive action against U.S. forces in the Gulf of Tonkin, firing on two ships and downing two aircraft.[37] Information flows from Hawaii, Washington D.C., and across Vietnam saturated the existing wideband and High-Frequency networks.[38] Atmospheric and maintenance problems at the height of the attacks also contributed to communications failure. The Johnson administration responded to the attacks with an increase in U.S. forces, including the introduction of modern jet aircraft and tanker support.[39]

---

[33] Carl O. Clever, "F031100450859, Project CHECO Southeast Asia Report #62 - Part VI - Support Activities," 51.
[34] Carl O. Clever, 53.
[35] Carl O. Clever, 54.
[36] Carl O. Clever, 54.
[37] Corum and Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists*, 266.
[38] Rienzi, Thomas Matthew, *Vietnam Studies: Communications-Electronics 1962-1970*, 18.
[39] Corum and Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists*, 267.

As U.S. aircraft undertook more operational missions against North Vietnam independent of the South Vietnamese air force, another Tactical Air Control Center was established at Tan Son Nhut Air Base. Additional communications capabilities were required and, by 1965, all Air Force tactical communications forces and equipment stationed in the Pacific theater were deployed.[40] Stateside units were then tapped to fill the gaps until the Integrated Wideband Communications System was completed.

By 1965, the Operation Wet Wash submarine cable connection to the Philippines was completed. However, the limitations on the design of the Southeast Asia Wideband System, developed under Operation Back Porch, and the need for additional inter-theater communications lines became evident as the potential for a U.S. withdrawal faded. Under the name of Integrated Wideband Communications System, the Defense Communications Agency, U.S. Army, and U.S. Air Force aimed to develop a robust fixed communications network based on commercial equipment capable of supporting 40,000 personnel. [41] This system would not come online until 1968 as the number of U.S. forces in country exceeded 350,000.[42]

Summary

Communications in Vietnam prior to major combat operations in 1965 were constantly in flux. Rapid growth of the Tactical Air Control System in-country was not met with an appropriate growth in Air Force communications capabilities. Part of this can be explained as an effort to keep the U.S. footprint small across the country. However, the ability to provide effective air control, based on the system developed by the service, required reliable and high-capacity communications. With no in-country system to rely upon, the Air Force and Army were forced to address growing requirements collectively with limited ability to surge. The consequences of these decisions significantly impacted forces operating in Vietnam after 1965. The need to provide logistics capabilities in Vietnam taxed the communications architecture substantially. The number of dedicated circuits for logistics were second only to Command and Control.[43] As teletype was

[40] John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, I:142.

[41] Rienzi, Thomas Matthew, *Vietnam Studies: Communications-Electronics 1962-1970*, 77.

[42] Rienzi, Thomas Matthew, 85.

[43] Joint Logistics Review Board, "1070803002, Logistics Support in the Vietnam Era - Monograph 5: Communications," 25.

replaced by the Automatic Digital Network, the tactical communications backbone in Vietnam hindered operations; courier flights carrying punched data cards were used as a stop gap measure.[44] The initial tactical infrastructure was forced to operate well past its intended purpose.[45] As a result, the communications infrastructure was neither flexible enough for the tactical mission nor robust enough for the information demands of processes optimized for the U.S. In essence, the system was not ideal for either mission.

[44] Joint Logistics Review Board, 67.

[45] John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, I:144.

Chapter 4

Access in the Gulf War

This chapter covers the history of U.S. communications in the Middle East during the Gulf War, focusing specifically on Operation DESERT SHIELD from August 1990 to January 1991. There are three reasons to cover this period of the Gulf War, which was ultimately longer than actual combat operations under Operation DESERT STORM. First, DESERT SHIELD was the first operational test for U.S. Central Command and the first large-scale military deployment since Vietnam. Second, these first five months were the most active period of access for U.S. forces. The rapid deployment of combat and sustainment forces stressed the ability of communications equipment to provide access to information resources for war. The access conditions in place on 15 January 1991 set the conditions by which the air and ground war were waged by U.S. and coalition forces. Third, the Gulf War occurred during the era of the microprocessor and personal computer. Unbeknownst to the access planners, these two technological developments would tax their ability to assure access for a force of mixed legacy and modern equipment and information needs.

Operation DESERT STORM is often used synonymously with the actions of military forces against Iraq in 1991. Despite the massive success of coalition forces, the battle for access was conducted nearly entirely during Operation DESERT SHIELD. Conceiving of DESERT STORM as the first "information war" can only be understood in the context of the actions taken to establish the largest joint communications network ever established.[1]

There are several questions whose answers are important to understanding access in the Gulf War. What were the communications plans? How were these plans executed? Who were the key players? What physical or geographic restraints and constraints existed impacting communications? Why did the communications plan evolve? The answers to these questions can provide an understanding of the lessons the U.S. Air Force learned during these early years of access to cyberspace.

---

[1] Alan D. Campen, ed., *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War* (Fairfax, VA: AFCEA International Press, 1992), 1.

This chapter is divided in three sections. It begins in the Summer of 1990 with the development and challenges of Operations Plan 1002-90, which outlined how U.S. Central Command would defend Saudi Arabia. Next is an analysis of the early months of Operation DESERT SHIELD, from August to September 1990, when initial airfields and combat airpower were deployed into the Middle East theater. It concludes with an analysis of the final months of DESERT SHIELD, from October 1990 to January 1991, assessing the continuing deployment of combat and sustainment into theater as well as the major challenges of meeting the access requirements of the modern military.

Mid-1990 – Geography, Architecture, and Operations Plan 1002-90

Within the hierarchy of importance to the U.S. defense establishment, the Middle East ranked far behind the Russian threat to Europe. From 1971 until 1991, responsibility for the Middle East was split between the European, Pacific, and Atlantic Commands.[2] After multiple force restructures and catastrophes in the Middle East, responsibility was finally consolidated under a newly established U.S. Central Command in January 1983. Headquartered at MacDill AFB, Florida, Central Command's primary wartime objective, as outlined in Operations Plan 1002-90, was to defend Iran from Soviet invasion.[3] However, the collapse of the Soviet Union in early 1990 forced a strategic shift in priorities for the command.

During the 1980s, Iraq drastically improved its military capabilities. Under the leadership of Saddam Hussein, the Iraqi military was the fourth largest force in the world.[4] Searching for a new potential adversary in theater, the Commander-in-Chief, U.S. Central Command, General Norman Schwarzkopf, tasked his staff to begin a revision of OPLAN 1002-90 for the defense of the Arabian Peninsula from Iraqi invasion.[5] From a communications perspective, the Middle East was a near dead-zone for access. Although a U.S. military presence existed in the region, the worldwide Defense Communications System was less than adequate for the full combat force necessary for the scenario envisioned. Contrary to some reviews of the initial communications capability in the

[2] United States Department of Defense, "Conduct of the Persian Gulf War: Final Report to Congress, Annex K" (United States Department of Defense, April 1992), 2.

[3] James Kitfield, *Prodigal Soldiers* (New York: Simon and Schuster, 1995), 330.

[4] Shannon Collins, "Desert Storm: A Look Back," U.S. Department of Defense, January 11, 2019, https://www.defense.gov/Explore/Features/story/Article/1728715/desert-storm-a-look-back/.

[5] Kitfield, *Prodigal Soldiers*, 330.

