Spring 5-6-2020

Rethinking Boundaries, Spaces, and Networks Between Geography and Military Science: Understanding and Actualizing Real-Time Integrated Command and Control for Joint Air Operations

Samuel Wright

RETHINKING BOUNDARIES, SPACES, AND NETWORKS BETWEEN GEOGRAPHY AND MILITARY SCIENCE: UNDERSTANDING AND ACTUALIZING REAL-TIME INTEGRATED COMMAND AND CONTROL FOR JOINT AIR OPERATIONS

By

Samuel Alden Wright

A thesis submitted to the faculty of The University of Mississippi in partial fulfillment of the requirements of the Sally McDonnell Barksdale Honors College.

Oxford

May 2020

Approved by

_____

Advisor: Professor Christian Sellar

_____

Reader: Mr. Kenneth Pope

_____

Reader: Mr. Wesley Yates

ABSTRACT

SAMUEL ALDEN WRIGHT: RETHINKING BOUNDARIES, SPACES, AND NETWORKS BETWEEN GEOGRAPHY AND MILITARY SCIENCE: UNDERSTANDING AND ACTUALIZING REAL-TIME INTEGRATED COMMAND AND CONTROL FOR JOINT AIR OPERATIONS

(Under the direction of Christian Sellar)

Imagine a military commander standing around a table with a three-dimensional hologram projected onto to it. The hologram is of an ongoing air war of which this general is in command. Friendly forces are portrayed in blue and enemy forces in red as the opposing forces movements and actions are tracked and continuously updated. The commander has god's eye view of where his forces are positioned relative to the enemy's forces. Because of this view, the commander is able to make effective decisions with quick synergistic efficiency to achieve his desired outcome: defeat of the enemy. This scene invokes an image akin to a science fiction film of a futuristic air war with man and machine delicately intertwined. Films such as Star Wars and, notably, Ender's Game have portrayed this concept; however, technology and human understanding has made these new concepts a reality. **For the United States military to maintain its overmatch capability advantage over the advanced technologies and concepts of the enemy we must fundamentally shift our doctrine, policies, concepts for better integration of joint air operations. Informed by geography, the goal of this thesis is to call for a new approach to integrating command and control in the context of joint air operations**. China and Russia are growing peer threats that seek to challenge the United States militarily. The current system does not integrate the air, space, and cyberspace domains enough to prosecute air wars. This new approach for joint air operations is called the Real-time integrated command and control system.

Table of Contents

Introduction

From my earliest childhood memories, aviation played a large role in my upbringing. I was born into an Air Force family and can vividly recall the memories of my first military airshow. From that airshow my passion and love for military aviation continued to grow stronger as the years went by. My father was a career Air Force officer, my mother a Peace Corps volunteer. From a very young age, service to my fellow man and woman was instilled in me. My father is a storyteller and he had many to share about his experiences in the Air Force, I listened intently. His stories left me in wonder and awe and further sparked an analytical curiosity. His lessons have a played a large role in me wanting to serve my country as an Air Force pilot. My mother always encouraged and supported me to pursue my dreams. She took me to aviation museums, to buy the next model plane I wanted to build, and the library where I could find those glossy aviation books. Through their love and kindness they encouraged me to take my dreams a reality.

I began to seriously study military aviation in high school, the same time that I began a serious effort toward serving my country as a military pilot. These extracurricular studies led me to books such as *Every Man a Tiger* which was about leading the air campaign during Operation Desert Storm, *Heart of the Storm: The Genesis of the Air Campaign Against Iraq* that discussed planning the air campaign during Operation Desert Storm, and finally *Boyd: The Fighter Pilot Who Changed the Art of War* that discussed rapid decision making processes. All three of these book have a great impact on my thinking. The first two books offered great insight into why the air campaign against Iraq in 1991 was so successful. From them I developed a passion for understanding what it took to plan and lead a successful air campaign. The last book underpinned my foundation for it all, understanding leadership and decision-making processes was what truly

fascinated me. Solving problems that centered around the combination of man and airplane in complex military environments, known as air operations, is where I sought to focus my studies.

As I focused my studies on air operations I began to think about how current and future air operations could be understood given the threats of today and tomorrow. These complex problems meet at the intersection of advanced technology, military thinking, and leadership. It became clear to me that the various mediums that the military operates in have different fundamental understandings of space and time. The mediums, or domains, of air, space, and cyberspace exist in different physical and non-physical environments and have different characteristics. The air and space domain exist in the vertical dimension that allow greater maneuver across vast distances. In the air domain we see the use of aircraft and missiles to reach around the globe in hours and minutes. The military uses the space domain for satellites allowing near-real-time information and communication from across the physical globe. The cyberspace domain exists in a non-physical networked space while being tethered to and having effects in the physical space after spanning the globe within seconds. These different understandings of space and time relative to their respective domains present a fundamental issue with integrating these domains. A large problem that began to formulate in my thoughts was that the military was having a tough time adapting to advanced technologies and future concepts that emphasized integration. The Department of Defense has been slow to react to these growing and modernizing forces, with special attention given to China and Russia. Department of Defense leaders have only advocated for incremental changes to how we think and operate in the joint environment. A fundamental generational gap exists between current military leaders and future military leaders in understanding networks and how to use advanced technologies to achieve military objectives. In the past few years potential adversaries have begun developing advanced technologies and

concepts for military use. It became clear to me that whoever could integrate these technologies and concepts rapidly and effectively would have a distinct military advantage over the other. If a potential adversary were to integrate these advanced technologies and concepts before the United States, the United States would be at a large disadvantage if conflict were to erupt. In the context of joint air operations this means the potential conflicts of the future will be defined by advanced technologies and concepts.

My time spent in geography classes has inspired me to think about military domains in new and creative ways. Three concepts from geographies have played a vital role in this thinking they are, networked spaces, borders as gradients, and vertical geographies. Networked spaces helped in understanding the relationships that exist between humans, machines, places, ideas, and systems across all domains but especially in the cyberspace domain. The notion that borders (boundaries) that exist between all things are gradients rather than hard delineations helped with my thinking on integrating the air, space, and cyberspace domains. And the notion of vertical geographies and the power and height relationship associated with it helped with making sense of the three-dimensional spaces that the air and space domains exist within. The perspective of a geographer helped orient my thinking about how to better integrate military thinking, doctrine, policies, and concepts for joint air operations.

This thesis is a culmination of my passion for military aviation and my thoughts that I have developed over the years. I intend it to be the culmination of my youthful years and the start to a professional career in military aviation. **For the United States military to maintain its overmatch capability advantage over the advanced technologies and concepts of the enemy we must fundamentally shift our doctrine, policies, concepts for better integration of joint air operations. Informed by geography, the goal of this thesis is to call for a new approach**

to integrating command and control in the context of joint air operations. This new approach will be called the Real-time integrated command and control system. The Department of Defense needs to rethink joint air operations completely. It will require a fundamental shift in thinking, doctrine, policies, and concepts for joint air operations. The system itself will be based upon nine foundations: creating an operational environment, establishing operational centers, defining mission requirements, developing operational planning tools, conducting training and exercises, exploring advanced technologies and systems, developing network security, emphasizing force development, and infusing real-time integrated command and control into military thinking**. Three research questions will guide this research and each will inform each of it own subsequent chapters. They are: 1. How has the creation and evolution of military aviation, space, and cyber networks affected how the military interprets space and time? 2. What policies and doctrines guide military air, space, and cyberspace and how do they help or hinder development? 3. How does the integration of the air, space, and cyberspace domains affect the execution of joint air operations?**

Literature Review

Military science and doctrine as described below, will assist us in understanding joint air operations from a three dimensional and network-oriented view. Underpinning all of the work related to current joint air operations are Colonel John Warden's and Colonel John Boyd's theories related to strategic paralysis. Warden argues for viewing the enemy as a system and developed a theory aimed at physical paralysis of the enemy by attacking its five rings (Leadership, Organic/System Essentials/Key Production, Infrastructure, Population, and Fielded Military Forces). Warden was biased towards the use of air power to achieve military objectives and effects with his theory, however his theory was the basic concept for which the air campaign in Desert Storm was planned and executed upon. The Gulf War Air Power Survey, commissioned by the Air Force and conducted independently, provides a supporting argument that Warden's theory was proven correct by the success of the air campaign against Iraq's command and control structure. Boyd argues for psychological paralysis of the enemy through the OODA (Observe, Orient, Decide, Act) loop forcing the enemy to become confused and disoriented (Fadok 1995). Boyd's OODA loop concept can be applied to decision making at any level and is much more expansive in nature than Warden's theory. Because of this, Boyd was not necessarily biased towards air power in his thinking. These two theories are of extreme importance to this body of work.