Middle East, there were only two U.S. military satellite ground terminals with worldwide access: one in Bahrain, United Arab Emirates and one in Riyadh, Saudi Arabia.[6] A terrestrial link from the Riyadh communications center provided limited access to Dhahran, Saudi Arabia. The nearest hubs for robust access existed in Turkey to the West and the Philippines to the East (Figure 4).[7]

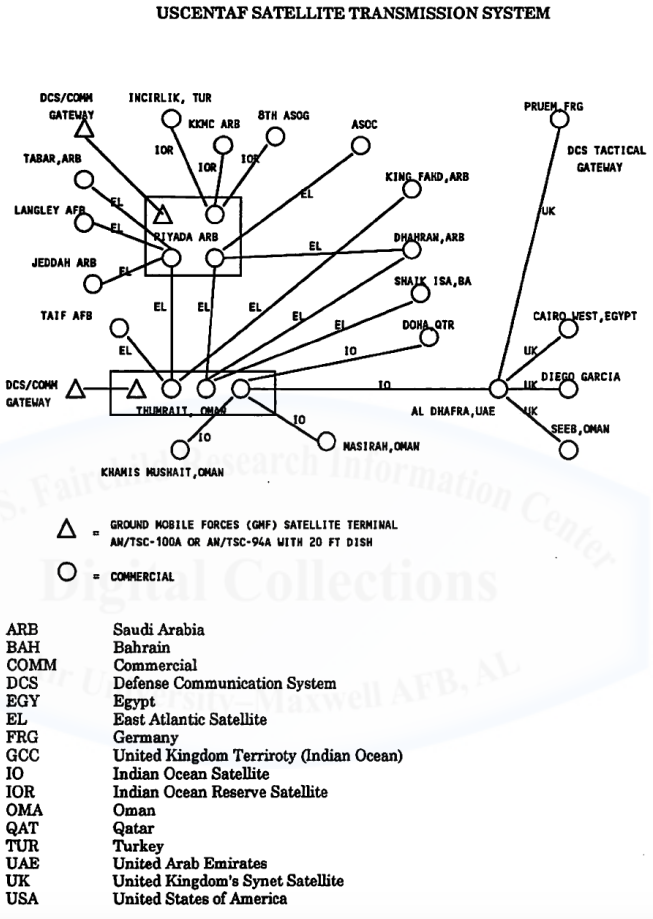

Figure 4 U.S. Central Air Force's Satellite Communications Architecture (reprinted from Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story)

[6] Alan Campen in "Silent Space Warriors" from the book *The First Information War* states there were three tactical satellite terminals in the Gulf area. However, the Gulf War Air Power Survey only identifies two military satellite terminals in the Gulf Area based on James P. Coyne's *Airpower in the Gulf* book and an interview with Colonel Charles Pettijohn, Commander of the 4409th Operational Support Wing. The Gulf War Air Power Survey does account for an additional commercial satellite links but these were not U.S. military operated terminals. Since Campen provides no evidence to support the existence of three military satellite terminals in the Gulf, I will use the Gulf War Air Power Survey's number. Although my accounting of two versus three is valid only to clarify the state of access in the Gulf, the end result remains unchanged – there wasn't enough capacity in theater for U.S. military forces. For the account of two tactical satellite terminals see: Eliot A. Cohen, ed., *Gulf War Air Power Survey* (Washington, D.C: Office of the Secretary of the Air Force, 1993), 93.

[7] Campen, *The First Information War*, 2.

As planning efforts matured across U.S. Central Command, the challenges of establishing communications within the Arabian Peninsula became evident. No country in the region possessed the appropriate infrastructure for modern military forces. In 1986, the United Arab Emirates sought to procure new U.S. military hardware in order to build a national defense communication system.[8] Although Congressional approval was granted in 1989, delays in producing the first production system for U.S. forces delayed delivery of the system to the United Arab Emirates until after Operation DESERT STORM.[9] Saudi Arabia had by far the most modern infrastructure in the region, to include the commercial telephone network.[10] However, its digital telephone network was not fully deployed throughout the country and did not connect adequately to other nations in the region whose support and cooperation would be crucial in the months ahead. One planner assessed in April that "communications support will be austere with heavy reliance on early airlift and satellite systems."[11] As a result, the new OPLAN 1002-90, if executed, would result in increased demand for service deployable communications capabilities.[12]

The revised OPLAN 1002-90 was tested in July 1990 during U.S. Central Command's massive command post exercise called INTERNAL LOOK 90.[13] Held in simulated conditions at Duke Field, Florida, INTERNAL LOOK 90 provided early validation of the April assessment. Establishing communications access would be critical to the successful conduct of war in the Middle East. The Middle East was 7,000 miles away from the main coordinating headquarters in Florida.[14] No combat force would be effective until a theater communications architecture was in place. A lack of access to the

[8] "TRC-170(V) - Archived 7/2000," Land & Sea-Based Electronics Forecast (Forecast International, July 1999).

[9] Michael J. Sullivan, United States of America v Raytheon Company, and Raytheon Canada LTD. (United States District Court District of Massachusetts February 27, 2003); "TRC-170(V) - Archived 7/2000."

[10] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," Project Air Force (RAND Corporation, n.d.), 26.

[11] Cohen, *Gulf War Air Power Survey*, 93.

[12] Campen, *The First Information War*, 25.

[13] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," Case Study (Riyadh, Saudi Arabi: Headquarters United States Central Command Air Forces, March 1991), 1–1.

[14] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 186.

worldwide Defense Communications System, the Department of Defense's global telecommunications network, meant a premium was placed on military satellite communication assets, which were limited in quantity, capacity, and availability. Ideally, execution of OPLAN 1002-90 would include the rapid deployment of the military's jointly developed and interoperable Tri-Service Tactical (TRI-TAC) communications system. Designed in 1971 to satisfy the military's analog and digital information requirements, TRI-TAC equipment was not small, light, or flexible; it was interoperable with legacy equipment while providing the ability to interface with future technologies.[15] As reports from INTERNAL LOOK were captured, actual intelligence reports of Iraq's mobilization on the border of Kuwait in late July changed the dynamics of OPLAN 1002-90.

August – September 1990

On 2 August 1990, the Iraqi military invaded Kuwait. By 6 August, the initial U.S. Central Command forward headquarters was established at Riyadh, Saudi Arabia with the approval of the King Fahd.[16] Even in retrospect, the parallels between the fictional scenario of INTERNAL LOOK 90 and the actual events unfolding are shocking. OPLAN 1002-90, still in draft with the Joint Staff and lacking coordination with the services, became Operation DESERT SHIELD – a rapid force buildup to defend Saudi Arabia from an Iraqi invasion launched from Kuwait.[17] However, early confusion over the number and location of combat forces to be deployed for Operation DESERT SHIELD contributed to delays in communications access.

Initially, U.S. Central Air Forces executed a different plan, OPLAN 1307, which would deploy a rapid reaction force into the Middle East. Consisting of a small number of combat and battlespace control aircraft, OPLAN 1307 was limited to light operations from a single airfield.[18] To support this small footprint, a modest Air Force communications capability was deployed to Riyadh. By the time these initial

[15] James M. Rockwell, ed., *Tactical C³ for the Ground Forces*, AFCEA/SIGNAL Magazine C³I Series, v. 4 (Washington, D.C: AFCEA International Press, 1986), 86–88.

[16] United States Department of Defense, "Conduct of the Persian Gulf War: Final Report to Congress, Annex K," 4.