Theoretical and doctrinal foundational work will come from the Department of Defense and the United States Air Force. Material for understanding the creation and evolution of early airpower theories from General Billy, General Douhet, and General Trenchard will come from Air University's official Air and Space Power Course (ASPC). Air Power in the Age of Total War will prove that Douhet's theory was correct in total war. The bias of this material is pro-air

power. Officially sanctioned joint and Air Force foundational doctrine will support this body of work with definitions and basic understandings. They are the official beliefs and guidance held by the Department of Defense and the United States Air Force. The works are titled: Air Force Basic Doctrine, Doctrine for the Armed Forces of the United States, Air Warfare: Air Force Doctrine Document, Annex 3-13 Information Operations, Department of Defense Dictionary of Military and Associated Terms, and Joint Air Operations. One Air Force procedural document will aid in understanding the Air Operations Center, Operational Procedures - Air Operations Center. One study conducted by RAND will help with explaining the air and space environments and the fundamental characteristics of air, space, and cyberspace forces. An analysis of the issues surrounding the Joint Forces Air Component Commander and the air operations center will aid this thesis in understanding the current level of integration of the air operations center (Woodcock, 2003).

Associated policy and doctrine documents that will aid this body of work will be the Executive Branch's National Security Strategy, the Department of Defense's National Defense Strategy, the Chairman of the Joint Chiefs' National Military Strategy, and Joint Operating Environment 2035. Analytical discussion of the threat posed by peer adversaries will be supported by the Defense Intelligence Agency's reports, China Military Power and Russia Military Power. Further analytical document support will come from the Department of Defense's Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019. These are all officially sanctioned bodies of work published by the United States government.

This work is informed by border geography. The theories and concepts developed by geographers will orient thinking and aid in the creation of the new Real-time integrated

command and control system in chapter three. Three concepts inform this work networked spaces, borders as gradients, and vertical geographies. Many works have some or part of these three concepts included in them. Boundaries affect humans routinely and geographers agree that every aspect of daily life is defined by either a border or borders (Jones 2014, Nail 2016). William Walters has put forth a work that theorizes "live governance" where he discusses how "information, infrastructure, and reaction capabilities combine in such a way that social events and emergencies can be monitored and acted upon in near real-time" (Walters 2016). Many works have provided us various tools to interpret and analyze the border such as Brunet-Jailly's borderlands theory. His theory argues that if four analytical lenses (local cross border culture, political clout, multi-level governance, and market forces/trade flows) help or enhance each other, the border region is more likely to be well integrated (Brunet-Jailly 2005). With regards to vertical geography, Andrew Harris discussed the link associated with power and height (Harris, 2014). The scholarly works mentioned above will aid the thesis by helping to better examine the air, space, and cyberspace domain from the perspective of a border geographer and aid in the development of a three-dimension and network oriented perspective.

Methodology

The following questions will guide the bibliographic research based upon secondary sources concerning military science, history, doctrine, policies, and analyses supported by an interview with a military strategic planner. The research questions are: A) How has the creation and evolution of military aviation, space, and cyber networks affected how the military interprets space and time? B) What policies and doctrines guide military air, space, and cyberspace and how do they help or hinder development? C) How does the integration of the air, space, and cyberspace domains affect the execution of joint air operations?

An interview was conducted with John D. Wright, Colonel, United States Air Force (Retired): Colonel Wright was a leading cyberspace and information warfare strategic planner in the USAF and on the Secretary of Defense's staff. He was engaged in Air Force cyberspace planning to include joint-cyberspace planning and information warfare policy. In 1995, he helped to write "Cornerstones of Information Warfare" for the Air Force which established what is now known as the cyberspace domain. Colonel Wright holds Masters degrees in National Security Strategies (MS) and Human Resource Development (MA).[1]

To answer question A) I will analyze written documents and ask the interviewee questions such as: How has the creation of military aviation, space, and cyberspace networks affected how the

[1] Colonel Wright previously served as a senior Air Force officer (Colonel) for 29 years, with assignments in multiple specialties, as an intelligence, special technical operations, space (operations/control), and information operations officer, in the field in Kosovo during Operation Joint Guardian, Enduring and Iraq Freedom and other operational positions in the Air Intelligence Agency, Air Force Information Warfare Center, Air Combat Command, US Air Forces Europe, Electronic Security Command, National Security Agency, and U.S. Space Command. He commanded at the Group, Squadron, Center, and Detachment levels. As a Joint Specialty Officer, he held transformational Joint positions on a Combatant command, and on the Office of the Secretary of Defense staff. Colonel Wright graduated from Squadron Officer School, Air Command and Staff College, and the Industrial College of the Armed Forces (ICAF) [The current Dwight D. Eisenhower School for National Security and Resource Strategy, formerly known as ICAF.]

military interprets space and time? What are the theoretical and doctrinal foundations of air operations and how have they developed?

To answer question B) I will analyze written documents and ask the interviewee questions such as: What policy and doctrines guide military air, space, and cyberspace and how do they help or hinder development? How do these policies affect joint air operations?

To answer question C) I will analyze written documents and ask the interviewee questions such as: How does the integration of the air, space, and cyberspace affect the execution of joint air operations? What are the current and future threats to joint air operations? What level of integration is needed to defeat current threats? What is needed for the future?

Assumptions

The writer assumes the reader has a basic understanding of the nature and principles of war. The nature of war as described by United States Air Force Basic Doctrine is, "War is an instrument of policy, strategy, or culture…War is a complex and chaotic human endeavor…War is a clash of opposing wills" (AFDD-1, 2015). Following this understanding of the nature of war are the principles of war. The Doctrine for the Armed Forces of the United States identifies nine principles, "Objective, Offensive, Mass, Economy of force, Maneuver, Unity of command, Security, Surprise, and Simplicity" (JP-1, 31, 2013). The nature and principles of war permeate this thesis and must be kept in mind when reading the document.

Chapter 1: The creation and advancement of aviation and cyber networks affect on military science and doctrine

"The airplane is the only weapon which can engage with equal facility, land, sea, and other forces . . . ."

- *Major General Frank M. Andrews*

The creation of air forces, space forces, and cyberspace forces has precipitated new understandings of space and time in the military as an evolving process. New military technologies have enabled the exploitation of the airspace, space, and cyberspace environments. Theory and doctrine has fostered these technological advancements and helped shape how the military views space and time. It has been proven that strategic attack against command and control structures has worked previously. This theory and doctrine discussion serves as background and underpins the conceptual basis of the real-time integrated command and control system for joint air operations.

1.1 The evolution of air, space, and cyberspace technologies on military science and doctrine

In 1909, the first heavier than air military aircraft flew for the first time. Early World War I uses of aircraft for military purposes were initially for reconnaissance purposes. This offered only a vertical perspective similar to the balloons that had preceded them. Technology and counter technologies led to the formulation of basis for varying types of aircraft such as the

fighter, the bomber, and the attack aircraft. During World War I, aircraft and their use were tied heavily to the land domain. It took General Billy Mitchell's anti-ship bombing demonstration in 1921 to prove that surface domains were highly susceptible to aerial attack. In this inter war period, airpower theorists began to emerge with theories typically associated with the future use of air power. General Billy Mitchell, General Guilio Douhet, and Hugh Trenchard became leading air power theorists in this era. Known as the father of the modern Air Force, Mitchell's theory advocated for an independent Air Force separate from the U.S. Air Force and Navy. Mitchell believed that an independent Air Force could be the most effective way of defending the United States and when fighting abroad it could, "decisively attack enemy vital centers without first defeating enemy armies and navies" (ASPC). Mitchell believed that air superiority, or control of the air, was a necessary precondition for all military operations that would follow. Once air superiority was established, Mitchell believed that the air domain could be exploited by targeting vital centers roughly described as, "industry, infrastructure, and agriculture which, when destroyed, would lead to the collapse of civilian morale" (ASPC). This is the foundation of what would become the Strategic Bombing Theory. The theory was developed by Mitchell's disciples at the Air Corps Tactical School in the 1930s. The strategic bombing theory would later play a large and vital role against Germany and in World War II with two years of sustained bombing in Europe before any ground troops arrived. Mitchell's disciples would later be key leaders of U.S airpower: with General Arnold, Commander of U.S Army Air Forces in World War II, and General Spaatz, the first Chief of Staff of the USAF. Mitchell's theories were ahead of their time and the technology needed to accomplish would take years to develop. His thoughts on the prerequisite of air superiority have persisted into the modern day. Parts of his theory were proven correct by the U.S. military's use of air power in the opening part of the Gulf War.