[17] United States Department of Defense, 3.

[18] Diane T. Putney, *Airpower Advantage: Planning the Gulf War Air Campaign, 1989-1991*, The USAF in the Persian Gulf War (Washington, D.C., 2004: United States Air Force, n.d.), 22.

communications capabilities arrived on 8 August, planners increased the number of airbases to four, with new requirements at Dhahran, Saudi Arabia; Al Dhafra, United Arab Emirates, and, on 10 August, Thumrait, Oman.[19]

Rapidly deploying combat power to the Middle East theater was an urgent priority. With the exception of the Joint Communications Support Element, which arrived at Riyadh to provide headquarters communications capabilities on 8 August, communications equipment and forces were not a significant part of the initial deployment.[20] Because simulations during Exercise INTERNAL LOOK the previous month predicted catastrophic losses of U.S. Army forces, General Schwarzkopf placed strict constraints on airflow into theater.[21] Combat forces took priority on airlift over combat support and sustainment capabilities; this included the large amounts of communications equipment necessary to command and control the vast theater.[22] As a result, combat aircraft arrived in August to bases devoid of the necessary communications architecture for a modern air force.[23] In the interim, units were forced to rely on limited communications assets to receive operation orders from Central Command's forward headquarters in Riyadh. [24] Available single-channel High-Frequency radio and leased commercial telecommunications lines from host-nation providers were ineffective transmission methods for large data files like the air tasking order and imagery intelligence.

By the end of August, more communications equipment and personnel began to arrive in theater aiming to overcome the major access obstacle: geography. Spanning the Arabian Peninsula, Turkey, Spain, Diego Garcia, the United Kingdom, and the U.S., the area of operations lacked an interconnected intra-theater and inter-theater

---

[19] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," 1-4.

[20] The Joint Communications Support Element (JCSE) is a jointly manned tactical command, control, and communications force which can be rapidly deployed worldwide for contingencies and war. In 1990, JCSE reported directly to the Chairman, Joint Chiefs of Staff. At the time of this writing, JCSE is aligned under U.S. Transportation Command. United States Department of Defense, "Conduct of the Persian Gulf War: Final Report to Congress, Annex K," 27.

[21] Diane T. Putney, *Airpower Advantage: Planning the Gulf War Air Campaign, 1989-1991*, 17.

[22] Diane T. Putney, 154.

[23] Campen, *The First Information War*, 26.

[24] United States Department of Defense, "Conduct of the Persian Gulf War: Final Report to Congress, Annex K," 28.

communications architecture for access.[25] Central Command's airlift priorities did not include combat support materials, which reduced the amount of communications equipment deploying into the Middle East theater. This included the TRI-TAC programs TRC-170 Tactical Tropospheric Scatter Radio system. Bulky, heavy, yet capable of providing long distance communications access, the TRC-170 system did not compete well with combat forces for space on air mobility assets.[26] Additionally, the lack of a Defense Communications System gateway in Saudi Arabia, United Arab Emirates, or Oman required the establishment of an inter-theater long-haul communications capability to connect deployed forces with information resources in Europe and the United States. These two requirements would come to depend heavily on one medium – satellite communications.

Initial communications planning identified satellite communications as a scarce resource critical to Central Command's success. Two types of satellite systems were available: Ultra-High Frequency (UHF) and Super-High Frequency (SHF). Each service possessed ground terminals to use UHF for their deployable forces. However, the Navy, lacking SHF terminals on their surface vessels, was solely dependent on UHF satellite communications.[27] Fearing early saturation of limited UHF assets, U.S. Central Command made two important decisions. First, satellite access would be controlled by the U.S. Central Command J6 instead of the Defense Communications Agency.[28] Second, a hub-and-spoke architecture would be used to connect ground and air forces on the Arabian Peninsula through SHF satellite communications.[29] Both decisions would prove wise. Over 95% of all long-haul communications were carried by satellite and the J6 had the authority to address the impacts of an extremely active period of solar activity.[30]

[25] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," 2–1.

[26] "TRC-170(V) - Archived 7/2000," 3.

[27] United States Department of Defense, "Conduct of the Persian Gulf War: Final Report to Congress, Annex K," 34.

[28] United States Department of Defense, 30.

[29] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," 1-5.

[30] Campen, *The First Information War*, 2, 140.

At the start of Operation DESERT SHIELD, only two SHF satellites from the Defense Satellite Communications System (DSCS) covered the Middle East.[31] Established in 1966, the DSCS provided global high-capacity communications via satellites in geosynchronous orbit.[32] The first satellite covering the Middle East was an aging DSCS orbiting over the Indian Ocean; the second was a newer DSCS orbiting over the Eastern Atlantic. In order to efficiently leverage the SHF constellation, U.S. Central Command envisioned central tactical hubs on the Arabian Peninsula to consolidate inter-theater traffic bound for Europe and the United States as well as intra-theater traffic bound for Riyadh.[33] To control access to the DSCS constellations, U.S. Central Command J6 permitted each of the services operating on the ground to establish a limited number of hubs to serve as gateways into the larger Defense Communications System. The Air Force established its first hub at Thumrait, Oman. Although Saudi Arabia is where the majority of combat forces, headquarters elements, and the Tactical Air Control Center were located, Thumrait, Oman was outside of Iraq's air attack and tactical ballistic missile range.[34]

[31] Campen, 137.

[32] "DSCS (Defense Satellite Communications System)," Mission and Spacecraft Library Jet Propulsion Laboratory, accessed March 20, 2020, https://space.jpl.nasa.gov/msl/Programs/dscs.html.

[33] Campen, *The First Information War*, 2.

[34] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," p.1-5.

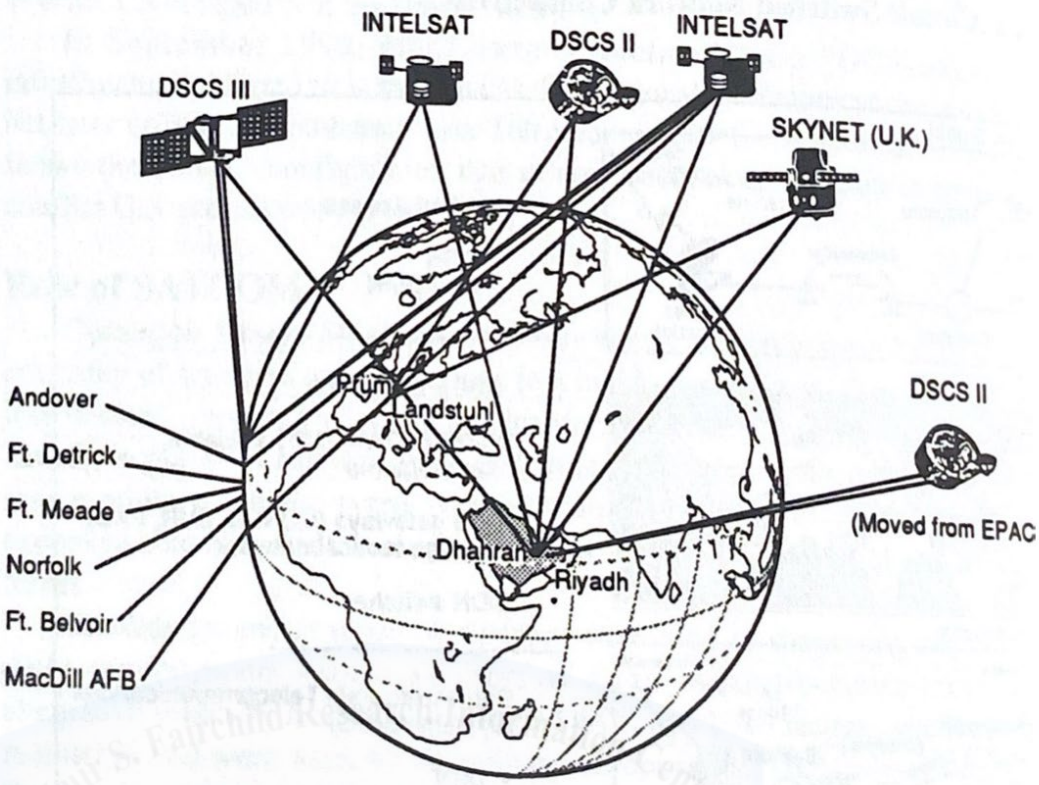

Figure 5 DESERT SHIELD/STORM Satellite Communications Architecture on January 17, 1991 (reprinted from The First Information War: the story of communications, computers, and intelligence systems in the Persian Gulf War)

Until establishment of additional hubs, Thumrait, Oman was the critical communications entrance and exit point for Air Force communications in theater. Had the site been destroyed or disrupted before mid-September, when Al Dhafra was established as the Air Force's second hub, the results could have been catastrophic for U.S. forces. One element heavily reliant on this nascent architecture was U.S. Central Command's Scud early warning system. Utilizing space-based infrared sensors, Air Force space operators in Colorado Springs monitored the region for indications of Scud launches and trajectories.[35] Notifications of launches were passed first through voice channels, then through message channels to U.S. Central Command's Riyadh Headquarters for dissemination. Without the DSCS satellite constellation to provide long-

[35] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 193–94.

haul and long-line access on the Arabian Peninsula, deployed forces would have experienced significant if not catastrophic losses from an Iraqi Scud attack.

Despite exclusive allocation to the Middle East, the small DSCS constellation was taxed by the explosive growth in the number of satellite ground terminals from 4 to 49 within the first month.[36] In early September, additional DSCS capacity was allocated to the theater at the expense of global communications for strategic forces.[37] By mid-September, the supporting satellite architecture expanded to include the United Kingdom's military SKYNET and commercial providers to include four International Telecommunications Satellite Organization satellites operating over the Atlantic.[38] Demand for satellite assets outstripped supply as the number of forces flowing into the theater increased.

Some scholars have argued the satellite shortfalls were driven by poor planning instead of asset availability.[39] Upon closer inspection, this criticism is unwarranted. Although 15 satellites were positioned over Arabian Peninsula, capabilities and requirements on the ground kept them from being interchangeable.[40] All UHF capacity was effectively consumed by ships afloat in November.[41] As the conflict progressed, UHF also proved insufficient in the transfer of critical information for the defensive and offensive air campaigns.[42] Commercial capabilities from INTELSAT were hindered by a lack of appropriate ground-terminals as well its susceptibility to jamming.[43] Other satellites in orbit, such as Defense Advanced Research Program Agency's Multiple Access Communications Satellite and Lincoln Laboratories' Lincoln Experimental Satellite 9, were experimental capabilities not designed to support the access requirements for a combat force. Use of the United Kingdom's SKYNET and North

[36] Campen, *The First Information War*, 137.

[37] Campen, 137.

[38] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 212.

[39] Ricky B. Kelly, "Centralized Control of Space: The Use of Space Forces by a Joint Force Commander" (Maxwell Air Force Base, Alabama, Air University, 1993), 19.

[40] Cohen, *Gulf War Air Power Survey*, 128.

[41] United States Department of Defense, "Conduct of the Persian Gulf War: Final Report to Congress, Annex K," 34.

[42] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," 2–10.

[43] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 210–11.

Atlantic Treaty Organization's NATO-3 satellite required approval through diplomatic channels. Based on these limitations, access through satellite communications were hampered by system incompatibilities and coverage deficiencies. Attempts to address the latter began in October.

October 1990 - January 1991

By October 1990, the number of combat forces in theater was overwhelming the tactical architecture. Over 53 SHF satellite ground terminals were in use when sustainment forces arrived to the Arabian Peninsula armed with Personal Computer devices and an expectation of garrison communications capabilities. Also, the two major Air Force communications hubs at Thumrait, Oman and Al Dhafra, U.A.E. were operational liabilities because of their sole dependence on satellite communications to access the growing theater network. Although the loss of one-hub would not completely isolate air forces in theater, the sites operating as "spokes" would be forced to revert back to leased commercial lines and limited single-channel High-Frequency radio. Fortunately, additional communications equipment and the much-needed TRI-TAC equipment also began arriving into theater to relieve the stress and vulnerabilities from the hub and spoke architecture. Establishment of an "Eastern Corridor" through tropospheric scatter radio connected five critical air base locations: Riyadh and Dhahran, Saudi Arabia; Shaik Isa, Bahrain; Doha, Qatar; and Al Dhafra, U.A.E.[44]

[44] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," 4–2.

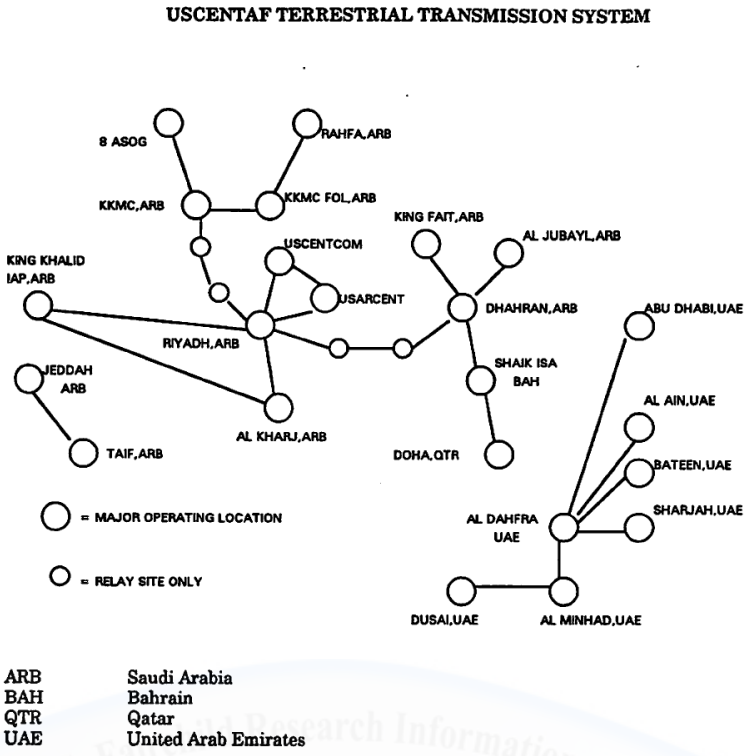

Figure 6 U.S. Central Air Forces Terrestrial Communications Architecture (reprinted from Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story)

Installation of terrestrial connections through tropospheric scatter radio and microwave radio equipment to the East, West, and North of Riyadh fixed major issues for the Theater Air Control System (TACS). As a system, the TACS used line of site UHF radio networks to provide access for air-to-air and air-to-ground forces.[45] At the core of the TACS was the Theater Air Control Center (TACC) located in Riyadh, Saudi Arabia. Due to the vastness of airspace encompassing the operational portions of the Arabian Peninsula, line of sight between the TACC and two airborne elements of the TACS - the Airborne Warning and Control System and the Airborne Command and Control Center - was often lost.[46] Although High-Frequency radio was the alternate access plan, its reliability was seldom an improvement. In response, additional tropospheric scatter radio systems were deployed to Al Rahfa and King Khalid Military City, Saudi Arabia, West

[45] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," 2–2.