General Giulio Douhet is an another influential airpower theorist. An Italian army officer, he led the first Italian aviation unit during World War I. After the war, Douhet would become a vocal airpower advocate publishing Command of the Air in 1921. His theory had many overlapping assertions shared with Mitchell. Douhet and Mitchell's thoughts aligned on independent air forces separate from army influence, strategic bombing, air superiority, and the offensive role of airpower. Douhet diverged from other theorists with his idea of directly bombing the civilian population to break their morale. A proponent of total war, he believed that breaking civilian morale was crucial, "Once command of the air is won, it must be used to punish the civilians, so that they will coerce their own government to come to terms in order to end the suffering. This will happen so rapidly that total suffering will be less than that experienced in the trenches" (ASPC). Douhet's influence and work eventually culminated in an independent Italian air force in 1923. Parts of his work were translated into English and used in the Air Corps Tactical School in the United States that educated future U.S airpower leaders who would eventually shine during World War II. His total war theory were proven correct under the multiple firebombing raids and two atomic bombs against Japan. Over 100,000 people died in the firebombing raid in Tokyo, 40 percent of the area destroyed, and around one million people left homeless (Buckley, 193, 1999). Firebombing would destroy many other cities in Japan. His controversial thoughts on targeting civilian populations illustrate the grimmer side of airpower and its potential applications.

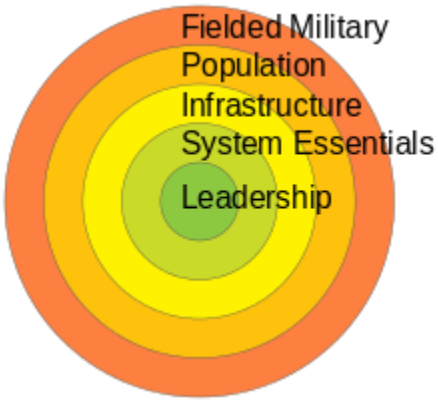
The last of the three great airpower theorists is Marshal of the Royal Air Force, Hugh Trenchard. Like Mitchell and Douhet, Trenchard flew in World War I and would later serve as the head of the British Royal Air Force. During the war, Trenchard was opposed to an independent air force and the strategic bombing concept. His initial opposition was largely in

part to his upbringing as a traditional infantry officer, during World War I, "… he was firm in his commitment to ground support and only allowed excess aircraft to be dedicated to independent operations" (ASPC). With the evolution of technology and the conclusion of the war, he changed his views in favor of maintaining an independent air force and the strategic bombing concept. Trenchard had a large influence on the early development of the British Royal Air Force as Chief of the Air Staff after the war. He faced heavy resistance from the army and navy who sought to reintegrate flying as part of their respective services. The Air Marshal was crucial in building the foundational institutions and doctrine required for an independent air force. He began to rely heavily on the strategic bombing concept to distance himself from his army and navy counterparts and create a unique mission for the Royal Air Force. Trenchard also had influence on U.S. air power theorists by showing them what not to do. The Royal Air Force originally combined the army and the navy's aircraft into one service; however this was a blunder for the Royal Navy and their air arm was eventually returned. This helped to strengthen the position for retaining U.S Naval aviation. For the majority of World War II, the Royal Air Force participated in the strategic bombardment of Europe due in part to Trenchard's early influence on the service.

The strategic bombing concept played a great role in showing the value of independent air forces to concentrate mass upon the enemies. No longer was air power tethered to the ground solely supporting surface forces through tactical air power and close air support. The effect of the stagnant trench warfare in World War I helped to inform air power theorists that an alternative means to victory was needed. The evolution of technology and World War II proved many early air power theorists ideas effective with the use of air power and the strategic bombing in the defeat of the axis in Europe and Asia. As the ideas and technology matured, the capabilities of

air forces grew and subsequently allowed greater effects on the enemy through a wider range of strategies and tactics for campaign planning and execution.

While strategic bombing focused heavily on destroying the enemies economic capacity to wage war by attacking physical targets such as "industry, infrastructure, and agriculture," the next evolution would focus on achieving strategic paralysis by taking out an adversary's ability to command and control his forces. Focusing on maneuver warfare, two air power theorists, Colonel John Warden and Colonel John Boyd, developed two differing approaches to achieving strategic paralysis by going after the command and control functions of the enemy. Colonel Warden's model focused on five rings in a bullseye orientation. The rings consists of leadership at the center, system essentials, infrastructure, population, and then the fielded military as the outermost ring. Leadership is the most important ring to attack as it is in the center. Warden advocated for striking at the heart of the enemy by going after their leadership and leadership functions. Warden's theory was focused on attacking physical targets and thus achieving physical paralysis.



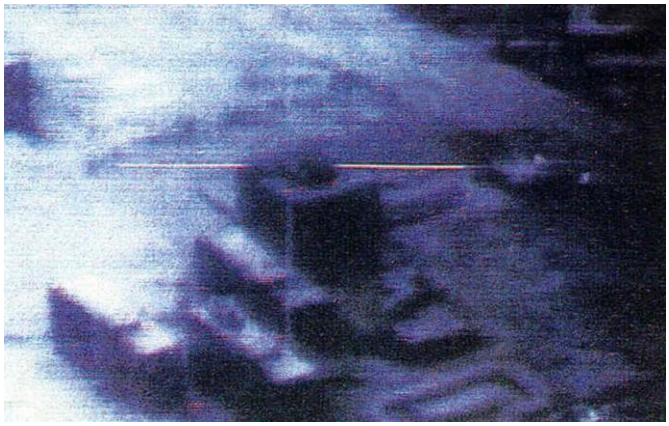


Figure 1-1. Warden's five rings on left (Five Rings, 2014) Figure 1-2. The central Iraqi communications hub from a USAF F-117 moments before being destroyed in the early moments of Operation Desert Storm on right (Rogoway, 2018)

Warden's theory heavily influenced the air campaign planning for Operation Desert Storm where U.S. and coalition air power heavily focused their efforts on striking at heart of the Iraqi leadership's command and control of their forces. His theory was proven correct by the success of the air campaign (Keaney, Cohen, 242, 1993). Colonel John Boyd's theory emphasizes achieving strategic paralysis of the enemy through psychological incapacitation. Boyd's concept is known as the OODA loop, each letter standing a different part of the loop Observe, Orient, Decide, Act. The loop itself explains a process for decision making; however, Boyd went further by detailing how the OODA loop could be used against an opponent. He contended that whoever completed the OODA loop cycle quicker would be able to get inside the adversary's OODA loop and gain the advantage. This would cause the adversary to focus on reaction and defensive measures and allow the friendly forces to gain the offensive or create space for the next decision. If friendly forces got inside the decision making loop of the opponent, the enemy would be concentrated internally instead of externally, eventually loosing situational awareness.

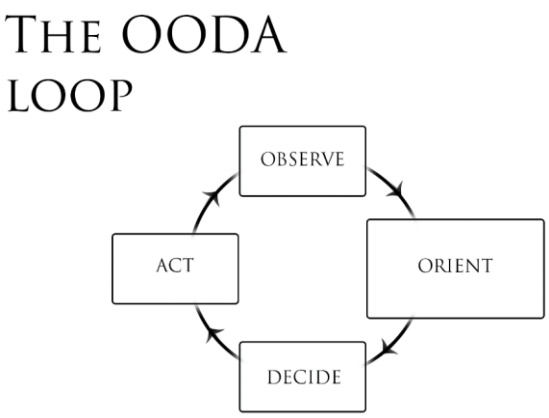


Figure 1-3. The OODA Loop showing the four stages of the decision making process (Pearson, 2019).