[46] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," 6-2.

and North of Riyadh respectively, to cover the UHF blind spots.[47] Designated as Ground-to-Air Transmission Sites in support of the TACS, these tropospheric scatter systems became vital to the successful execution of the initial night interdiction missions on 17 January 1991.

Despite the continued expansion of the communications architecture on the Arabian Peninsula, the suboptimal reality of the tactical communications architecture could no longer be escaped. Simply stated, the systems could not meet the expectations of a force optimized for modernized garrison communications. Units often failed to receive intelligence and weather information collected, processed, and transmitted by specialized organizations in the U.S.[48] In November, voice calls over the Defense Switch Network from the U.S. to deployed forces failed an astonishing 70% to 80% of the time. Discovering and resolving the root cause, which turned out to be related to long-distance transmission, took over three months.[49] In the meantime, the Air Tasking Order had to be delivered to the Navy via daily flights of paper copies, an issue well-documented in discussion of air operations during DESERT STORM.[50] Nor was this solely a Navy solution: many Air Force units were also supplied the Air Tasking Order via Learjet deliveries due to limitations in access across the theater.[51] Less widely known is the inability of Navy F-14 aircraft to provide adequate battle damage assessments as part of the TACS due to UHF saturation.[52] These challenges were present although the U.S. military placed more communications access capabilities on the Arabian Peninsula in 90 days than all of Europe in 40 years.[53]

Impacts of the inadequacy of the communications architecture were felt beyond the Arabian Peninsula. The Air Force deployed nearly all of its active duty tactical

[47] Al Rahfa, Saudi Arabia is approximately 28 miles to the Iraqi border. Campen, *The First Information War*, 30.

[48] United States Department of Defense, "Conduct of the Persian Gulf War: Final Report to Congress, Annex K," 140; Cohen, *Gulf War Air Power Survey*, 101.

[49] Campen, *The First Information War*, 145.

[50] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 110–11.

[51] "Getting USAF C3I off the Ground," *Jane's Defense Weekly*, May 22, 1993.

[52] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 196.

[53] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, 205.

communications equipment.[54] If requirements increased, the Air Force would have needed a Presidential Directive to activate more Air National Guard units in order to gain access to the additional equipment.[55] Poor access also caused message traffic to bottleneck at switching centers outside the area of operations. Message traffic destined for the carrier battle groups in the Persian Gulf so inundated the Naval Communications Area Master Stations in Europe and the Pacific that the Joint Staff had to effectively implement message restrictions on all traffic destined for the European theater.[56] By January, the Joint Staff was forced to implement these restrictions on all traffic globally.[57]

Summary

Histories of Operation DESERT STORM often focus heavily on the technological advances present in the U.S.'s modern military. Establishing the backbone critical to this success took over four months and thousands of communications professionals. Lacking a robust pre-existing communications infrastructure, the U.S. was forced to build both an inter-theater long-haul and intra-theater long-line communications architecture. Part of the challenge in establishing the architecture was the lack of prioritization of communications equipment in the early weeks of Operation DESERT SHIELD. By prioritizing combat forces over command and control capabilities early in the war, the Commander-in-Chief, U.S. Central Command gambled the combat effectiveness of U.S. forces. Given the lack of effective communications across the combat formation for almost two weeks, an aggressive Iraqi attack could have decimated forces in theater. As communications equipment began to arrive in theater, the heavy reliance on satellite communications saturated regional capacity. With 95% of all long-haul communications provided over satellite communication, the U.S. was dependent on both good processes and an inept adversary incapable of recognizing a critical vulnerability. Terrestrial networks were the last to fully come on-line and were successful in resolving some issues particularly with the TACS. However, the tactical equipment was not designed to support the massive demand for communications requirements of the modern force.

[54] Campen, *The First Information War*, 25.
[55] Campen, 27.
[56] Campen, 146.
[57] Campen, 146.

When the war finally began, the problems of access were overcome through the hard work of personnel and refinement of processes. By addressing line-of-sight issues, the Air Force's experimental airborne platform Joint Strategic Targeting and Attack System was able to effectively integrate into the TACS and bring substantial combat capabilities to the ground campaign.[58] Communications rehearsals conducted the nights prior to January. 17, 1991 ensured the first air strikes into Iraq were a success.[59] Finally, the reliability of the communications infrastructure supporting the Scud early warning and alert system between Colorado and Riyadh ensured the security of coalition forces and ensured Israel stayed out of the war – a key political objective.[60] Despite the issues, Operation DESERT SHIELD, the largest joint communications access operation in the history of the U.S. military, was a success. [61]

[58] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 207.

[59] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," 2–5.

[60] Patriot Missile Batteries from the U.S. Army were deployed to Israel by order of President Bush and were integrated into the theater missile defense system. See: James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 34 & 209.

[61] Campen, *The First Information War*, 1.

Chapter 5

Cyberspace in War

As theorists are fond of repeating, there is nothing new is under the sun. I believe cyberspace is no different. Developing strategies for the domain should not be an insurmountable obstacle. Fascination with the potential of the logical and persona layers of cyberspace, both abstractions from reality, have created a military and public enamored with ideas of cyberwarfare and virtual fighting. Debates about the strategic effects' computer-coded cyber-attacks and cyber-defenses might have on the ability to access cyberspace obscure how the physical components determine access. I argue this very "physical-ness," is the most important element in the development of strategy for cyberspace in war.

Cyberspace is physical first, which means it is influenced by geography and politics. Many of the information-technology devices and infrastructures forming cyberspace are disproportionately concentrated in discrete regions of the globe. North America, Western Europe, and Japan are the main transit routes for global information composing what one analyst calls a, "lateral band," across the world. [1] States further away from this lateral band are more susceptible to disruption. Additionally, globalization has provided state-owned Internet Service Providers markets to expand their architectures and services creating the potential for the Internet, a key component of cyberspace, to be partitioned. [2] Unlike concepts such as cyberwarfare, these physical layer actions have occurred with clearly observable impact.

For the military strategist, an oblivious understanding of the physical layer of cyberspace will lead to uninformed assumptions and poor strategy in the information age. Occurring during an era of analog communications, the communications architectures and challenges illustrated in the preceding case studies are effective examples of the importance of the physical layer of cyberspace. These historical experiences are valuable because the challenges to control access to cyberspace will be similar in future conflicts.

---

[1] Jayne Miller, "Where the Internet Is (And Why)."

[2] Martin A. Brown, Clint Hepner, and Alin C. Popescu, "Internet Captivity and the De-Peering Menace, Peering Wars: Episode 1239.174."

Subsequently, operational impacts from geography and politics should be reasonably comparable.