1.2 The military understanding of Air, Space, and Cyberspace Environments

A basic understanding of the environments is needed to grasp how these three forces act in their respective domains. Air and space domains, "are continuous around the globe, have no boundaries, are above the mediums of land and sea, permit observation of operations in these other mediums, and provide free access to any point on or above the earth" (RAND, 11). The cyberspace domain is indeed continuous around the globe, without classic boundaries, and permeates the physical mediums. The air and space domains are found in the third vertical dimension. Cyberspace is described in terms of a layered model. Three interrelated layers are described as the physical network, the logical network (virtual), and the cyber-persona. As this thesis focuses on the real-time integration of command and control for joint air operations, the space and cyberspace domains will further enable operations in the air domain.

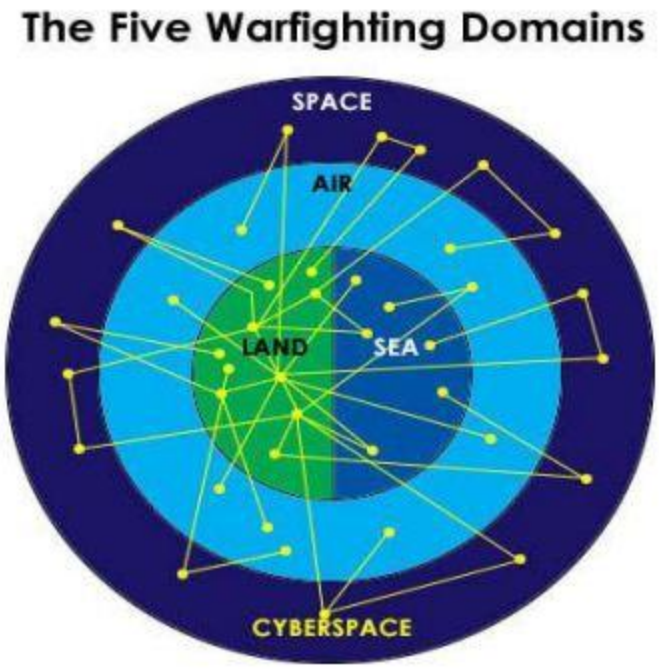


Figure 1-4. The five domains on the left showing air, space, and cyberspace in orientation to the other domains (Modern War Domains)

1.3 Air, Space, and Cyberspace Forces Characteristics

Forces within these three domains possess unique characteristics inherent to them. Air and Space forces possess, "speed, range, maneuverability, perspective, and mobility of large payloads" (RAND, 10). Cyberspace forces also utilize, speed, range, maneuverability in addition to connectivity and accessibility through various means. All three forces are flexible and versatile because of these characteristics. Air, space and cyberspace characteristics, "provide the opportunity to gain perspective over the entire battle space and to apply power directly against all elements of an enemy's resources, regardless of their location" (RAND, 11).

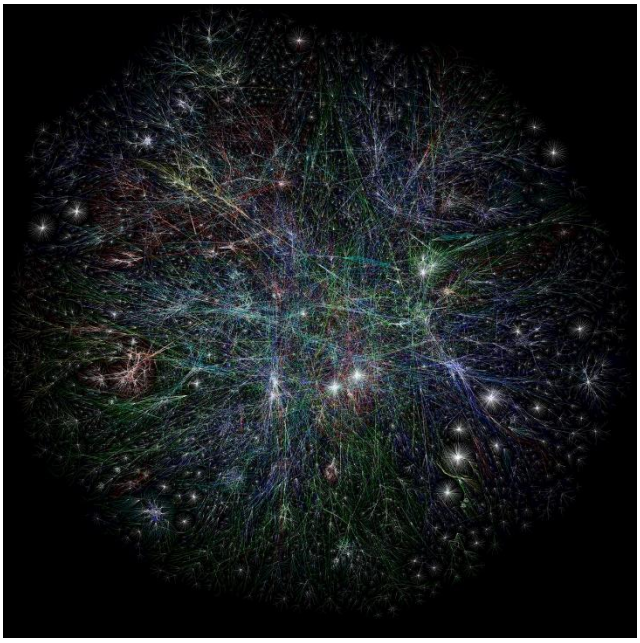


Figure 1-6. A map of the internet circa 2005, highlighting the connectivity that cyberspace affords (7 Amazing, 2015)

1.4 Technologies, Capabilities, and Effects

The military describes new technologies in terms of capabilities related to the air, space, and cyberspace domains and their respective characteristics. Technologies are viewed as a way to achieve a desired outcome. In this case, the desired outcome maybe certain objectives or effects against an enemy. Because of the three-dimensional orientation (vertical) coupled with the network orientation (horizontal) of air, space, and cyberspace these technological capabilities can create synergistic effects around the globe measured in hours and minutes (aircraft) and seconds (space and cyberspace).

1.5 Understanding the interconnected relationships of machines and humans

Three interconnected digital and cognitive relationships exist between machines and humans. Generic levels are machine to machine, machine to man, and man to man. Air

operations inherently embed humans and technology and intertwine them together. Understanding and codifying these three inter and intra-dependent relationships will assist this thesis in organizing the interaction of these relationships.

1.6 Air Operations and Information Operations

From recent conflicts we have learned that two type of operations that enhance each other significantly are air operations and information operations. Due to the technical and psychological nature of air and information operations, they are closely linked and are best employed by effective command and control. Air operations, in the simplest terms, is described by the air force as operations that, "…involve the employment of air assets by themselves or in concert with other assets or forces and are part of the overall joint campaign" (AFDD3-1, 2, 2011). While the basic definition for information operations is, "the integrated employment, during military operations, of information-related capabilities [IRCs] in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own" (AFDD3-13, 1, 2016). Within both definitions, they recognize the necessity and interdependency for the other type of operation as well as the integration of both.

1.7 Command and Control (C2)

Air operations requires robust command and control. The United States Department of Defense defines command and control (C2) as, "The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission" (JP 1-02, 40, 2010). Due to the characteristics of air operations mentioned in section 1.3, air operations are best conducted, "using centralized control and decentralized execution to

achieve effective control and foster initiative, responsiveness, and flexibility. Centralized control is giving one commander the responsibility and authority for planning, directing, and coordinating a military operation or group/category of operations… Decentralized execution is the delegation of execution authority to subordinate commanders." (JP 3-30, I-3, 2019). The principal location where command and control of air assets takes place is the air operations center (AOC).

Chapter 2: Policy and Doctrine's Affect on Air Operations

Policy and doctrine guides and informs how air operations are formulated and conducted, therefore it is important to understand and analyze specific policy and doctrine guidance related to air operations. This chapter will focus on a top down policy and doctrine approach that starts with the President's guidance that is articulated through the National Security Strategy, then to the Department of Defense's National Defense Strategy, the Joint Staff's National Military Strategy, followed by Joint Operating Environment. The policy and doctrinal guidance gleaned from these documents asserts that the United States military must retain overmatch capabilities to win against peer adversaries. The documents give the strategic and operational policy and doctrinal guidance necessary to create a new system for joint air operations. Peer adversaries are building their military capabilities with advanced technologies and operating concepts. This thesis aims to provide an overmatch capabilities in the form of the Real-time integrated command and control system.

2.1 The 2017 National Security Strategy

The President and the Executive Branch periodically issue a National Security Strategy that outlines national interests and establishes goals and priorities in line with the national interests. The strategy illustrates the geo-political and geo-economic factors that the United States has prioritized. The document focuses on synthesizing the instruments of national power commonly referred to as DIME. The acronym, DIME, each letter stands for the four instruments diplomatic, informational, military, and economic. The aim is to give broad and clear guidance to

the federal government and allows individual departments and agencies to align their missions and functions with the document. The most recent National Security Strategy was published in 2017 under the Trump Administration.

The National Security Strategy recognizes upfront that the world is competitive and that many authoritarian state and rogue non-state actors are on the rise. It emphasizes a shift back to great power competition as authoritarian regimes such as China and Russia seek to challenge the United States. The strategy states that Russia and China, "are determined to make economies less free and less fair, to grow their militaries, and to control information and data to repress their societies and expand their influence" (NSS, 2, 2017). It further addresses the growing regional security concerns surrounding North Korea's nuclear missile program and Iran's growing influence in the Middle East. The strategy then shifts gears in acknowledging the transnational threat that terrorists networks pose to the United States. Two key points are taken from the introduction that will further assist this thesis. They are, "U.S. advantages are shrinking as rival states modernize and build up their conventional and nuclear forces…," and that, "The ability to harness the power of data is fundamental to the continuing growth of America's economy, prevailing against hostile ideologies, and building and deploying the most effective military in the world" (NSS, 3, 2017). With the threats to the United States' security laid out, the National Security Strategy seeks to address those concerns.

The current National Security Strategy focuses on the security of four national interests known in the document as the four pillars. The strategy is based on the idea of putting America first and the four pillars align to achieve this. The four pillars are first, "to protect the American people, the homeland, and the American way of life… promote American prosperity… preserve peace through strength… advance American influence…" (NSS, 4, 2017). The first pillar is

focused on the defense on the United States and outlines some of its priorities. The priorities focus on homeland defense from unconventional threats at home and abroad. This pillar prioritizes preventing, "…nuclear, chemical, radiological, and biological attacks, block terrorists from reaching our homeland, reduce drug and human trafficking, and protect our critical infrastructure" (NSS, 7, 2017). The second pillar emphasizes the economy through promoting American prosperity, with the underpinning belief that "Economic security is national security." The pillar centers on the notion, "American prosperity and security are challenged by an economic competition playing out in a broader strategic context… Experience shows that these countries distorted and undermined key economic institutions without undertaking significant reform of their economies or politics" (NSS, 17, 2017). This pillar seeks to hold other countries accountable through reciprocity and fair trading. The third centers on deterrence or as the strategy states, "preserve peace through strength" (NNS, 35, 2017). The strategy intends to accomplish this by, "rebuilding our military so that it remains preeminent, deters our adversaries, and if necessary, is able to fight and win. We will compete with all tools of national power to ensure that regions of the world are not dominated by one power. We will strengthen America's capabilities—including in space and cyberspace—and revitalize others that have been neglected. Allies and partners magnify our power…" (NSS, 14, 2017). The third pillar aligns directly with this thesis as it provides the broad guidance necessary to facilitate a new approach to command and control for joint air operations. The fourth and final pillar concentrates on promoting American influence by placing a strong emphasis on American global leadership and advancing American values. The first paragraph of this section clearly states the importance that the, "America First foreign policy celebrates America's influence in the world as a positive force that can help set the conditions for peace and prosperity and for developing successful societies"

(NSS, 37, 2017). This is in recognition of the growing threats and influence from actors that seek destabilization and authoritarian approaches.

Within the third pillar of preserving peace through strength places a great significance in renewing military capabilities. The strategy states that, "The United States must retain overmatch— the combination of capabilities in sufficient scale to prevent enemy success and to ensure that America's sons and daughters will never be in a fair fight… To retain military overmatch the United States must restore our ability to produce innovative capabilities, restore the readiness of our forces for major war, and grow the size of the force so that it is capable of operating at sufficient scale and for ample duration to win across a range of scenarios" (NSS, 28, 2017). The most important quote that enhances this body of work and puts it directly in line with the National Security Strategy is that, "The Department of Defense must develop new operational concepts and capabilities to win without assured dominance in air, maritime, land, space, and cyberspace domains…" (NSS, 29, 2017). This statement and the one above gives the broad policy guidance needed to implement a new approach is needed to integrating command and control in the context of air operations so that the United States can retain overmatch capabilities.

2.2 The 2018 National Defense Strategy

In line with the National Security Strategy, the Department of Defense regularly publishes a new National Defense Strategy. It is the Secretary of Defense's principal document and translates the geo-political and geo-economic interests of the United States into military guidance. Essentially, the National Defense Strategy is the link between the political leadership and the military leadership. It provides context by describing the strategic environment, objectives for the department, and a strategic approach for implementation. The current National

Defense Strategy was published in 2018 and penned under Secretary of Defense James Mattis and his staff.

The National Defense Strategy outlays a bleak look for the global environment. The current strategy emphasizes, "Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security" (NDS, 1, 2018). The strategy upfront mentions China and Russia as strategic competitors and as the main priorities for the department, as well as North Korea and Iran, and then a small blurb on terrorism. It states that, "The central challenge to U.S. prosperity and security is the reemergence of long-term, strategic competition by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model—gaining veto authority over other nations' economic, diplomatic, and security decisions" (NDS, 2, 2018). The strategy goes on to discuss the evolving technology and the essence of war, "The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology — the very technologies that ensure we will be able to fight and win the wars of the future." (NDS, 3, 2018). All of the above technologies will play a pertinent role in the need for a new approach to command and control in the context of air operations.

Eleven defense objectives are then outlined and focused around the following statement, "…the Department of Defense will be prepared to defend the homeland, remain the preeminent military power in the world, ensure the balances of power remain in our favor, and advance an international order that is most conducive to our security and prosperity" (NDS, 4, 2018). In the

context of the National Security Strategy, this is a refinement of the broad guidance given from within that document and translated into military specific guidance.

The final section focuses upon a strategic approach built upon three lines of effort to address the return to great power competition. The National Defense Strategy outlines three lines of effort, "First, rebuilding military readiness as we build a more lethal Joint Force; Second, strengthening alliances as we attract new partners; and Third, reforming the Department's business practices for greater performance and affordability" (NDS, 5, 2018). The first line of the strategic approach is expounded upon over three pages. A subset of rebuilding military readiness is the modernization of key capabilities. It places a strong emphasis on the cyber domain, "We will also invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations" (NDS, 6, 2018). The strategy outlines the importance of command and control and information operations, "Investments will prioritize developing resilient, survivable, federated networks and information ecosystems from the tactical level up to strategic planning. Investments will also prioritize capabilities to gain and exploit information, deny competitors those same advantages, and enable us to provide attribution while defending against and holding accountable state or non-state actors during cyberattacks" (NDS, 6, 2017). From there, the line of effort focused on rebuilding military readiness stresses the importance of "joint lethality in contested environments," it specifically states that, "The Joint Force must be able to strike diverse targets inside adversary air and missile defense networks to destroy mobile power-projection platforms" (NDS, 6, 2017). Other noteworthy sections discuss the need for agility in the contested operational environment in addition to advanced autonomous systems such as artificial intelligence and machine learning. The greatest piece of this strategy that aligns strongly with this thesis is the need to, "Evolve innovative operational concepts:"

> Modernization is not defined solely by hardware; it requires change in the ways we organize and employ forces. We must anticipate the implications of new technologies on the battlefield, rigorously define the military problems anticipated in future conflict, and foster a culture of experimentation and calculated risk-taking. We must anticipate how competitors and adversaries will employ new operational concepts and technologies to attempt to defeat us, while developing operational concepts to sharpen our competitive advantages and enhance our lethality (NDS, 7, 2018)

The combination of constantly evolving technology and new operating concepts is line with the purpose of this thesis, that we must develop new technologies and operating concepts for joint air operations. By rebuilding military readiness, the National Defense Strategy seeks to modernize capabilities in cyber, command and control, information operations, joint lethality in regards to air operations, autonomous systems, and the need for new operational concepts.

2.3 The 2018 National Military Strategy

The National Military Strategy is the document produced by the Chairman of the Joint Chiefs of Staff. The most recent National Military Strategy was published in 2018 under the 19th Chairman of the Joint Chiefs of Staff, General Joseph Dunford. The strategy links the Department of Defense's National Defense Strategy guidance to the operational level, and allows the Chairman to provide advice on joint force operations. The strategy outlines national military objectives, describes desired outcomes, capabilities, and risk assessments of the joint operational environment. Due to the sensitive nature of the document, it is classified, however an unclassified summary is available and will be analyzed in its place.

The summary is broad but touches on the key highlights of the actual National Military Strategy. It seeks to illustrate a strategic approach by relying on the security trends outlines in the National Defense Strategy. After outlining the security trends, the strategy states that, "To achieve military advantage over competitors and adversaries, the NMS introduces the notion of joint combined arms, defined as the conduct of operational art through the integration of joint capabilities in all domains. The Joint Force and its leaders must be as comfortable fighting in space or cyberspace as they are in the other three traditional domains of land, sea, or air" (NMS, 2, 2018). The need for the integration of domains and the necessity to emphasize the cyberspace domain is paramount to integrating the command and control of air operations. The strategy then pivots to force employment. It briefly describes the missions that the strategy helps to fulfill. The missions are, "Respond to Threats, Deter Strategic Attack, Deter Conventional Attack, Assure Allies and Partners, Compete Below the Level of Armed Conflict" (NMS, 3, 2018). From there it shifts to force development and force design, "Force Development adapts current planning, decision making, and force management processes to enable the Joint Force to do what it does better. Force Design enables the Joint Force to do what it does in fundamentally different and disruptive ways to ensure the Joint Force can deter or defeat future adversaries" (NMS, 4, 2018). In the conclusion of the document, the summary does make note that China and Russia are "great power competitors," which is the only direct mention of other state or non-state actors in the entire description. The National Military Strategy brings together the Chairman's guidance on force employment and joint combined arms, force development, and force design.