ASSESSMENT

In the Vietnam and Gulf Wars, commercial communications were not ubiquitous. South Vietnam's telephone network was antiquated and limited in capability; [3] Saudi Arabia,[4] by some accounts a country with modernized infrastructure, and the United Arab Emirates[5] lacked sufficient communications for their own military. Additionally, the nearest points of access to the U.S. military's global communication system were outside the area of conflict. This made establishing the infrastructure necessary to prosecute both wars take time. In Vietnam, it took years to build a rudimentary network connecting the country with the larger military communication system. Yet, the network proved massively insufficient to support both combat forces and logistics functions in Vietnam from 1965 to 1967.[6] For Operation DESERT SHIELD, a better communications architecture was available in a shorter amount of time, but a lack of sufficient communications for the Theater Air Control System in the early weeks would have been catastrophic to both ground and air forces.[7]

Initially, the U.S. Air Force was capable of substituting radio and satellite for wired infrastructure. However, as the number and type of forces increased, radio and satellite were not flexible enough to meet information demands. High-Frequency radio was heavily relied upon by early ground and air combat forces in both conflicts, but reliability and capacity problems created operational vulnerabilities particularly for tactical air control. In Vietnam, the large number of antennas coupled with competition for limited capacity created self-inflected interferences and outages.[8] This often led to cancelled or poorly coordinated air support missions. In the Gulf War, High-Frequency radio was insufficient for transmitting the large data packages needed for air control such

[3] John D. Bergen, *Military Communications: A Test for Technology*, 91:367.

[4] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 26.

[5] "TRC-170(V) - Archived 7/2000."

[6] Rienzi, Thomas Matthew, *Vietnam Studies: Communications-Electronics 1962-1970*, 24–25.

[7] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 54.

[8] Rienzi, Thomas Matthew, *Vietnam Studies: Communications-Electronics 1962-1970*, 15.

as imagery intelligence and the air tasking order.[9] Satellite communications were an alternative but, because of a limited number of satellites allocated to the theater, every location could not be connected independently.[10]

Deployable Air Force communications forces were capable of improving these early networks initially but were also resource-constrained. Providing robust and redundant communication to Vietnam required the deployment of entire mobile communications units garrisoned from Air Force Pacific Command.[11] To replace the need for tactical equipment and forces, the military funded four major communications projects: Barn Door I and II; Back Porch; and Wet Wash. Each was plagued by delays and, upon completion, unable to support the amount of combat forces in the theater. As a result, tactical equipment designed to provide temporary capabilities remained in place for years.

In the Gulf War, the amount of communications capabilities deployed was even more alarming. By the time Operation DESERT STORM began, nearly all active duty mobile communications units, then renamed combat communications units, were deployed to support the war.[12] Analysis conducted by the RAND Corporation on behalf of the Air Force noted "had a larger national emergency occurred at the same time as the Gulf War, a large number of combat communications units...would have to have been withdrawn from the theater."[13] This analysis assumed, perhaps correctly, that the Air National Guard, which held 80% of the Air Force's combat communications capability, would not be capable of responding to an emergency outside the U.S.[14]

Mobility limitations had substantial impacts on the communications system in both wars. The need for combat and support forces to operate in an expeditionary environment with equipment designed for a garrison environment created competing

[9] United States Department of Defense, "Conduct of the Persian Gulf War: Final Report to Congress, Annex K," 28.

[10] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," I-5.

[11] John J. Lane, Jr, *Command and Control and Communications Structures in Southeast Asia*, I:142.

[12] Campen, *The First Information War*, 25.

[13] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 206.

[14] Campen, *The First Information War*, 27.

requirements between form, function, and speed. In Vietnam, numerous small systems, such as the High Frequency radios, were highly mobile, flexible, and fast but limited in capability. As a result, a modular system was pursued to provide access faster than more robust commercial fixed-plant offering.[15] The Tri-Service Tactical communications program used by the services during the Gulf War was this envisioned system.[16] However, the system's modularity and robustness also made it large and cumbersome to airlift and difficult to relocate once established. When forced to prioritize airlift between combat forces and combat support, to include command and control systems under the TRI-TAC program, U.S. Central Command chose to deprioritize communications capabilities.[17] As a result, the Air Force's communications infrastructure was fragile for three-months with limited redundancy.

Some of the challenges identified were overcome through non-technical solutions. For example, in both wars, bases with poor or unreliable communications were connected by frequent courier flights. In Vietnam, unreliable communications for logistics elements were overcome by flying digital punch cards to the regional logistics center on Okinawa, Japan.[18] The same process was used during the Gulf War to deliver the air tasking order to Navy Aircraft Carriers and Air Force bases without access to high-capacity communications.[19] Although less than ideal, no location was truly absent communications.

IMPLICATIONS

The experience of the U.S. military, particularly the Air Force, in Vietnam and the Gulf War should help guide the development of strategies to exploit cyberspace in war. I propose three implications for consideration.

---

[15] Joint Logistics Review Board, "1070803002, Logistics Support in the Vietnam Era - Monograph 5: Communications," 71.

[16] Rockwell, *Tactical C³ for the Ground Forces*, 86–88.

[17] "TRC-170(V) - Archived 7/2000," 3.

[18] Joint Logistics Review Board, "1070803002, Logistics Support in the Vietnam Era - Monograph 5: Communications," 67.

[19] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 110–11.

Beware the lateral band

Executing operations away from the lateral band cyberspace requires more physical access capabilities. In some regions, it will also create more physical dependencies. Vietnam and the Arabian Peninsula are below this lateral band and their access, even today, is capable of being controlled through decisive strategic points in the region. The number of hubs constituting the current Defense Communication System has increased to provide more coverage in the Middle East and the Korean Peninsula, but gaps in the system still persist in the Indian subcontinent, Africa south of the Sahara, South America, and the South Pacific.[20]

Although no strategist can see the future, those tasked with developing strategies for these areas must seriously consider the cyberspace access challenges for friendly and enemy forces. This warrants a more nuanced assessment of access plans for operations. One method to inject more rigor would be to return focus to the age-old PACE plan. By designating the primary, alternate, contingency, and emergency (PACE) communications plans, the PACE approach is intended to address dependencies through a tiered network of capabilities. Even PACE, however, may be insufficient in today's environment: geographic and political considerations may require even more than a back-up to the back-up access plan.

Strategists should also consider air mobility as a key factor regarding a military's ability to control access to cyberspace. Historically, traditional weapons of war were favored over communications equipment when airlift capacity was limited. In future conflicts, where information becomes the preferred weapon, this trend may need to be reversed. Overcoming the lateral band problem will become a priority for those countries operating at a geographic cyberspace disadvantage. As a result, concepts such as reachback, distributed, and split operations will require more scrutiny before being employed. For example, providing reachback weather capabilities from Omaha, Nebraska, where military weather information is analyzed and distributed to U.S. forces across the globe, may not make sense for combat operations in Myanmar.

[20] Joint Logistics Review Board, "1070803002, Logistics Support in the Vietnam Era - Monograph 5: Communications," 39.

Information Mobility or Death

Advancements in computing technologies and artificial intelligence may help create a "Goldilocks-type" solution for the contested cyberspace environment, a small and lightweight system capable of high information veracity without persistent access to cyberspace. The possession and ability to rapidly maneuver such a capability would reduce the attack surface of the physical layer of cyberspace.[21]The feasibility of on-orbit cyberspace access capabilities beyond long-haul communications satellites is also worth exploring. Information and its exchange need not be terrestrially bound, after all. Space-based data centers, supported by solar power and cooled by the vacuum of space, could eliminate some of cyberspace's physical decisive points on Earth. Until such game-changing solutions are fielded in sufficient quantities with the requisite processes to make them successful in war, a closer examination at the problems of access deserve more attention.