2.4 The Joint Operational Access Concept and Joint Operating Environment: 2035

The Joint Operating Environment: 2035 (JOE 2035) provides a picture of the security situation of the world in 2035 and what challenges the United States military will face due to

future trends. The security situation in 2035 will be one that is based on "contested norms and persistent disorder" (JOE 2035, 4, 2016). The document paints a very complex and challenging global environment that the military has to operate within. It is organized into three sections, the future security environment 2035, contexts of future conflict, and finally the implications for the joint force. The paper has pertinent relevance towards rethinking command and control for air operations.

In the first section of JOE 2035, the security environment in 2035 is laid out. It subsequently has three sub-sections that identify trends in world order, human geography, and science, technology, and engineering. For this thesis, the last sub-section is germane as it discusses future systems integration and the proliferation of information technology. Future joint air operations will further rely upon increased systems integration for greater capability and effect. The future proliferation of information technology poses a threat to joint air operations and further justifies the need for an overmatch capability in joint air operations. The sub-section identifies the need for effective systems integration,

> Effective technology integration into military operations requires the capacity to bring together many different capabilities into a coherent, purposeful whole. Even today, the largest, most capable states struggle to match their ability to develop individual technologies with the ability to integrate these technologies into a single system. By 2035, improvements to individual devices, tools, or platforms will likely become less important than the system architectures which allow dissimilar capabilities to work together coherently (JOE 2035, 16, 2016).

The level of integration that JOE 2035 is identifying as a trend is paramount to the holistic approach of the integration of command and control structures for air operations. The security

environment section then shifts to the emerging trend of proliferated information technologies. It broadly identifies the diffusion of expensive information technologies and data to actors and smaller countries that did not previously have access. Two specific trends of note are regional command and control parity and the exploitation of command and control vulnerabilities (JOE 2035, 18, 2016). The document assesses that, "As a range of sensors, information networks, information processing, and data fusion capabilities becomes widely available to potential adversaries from high-end states to lower-end insurgent and irregular forces, U.S. military forces may be identified, tracked, targeted, and attacked at range" (JOE 2035, 18, 2016). The next trend noted in this section tackles the technological exploitation of command and control vulnerabilities and notes a complex and dynamic environment. JOE 2035 states that, "Technologies that can damage, spoof, confuse, or disrupt integrated battle networks will become increasingly available. U.S. and partner C3/ISR systems will require enhanced system protection, greater network redundancy, and automated defenses capable of reacting in a highly dynamic environment" (JOE 2035, 18, 2016). The assessment that command and control exploitation capabilities will become more readily available requires strong defensive measures for protection in the future. The future shift towards increasing systems integration, information parity, and the increasing exploitation of command and control capabilities will require a new approach to the command and control of air operations.

The next section of the JOE 2035 centers around what conflict may look like in the future. Overall, this section identifies six "contexts" associated with conflict of the future. Two of these contexts are noteworthy and are key to improving command and control for air operations. JOE 2035 identifies the future conflicts as "disrupted global commons" and "a contest for cyberspace." The context of disrupted global commons focuses on the notion of anti-

access/area-denial in spaces and places available to all but owned by none," while a contest for cyberspace emphasizes the, "struggle to define and credibly protect sovereignty in cyberspace" (JOE 2035, 31, 34, 2016). Highly advanced technological adversaries will threaten and disrupt the global common and challenge the United States military, "…to break the power projection capabilities of adversary states, including modern mechanized forces on land and sophisticated naval forces at sea, all protected by advanced aerospace and electromagnetic jamming and spoofing capabilities. Furthermore, a number of adversaries will invest in hypersonic weapons, and the first nation to successfully deploy an operational system will gain significant military advantages due to the speed at which targets can be engaged" (JOE 2035, 30, 2016). Conflict in 2035 will also see a heavily contested cyberspace domain. While this context is heavily focused on the idea of defining and protecting cyberspace sovereignty, it does mention the future development of states cyberwarfare capabilities, "Some states may also integrate cyber warfare capabilities at the operational and tactical levels of war, attempting to degrade military networks in order to adversely affect the Joint Force as it deploys or operates in the field" (JOE 2035, 36, 2016). Future development of cyber warfare capabilities at the operational level may pose a significant threat to the command and control of air operations. The section further addresses the increasing speed of future warfare and the need to defend against it as, "…hypersonic weapons and robotic swarms will increase the tempo of conflict and will be countered by the development of artificial intelligence for battlespace characterization and management" (JOE 2035, 36, 2016). The notion that artificial intelligence for command and control purposes is also extremely pertinent for air operations.

The final section of JOE 2035 speaks to how the security environment will affect joint operations and how these security concerns must be addressed. From this certain military tasks

are brought to light that must be prepared for 2035. Recognizing that potential enemies of the future will focus on anti-access/area-denial to counter the United States, JOE 2035 argues that, "the Joint Force must be prepared to conduct Global Maneuver and Seizure to defend important interests, retake key terrain, or seize critical objectives captured by an adversary. In these missions, the Joint Force will delay further adversary aggression through defensive actions while simultaneously conducting targeted strikes and raids to disrupt adversary initiatives" (JOE 2035, 47, 2016). The emphasis on maneuver warfare complements and parallels discussion in chapter one on Warden's five rings and the OODA loop. JOE 2035 later moves to a discussion on large scale operations, "…the Joint Force must be prepared to conduct Major Sustained Combat to destroy a countervailing power, alliance, or partnership or compel them to recognize U.S. interests. These missions should seize the initiative by reducing adversary defenses at range, followed by the use of speedy, targeted offensive actions to destroy adversary global and regional strike assets, to include nuclear capabilities. Combined offensive operations will then be required to seize key terrain from adversaries and permanently eradicate resistance" (JOE 2035, 49, 2016). The document's attention to major sustained combat in the future further strengthens the need for extensive preparation against potential peer competitors with military parity.

Chapter 3: The Military Applications and Integration of the Air and Cyberspace Domains Affect on Air Operations

Figure 3-1. The air operations center of today, left (Strang) Figure 3-2. The real-time integrated command and control system, right (Eurofit)

"Using the cyberspace domain to give commanders better situational awareness warrants improving how we conduct ourselves today; using cyberspace to distribute decision making with new visualization, connected sensors and platforms, planning and decision tools, faster operational cycles, and battle-changing engagement - - is transformational."

- *Colonel John Wright*

The command and control of air operations must be further integrated in real-time to address threats. Chapter one of this thesis laid out the theoretical and doctrinal foundations of airpower and its use of technology. Discussion focused on a basic understanding of those foundations, maneuver warfare concepts, and the use of border geographer research for

understanding air operations. Real-time integrated command and control of air operations will be guided by these theories and doctrinal foundations. Chapter 2 then discussed the policy and doctrinal guidance associated with air operations. It found that the guidance in relevant policy and doctrine broadly calls for the need for better integration of the warfighting domains to defend against current and future threats from peer and near-peer adversaries. To maintain a competitive edge in the military battlespace, the command and control of joint air operations must be further integrated to real-time activities. This chapter will first discuss the current and future threat, then speak to the current level of integration for the command control of air operations, and finally the need for real-time integrated command and control of air operations.

3.1 The current threat and future threat

Currently, adversarial threats exist and others are beginning to take shape that seek to challenge the United States and its interests. These adversaries seek to challenge the United States militarily directly through conventional means of warfare and indirectly through unconventional means of warfare. Peer-adversaries have focused their efforts on so called anti-access/area-denial strategy and doctrine that seek to limit the United States' ability to wage war.

The National Security Strategy identified China and Russia as rising challengers to the United States power. China and Russia have in the past few years shifted their respective strategies to challenge the United States militarily. Both are currently modernizing and growing their militaries for potential conflict against a peer adversary. The countries are modernizing their command and control structures to reflect joint military operations similar to western militaries. China and Russia both emphasize strategies focused on anti-access/area-denial and are building their forces in kind.

The modernization of Chinese forces centers around building, "a strong, combat-effective force capable of winning regional conflicts and employing integrated, real-time command and control networks" (DIA, 23, 2019). China is emphasizing anti-access/area-denial forces, "In addition to strike, air and missile defense, anti-surface, and anti-submarine capabilities improvements, China is focusing on information, cyber, and space and counterspace operations" (OSD, 54, 2019). The modernization of the Chinese military means that they will be able to project military power farther than before and with more effect. Chinese anti-access/area-denial planning emphasizes a maritime focus on operations that, "…includes the development of anti-access/area-denial capabilities to conduct long-range attacks against adversary forces who might deploy or operate within the western Pacific Ocean" (OSD, 55, 2019). To keep the enemy out, China focuses heavily on the use of various long-range missiles. Notably, China is developing long range hypersonic cruise missiles capable of covering great distances in extremely short amounts of time. China is seeking to modernize their forces rapidly to project power regionally and eventually globally.

Figure 3-3. China's anti-access/area-denial capabilities (The Economist, 2018)

Russia is also emphasizing the growth of their military around an anti-access/area-denial strategy. Russia has payed close attention to how the United States conducts joint air operations since Operation Desert Storm, "Russia repeatedly cites in open source literature the need to repel or defend against a Western aerospace attack. Russia would seek to deter any Western use of aerospace power against Russia using its conventional, non-strategic nuclear, and, in extreme circumstances, its strategic nuclear forces" (DIA, 32, 2017). Russian anti-access/area-denial strategy focuses on information operations, offensive air operations, a robust integrated air defense system, and long-range cruise missiles including hypersonics. Heavy Russian emphasis on anti-access/area-denial will pose a viable threat to joint air operations.

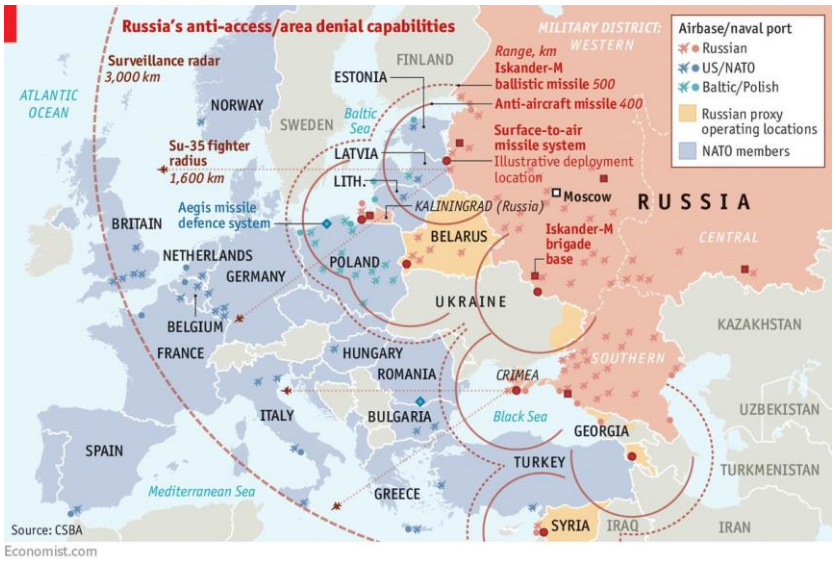


Figure 3-4. Russia's anti-access/area-denial capabilities (The Economist, 2018)

China and Russia both also believe that information operations are crucial to their warfighting capabilities and their respective anti-access/area-denial strategies. The Chinese People's Liberation Army, "…uses the term 'informatized warfare' to describe the process of acquiring, transmitting, processing, and using information to conduct joint military operations across the domains of land, sea, air, space, cyberspace, and the electromagnetic spectrum during

a conflict. PLA writings highlight the benefit of near-real-time shared awareness of the battlefield in enabling quick, unified effort to seize tactical opportunities" (DIA, 24, 2019). Russia also highly values information operations, they, "…are seen as a critical capability to achieve decisive results in the initial period of conflict with a focus on control of the information spectrum in all dimensions of the modern battle space. Authors often cite the need in modern warfare to control information—sometimes termed "information blockade" or 'information dominance'—and to seize the initiative early and deny an adversary use of the information space in a campaign so as to set the conditions needed for 'decisive success'" (DIA, 32, 2017). Information operations for both China and Russia play key roles in their anti-access/aera-denial strategies.

The United States reliance on the cyberspace domain for the command and control of joint air operations shall be increasingly threatened. Adversaries espouse advancing their cyberspace capabilities. Colonel Wright states that in cyberspace,

> …future attacks can and will occur worldwide, especially from adversaries not able to engage the U.S.A. with force by conventional means. Increases in computing power, doctrinal development, and changes in the focus of adversarial cyber-attacks will make cyberspace more challenging and hostile. Cyber-attacks will continue and become more related to military operations. Adversaries' will enhance their means, tactics, techniques, and procedures to challenge our military cyberspace capabilities. In redefining cyberspace power for this century, we must account for anti-American current and potential adversaries operating in vast corners of cyberspace, exploiting the low access costs and minimal technological investment needed to impact our missions. We also face increased levels of risk for information security because of greater network use and

> technology pervasiveness on a global scale. We can ill afford to allow adversaries to militarily employ these critical capabilities as we seek to deny them sanctuary while ensuring our access and operations in these domains (Wright, 2020).

China and Russia both are bolstering their cyber and electronic warfare capabilities. The Chinese Military Strategy noted that, "China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability" (DIA, 56, 2015). Russia has focused on building cyber capabilities as well, "Since at least 2010, the Russian military has prioritized the development of forces and means for what it terms "information confrontation," which is a holistic concept for ensuring information superiority, during peacetime and wartime. This concept includes control of the information content as well as the technical means for disseminating that content. Cyber operations are part of Russia's attempts to control the information environment" (DIA, 38, 2017). Both China and Russia argue for the control of information environment through cyberspace capabilities that are currently being built.

China and Russia have both been building up their electronic warfare capabilities in recent years. The Chinese People's Liberation Army has created the new PLA Strategic Support Force as a branch that is dedicated to employing space, cyber, and electronic warfare capabilities (DIA, 97, 2019). Russia also is building up their capabilities, "Russia has aspirations to develop and field a full spectrum of electronic warfare capabilities to counter Western C4ISR and weapons guidance systems" (DIA, 42, 2017). China and Russia both are building up their

electronic warfare capabilities for their anti-access/area-denial operating concepts against western adversaries.

3.2 The current level of integration: the air operations center

The current level of integration of the air and cyberspace domains is less than totally effective. In the face of the threats mentioned above, cracks begin to emerge in the integration of the air and cyberspace domains due to the reliance on a command and control center called the air operations center. While the air operations center is largely survivable and affords the necessary level of integration for the low intensity conflict of today, it is less survivable and not fully integrated enough to be effective in high intensity air operations of today and the future.

The air operations center is the single hub for the command and control of air operations. In Air Force doctrine, the air operations center is thought of and considered as a weapons system similar to how aircraft are viewed as they both enable and achieve effects (see section 1.4). The air operations center has an enormous staff and support personnel of over 1,300 (Woodcock, 126, 2003). The air operations center is based on the notion of centralized control and decentralized execution. This means that the air operations center is physically located in one place and operations are controlled from here. Specific execution of the orders of air operations takes place in many locations typically, theater wide. The air operations center has many functions, but the primary function is to, "Task and execute day-to-day air, space, and information operations; provide rapid reaction, positive control, and coordinate and deconflict weapons employment as well as integrate the total operations effort" (AFI13-1AOCV3, 10, 2011). The basic organization of the air operations center focuses on five divisions under the air operations center commander: strategy division, combat plans divisions, combat operations division, the intelligence, surveillance, and reconnaissance division, and the air mobility division.

It also has smaller specialty and direct support teams within itself when needed. The air operations center produces a plan for called the air tasking order which is the daily plan for air operations. It roughly takes 36 to 48 hours to complete one air tasking order. By the time it is disseminated the, "…the majority of its assumptions, analyses, and targeting decisions are out of date" (Woodcock, 127, 2003). Targeting processes are also of issue, "Too often, by the time the target is analyzed and identified, it is no longer visible… Current technology has not caught up with requirements; these tasks are not being performed rapidly enough" (Woodcock, 127, 2003). The air operations center has functioned well in the low and medium intensity conflicts of the past due to the enemy possessing little to no capability or will to render it ineffective.