Even if executed perfectly with futuristic equipment, personnel, and support, the demand for cyberspace access, if left unchecked, will outstrip the available supply. This is not a new observation but it is a pervasive one.[22] Processes and procedures optimized for a garrison environment, where flexibility is easily procured for a permissive geographic and political environment, are often undercut by the reality of the tactical environment. Information demands in Vietnam exceeded every project to improve cyberspace access from 1961 to 1964. Similarly, the race to keep pace with information demands during Operation DESERT SHIELD/STORM was ultimately lost in certain areas despite a high-level of access. To be effective in contested environments, future forces must be capable of decreasing their information demands as cyberspace access decreases. This could require executing operations without information now viewed as critical to air operations such as intelligence, [23] weather, [24] and early-warning. [25]

---

[21] Gerald R. Hust, "Taking Down Telecommunications" (Maxwell Air Force Base, Alabama, School of Advanced Airpower Studies, 1993), 33.

[22] Martin Van Creveld, *Command in War* (Cambridge, Mass: Harvard University Press, 1985), 265.

[23] Campen, *The First Information War*, 63.

[24] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, "A League of Airmen: U.S. Air Power in the Gulf War," 124.

[25] James A. Winnefeld, Preston Niblack, and Dana J. Johnson, 193–94.

Mission Command is the Way

When it comes to cyberspace in war, access requires mission command, defined as the "conduct of military operations through decentralized execution based upon mission-type orders."[26] Digital information may benefit from disaggregation but limited physical devices need to be employed towards a common objective. In Vietnam, the Commander of Military Assistance Command, Vietnam was charged to prosecute the war but had insufficient authority over tactical and strategic communications architectures. As a result, priorities were sometimes based on parochial service interests instead of supporting the larger operational objectives in Vietnam.[27] By comparison, empowerment of the Commander-in-Chief, U.S. Central Command was a major factor contributing to the success in the Gulf War. U.S. Central Command's Internal Look exercise illuminated the communications challenges that would have to be overcome to support a major combat force on the Arabian Peninsula. By understanding the commander's intent, the J6, as the Director of Communications and Information, was able to employ the communications infrastructure in support of the right mission agnostic of potentially prejudiced service interests.

Conclusion

Physical cyberspace matters. Areas where access is not pre-existing, where it is contested, or where it is denied, will be the most challenging to conduct operations if the history of Vietnam and the Gulf War are any indication. A global blockade of cyberspace access is not within any one state's control. A regional restriction, however, could be effective against a military force reliant on long-haul access to cyberspace in order to reach back to critical services and networks. Therefore, where and how military forces access cyberspace must become more important in strategic and operational discussions.[28]

---

[26] United Stated Department of Defense, Joint Staff, "Joint Publication 3-31, Joint Land Operations" (United States Department of Defense, Joint Chiefs of Staff, October 3, 2019), https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_31.pdf?ver=2019-12-18-153903-197.

[27] The entire report from the Joint Logistics Review board is a testament to this failure. See: Joint Logistics Review Board, "1070803002, Logistics Support in the Vietnam Era - Monograph 5: Communications." 67-68.

[28] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (Spring 1993): 31.

War in the information age and beyond will require access to cyberspace. An after-action report from Operation DESERT STORM/SHIELD stated, "remember that communications may affect operations but will seldom, if ever, dictate operational requirements," rather operational considerations will nearly always drive communications requirements.[29] Perhaps this was true at the dawn of the Information Age. Today, however, information is clearly a critical component, perhaps *the* critical component in modern war. As such, one should expect the ability to access cyberspace to prescribe major aspects of operations.

[29] "Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story," 2–6.

BIBLIOGRAPHY

"Air Force Tactical Communications In War: The DESERT SHIELD/DESERT STORM Comm Story." Case Study. Riyadh, Saudi Arabi: Headquarters United States Central Command Air Forces, March 1991.

Axelrod, Robert, and Michael Cohen. *Harnessing Complexity: Organizational Implications of a Scientific Frontier*. New York, N.Y.: Basic Books, 2000.

Blum, Andrew. *Tubes: A Journey to the Center of the Internet*. 1st ed. New York: Ecco, 2012.

Brewer, James F., Harry G. Howton, Janet M. Thies, David J. Orth, John G. Martin, and China-Burma-India Hump Pilots Association, eds. *China Airlift--the Hump*. Vol. 1. 2 vols. Poplar Bluff, Mo: China-Burma-India Hump Pilots Association, 1980.

———, eds. *China Airlift--the Hump*. Vol. 2. 2 vols. Poplar Bluff, Mo: China-Burma-India Hump Pilots Association, 1983.

Campen, Alan D., ed. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax, VA: AFCEA International Press, 1992.

Carl O. Clever. "F031100450859, Project CHECO Southeast Asia Report #62 - Part VI - Support Activities." Office of Air Force History, October 1961. Sam Johnson Vietnam Archive Collection, The Vietnam Center and Sam Johnson Vietnam Archive, Texas Tech University.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. 1st Ecco pbk. ed. New York: Ecco, 2012.

Cohen, Eliot A., ed. *Gulf War Air Power Survey*. Washington, D.C: Office of the Secretary of the Air Force, 1993.

Cooling, Benjamin Franklin. *Case Studies in the Development of Close Air Support*. Washington D.C.: Office of Air Force History, 1990.

Corum, James S., and Wray R. Johnson. *Airpower in Small Wars: Fighting Insurgents and Terrorists*. Lawrence, KS: University Press of Kansas, 2003.

Curtis E. Lemay Center for Doctrine Development and Education. "Annex 3-30 Command and Control," January 7, 2020. https://www.doctrine.af.mil/Doctrine-Annexes/Annex-3-30-Command-and-Control/.

David Aucsmith. "Disintermediation, Counterinsurgency, and Cyber Defense." In *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, edited by Herbert Lin and Amy Zegart. Washington D.C.: The Brookings Institution, 2018.

Diane T. Putney. *Airpower Advantage: Planning the Gulf War Air Campaign, 1989-1991*. The USAF in the Persian Gulf War. Washington, D.C., 2004: United States Air Force, n.d.

Dolman, Everett C. *Pure Strategy: Power and Principle in the Space and Information Age*. Cass Series--Strategy and History 6. London, United Kingdom: Frank Cass, 2005.

Mission and Spacecraft Library Jet Propulsion Laboratory. "DSCS (Defense Satellite Communications System)." Accessed March 20, 2020. https://space.jpl.nasa.gov/msl/Programs/dscs.html.

ICANN. “First ICANN Managed Root Server Instance Installed in Shanghai,” September 3, 2019. https://www.icann.org/news/announcement-2-2019-09-03-en.
Gareev, Makhmut. *If War Comes Tomorrow? The Contours of Future Armed Conflict*. Edited by Jacob Kipp. London, United Kingdom: Routledge, 1998.
Gerald R. Hust. “Taking Down Telecommunications.” School of Advanced Airpower Studies, 1993.
“Getting USAF C3I off the Ground.” *Jane’s Defense Weekly*, May 22, 1993.
Gray, Colin S. “Inescapable Geography.” *Journal of Strategic Studies* 22, no. 2–3 (June 1999): 161–77. https://doi.org/10.1080/01402399908437759.
———. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013.
———. *The Strategy Bridge: Theory for Practice*. Oxford, UK: Oxford University Press, 2010.
Internet Assigned Numbers Authority. “Domain Name System Root Servers.” January 30, 2020. https://root-servers.org.
James A. Winnefeld, Preston Niblack, and Dana J. Johnson. “A League of Airmen: U.S. Air Power in the Gulf War.” Project Air Force. RAND Corporation, n.d.
James Cowie on the Geopolitics of Internet Infrastructure. Harvard University: The Berkmen Klein Center for Internet & Society, 2011. https://www.youtube.com/watch?v=xx13GO2kJU0&feature=emb_title.
Jayne Miller. “Where the Internet Is (And Why).” *TeleGeography Blog* (blog), July 12, 2017. https://blog.telegeography.com/where-the-internet-is-and-why.
John Arquilla, and David Ronfeldt. “Cyberwar Is Coming!” *Comparative Strategy* 12, no. 2 (Spring 1993): 141–65.
John D. Bergen. *Military Communications: A Test for Technology*. Vol. 91. Washington, D.C.: Center of Military History, United States Army, 1986.
John J. Lane, Jr. *Command and Control and Communications Structures in Southeast Asia*. Vol. I. The Air War in Indochina. Maxwell Air Force Base, Alabama: Air University, 1981.
Joint Logistics Review Board. “1070803002, Logistics Support in the Vietnam Era - Monograph 5: Communications.” Joint Logistics Review Board, n.d. Glenn Helm Collection, The Vietnam Center and Sam Johnson Vietnam Archive, Texas Tech University.
Josephine Wolff. “Trump’s Reckless Cybersecurity Strategy.” *The New York Times*. October 2, 2018, New York edition, sec. A.
Kahneman, Daniel. *Thinking, Fast and Slow*. 1st edition. New York: Farrar, Straus and Giroux, 2013.
Kennett, Lee. *The First Air War: 1914-1918*. New York, N.Y.: Free Press, 1999.
Kilcullen, David. *Out of the Mountains: The Coming Age of the Urban Guerrilla*. Oxford University Press (2015), Edition: Reprint, 352 pages, 2015.
Kitfield, James. *Prodigal Soldiers*. New York: Simon and Schuster, 1995.
Kuehl, Daniel. “From Cyberspace to Cyber Power: Defining the Problem.” In *Cyberpower and National Security*, edited by Franklin Kramer, Stuart Starr, and Larry Wentz, 1st edition. Dulles, Virginia: Potomac Books, 2009.
Liddell Hart, Basil Henry. *Strategy*. 2nd rev. ed. New York, N.Y.: Meridian, 1991.

Lin, Herbert, and Amy Zegart. *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington D.C.: The Brookings Institution, 2018.
Martin A. Brown, Clint Hepner, and Alin C. Popescu. "Internet Captivity and the De-Peering Menace, Peering Wars: Episode 1239.174." Presented at the NANOG 45, Santo Domingo, Dominican Republic, January 2009. https://archive.nanog.org/meetings/nanog45/presentations/Tuesday/Brown_Internet_Peering_N45.pdf.
Merriam Webster's Collegiate Dictionary. 11th ed. Springfield, MA, USA: Merriam Webster, Incorporated, 2003.
Michael J. Sullivan. United States of America v Raytheon Company, and Raytheon Canada LTD. (United States District Court District of Massachusetts February 27, 2003).
Nathan McDonald. "Digital in 2018: World's Internet Users Pass the 4 Billion Mark." Global Digital Report 2018, January 30, 2018. https://wearesocial.com/us/blog/2018/01/global-digital-report-2018.
National Research Council 2003. *Internet Under Crisis Conditions: Learning from September 11*. Washington, DC: NATIONAL ACADEMIES Press, 2003.
"NTIA Announces Intent to Transition Key Internet Domain Name Functions." National Telecommunications and Information Administration, March 14, 2014. https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.
Panetta, Leon. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City." Presented at the Business Executives for National Security, New York City, NY, October 11, 2012. https://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.
Powers, Shawn M., and Michael Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom*. History of Communication. Urbana: University of Illinois Press, 2015.
Ricky B. Kelly. "Centralized Control of Space: The Use of Space Forces by a Joint Force Commander." Air University, 1993.
Rid, Thomas. *Cyber War Will Not Take Place*. Oxford University Press, 2013.
Rienzi, Thomas Matthew. *Vietnam Studies: Communications-Electronics 1962-1970*. 1st ed. Washington, D.C., 2002: Department of the Army, 1972.
Robert Fanelli, and Gregory Conti. "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict." Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, 2012. https://westpoint.edu/sites/default/files/inline-images/centers_research/cyber_research_center/PDFs/201206_fanelli.pdf.
Robert K. Knake. "2019: The Beginning of the End of the Open Internet Era." Council on Foreign Relations. *Digital and Cyberspace Policy Program and Net Politics* (blog), January 6, 2020. https://www.cfr.org/blog/2019-beginning-end-open-internet-era.
Rockwell, James M., ed. *Tactical C^3 for the Ground Forces*. AFCEA/SIGNAL Magazine C^3I Series, v. 4. Washington, D.C: AFCEA International Press, 1986.
Sean Kern. "Expanding Combat Power Through Military Cyber Power Theory." *Joint Force Quarterly*, no. 79 (October 1, 2015): 88–95.

Shannon Collins. “Desert Storm: A Look Back.” U.S. Department of Defense, January 11, 2019. https://www.defense.gov/Explore/Features/story/Article/1728715/desert-storm-a-look-back/.

Singer, Peter W., and Emerson Brooking T. *LikeWar, The Weaponization of Social Media*. New York: Houghton Mifflin Harcourt, 2018.

Singer, Peter W., and Allan Friedman. *Cybersecurity: What Everyone Needs to Know*. OUP USA, 2014.

TeleGeography. “Submarine Cable Map.” Submarine Cable Map. Accessed April 1, 2020. https://www.submarinecablemap.com/#/.

The Office of General Counsel, National Oceanic and Atmospheric Administration. “Submarine Cables.” Submarine Cables. Accessed April 1, 2020. https://www.gc.noaa.gov/gcil_submarine_cables.html.

“TRC-170(V) - Archived 7/2000.” Land & Sea-Based Electronics Forecast. Forecast International, July 1999.

United Nations Conference on Trade and Development. “Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries.” United Nations Publications, 2019. https://unctad.org/en/PublicationsLibrary/der2019_overview_en.pdf.

United Stated Department of Defense, Joint Staff. “Joint Publication 3-12, Cyber Operations.” United States Department of Defense, Joint Chiefs of Staff, June 8, 2018. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

———. “Joint Publication 3-13, Information Operations.” United States Department of Defense, Joint Chiefs of Staff, November 20, 2014. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf.

———. “Joint Publication 3-31, Joint Land Operations.” United States Department of Defense, Joint Chiefs of Staff, October 3, 2019. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_31.pdf?ver=2019-12-18-153903-197.

———. “Joint Publication 6-0, Joint Communications System.” United States Department of Defense, Joint Chiefs of Staff, October 4, 2019. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0ch1.pdf?ver=2019-10-15-172254-827.

United States Department of Defense. “Conduct of the Persian Gulf War: Final Report to Congress, Annex K.” United States Department of Defense, April 1992.

———. “Department of Defense Cyber Strategy 2018.” United States Department of Defense, 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

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

Yuxi Wei. “Chinese Data Localization Law: Comprehensive but Ambiguous.” The Henry M. Jackson School of International Studies, University of Washington, February 7, 2018. https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.