Per the threats, the current air operations center is vulnerable and likely not survive in high intensity conflict. The inherent nature of the center based on centralized control means that as it functions as a single point of failure once taken out, is not returning to operational status in sufficient needed time frames. While multiple air operation centers exist and it has been proven that other air operations centers can assume the responsibility of a down center, they remain at risk. Peer adversaries that possess comparable or superior air forces, advanced cyber capabilities, and advanced missiles shall be able to render the air operations center ineffective in conducting air operations.

3.3 The need for real-time integrated command and control capabilities

As stated previously, real-time integrated command and control for air operations must be developed and fielded. The command and control functions of air operations not only need to be effective in high intensity conflict, but survive for the entirety conflict. The current system, the air operations center, will likely not survive and not be effective enough in high intensity conflict and must be replaced. Colonel Wright states that, "…we must deliver joint component

situational awareness tools and techniques to robustly defend, anticipate, and respond to adversaries in joint air operations" (Wright, 2020). Broadly, the National Security Strategy asserts that the United States must maintain overmatch by producing innovative capabilities. To maintain an overmatch in the command and control of joint air operations in future conflicts against peer adversaries that have strategies supported by anti-access/area-denial capabilities and systems, a new system for air operations must be realized.

Foundations must be created at the strategic and theater level to actualize a real-time integrated command and control system for joint air operations. Outlined below are nine foundations: create an operational environment, establish operational centers, define mission requirements, develop operational planning tools, conduct training and exercises, explore advanced technologies and systems, develop network security, emphasize force development, and infuse real-time integrated command and control into military thinking. Each one of these nine foundations will be addressed below.

3.3.1 Create an operational environment

Real-time integrated command and control for joint air operations must work on distributed networks for future warfighting environment. The threats from China and Russia currently make it imperative to do so. These new capabilities must no longer focus on centralized control and decentralized execution due to the single points of failure of the current air operations center, therefore, it must be based on distributed and agile architectures. This will ensure the redundancy of the system in the face of an attack across multiple domains. Data processing must also be distributed further ensuring redundancy and survivability. As previously stated in chapter two, "…improvements to individual devices, tools, or platforms will likely become less important than the system architectures which allow dissimilar capabilities to work

together coherently" (JOE 2035, 16, 2016). It must integrate all systems and capabilities into a dynamic structure, meaning that every piece is part of the whole requiring open systems architecture so that different technologies and processes will be seamlessly integrated together. This means in the traditional sense that all military personnel, technology, equipment, and supplies will be distributed into self-sustaining cells needed to conduct joint air operations. These units will be able to operate independently against the enemy but also have the ability to operate as one against the enemy in coordinated attacks.

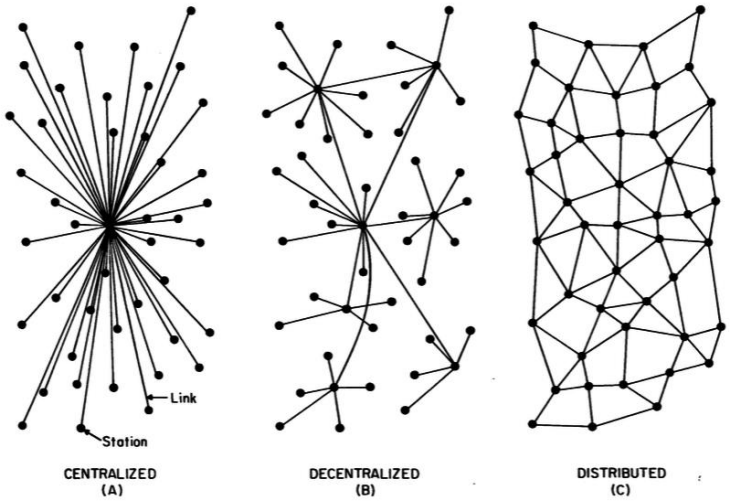


Figure 3-5. System architecture showing centralized, decentralized, and distributed networks (Eager, 2017)

3.3.2 Establish operational centers

Real-time integrated command and control for air operations will require the establishment of new operational centers. These survivable centers will enable leaders to rapidly plan, direct, coordinate, and control joint air operations. They will be able to be commanded by anywhere from the leader of the air campaign to small unit leaders who can disseminate orders

and quickly coordinate with other units. Operational centers must be distributed and will be small in size and staff and mobile allowing military commanders and planners the ability to maneuver quickly while operations are taking place. This shall afford commanders options in the face of advanced weapons systems that seek to target operational centers for destruction. The center must be capable of using many different user interfaces such as a table-top, tablet, or disk like structures along with human user interfaces. This system and sub-systems will produce a complete picture of the battlespace with enemy forces correlated against blue forces in a three dimensional and network-oriented view. It will also fuse together civilian leaders and non-adversary actors relative to the battlespace. Hologram technology that can enable voice and hand instruction may be used to display and operate the overall system. This should allow greater mobility and require less personnel to operate distributed centers.

3.3.3 Refine Mission Requirements

The real-time integrated command and control system must be able to anticipate and respond with air operations all the way from the strategic to the tactical level. This means that the system needs requirements focused on a range of operational environments. This could mean refining requirements for an air war against an irregular insurgency force in a low intensity conflict all the way to refining requirements for a mission against a peer adversary in a high intensity conflict. The system requirements shall be based lined but also flexible with deliverables that are scalable.

3.3.4 Develop operational planning tools

The real time integrated command and control system will require the development of operational planning tools. These tools will enable the rapid and effective fusion and

dissemination of accurate information, enhanced decision making, and analysis. These tools will assist in the quick and effective dissemination of combat orders or plans to relevant forces. Some possible tools may assist in the processes similar to what are now known as the Master Air Attack Plan, Air Tasking Order, Airspace Control Order, and Special Instructions. Operational planning tools shall be baked into baselines and adapt to be effective for coordination of air operations

3.3.5 Conduct testing, training, and exercises

The real-time integrated command and control system must be refined by training with and heavily used in joint air operations exercises and emphasize interoperability with all domains. Beforehand this system must be tested in research and development center settings. Users of the system must become effective in operating portions or all of the system from the strategic to the tactical level. At a minimum, users will be trained at multiple levels and shadow real world events plus pre-planned exercises to assess its effectiveness and remediate deficiencies.

3.3.6 Employ advanced technologies and systems

For this system to operate, advanced technologies must be employed. Research and development of technologies shall be conducted to include but are not limited to: autonomous systems, artificial intelligence, machine learning, quantum computing, nanotechnology, self-healing systems, self-replicating systems, sensor fusion, and human interfaces.

The system must rely heavily on advanced automation of the majority of previous processes and tasks done by trained military personnel so that military command and control decisions can be made rapidly and efficiently. Advanced algorithms with emphasis on artificial

intelligence, machine learning, and quantum computing can collect, analyze, and rapidly disseminate information inherent in the functions of command and control. The system will provide the most critical information available while handling the majority of tasks and processes for planning, exploitation, defense, and offense. The artificial intelligence will employ the tenets of air power and emphasize maneuver warfare, rely on border geography understanding, use strategic paralysis through targeting command and control processes, and emphasize rapid and effective decision making to defeat an adversary. Given decisions in real-time the advanced automation will then rapidly disseminate orders, associated information, and data quickly to relevant areas. These advanced algorithms, processing, and displays shall shoulder the burden previously done by the large staffs and the slow and sequential tool set of the current air operations center.

3.3.7 Develop network security

For a system of this nature to survive, the development of robust network security must be evolved and agile. The security operations of the distributed network must be able to be protect and defend the entirety of the system. This includes, but is not limited to, protecting information, computers, networks and shielding assets such as aircraft, satellites, vehicles, and humans from disruption, degradation, denial, or destruction from adversaries. The system must be self-healing and self-replicating and continue to operate in a degraded state to further ensure redundancy and survivability. If attacked in multiple domains, the system must be able to outmaneuver the adversaries by sensing and countering in multiple or all domains simultaneously. If the system does incur degradation or damage, the artificial intelligence and advanced algorithms must repair the system rapidly or self-replicate critical functions needed to continue air operations even in a reduced or degraded state. Real-time integrated command and

control for air operations must inherently be able to defend against advanced adversarial capabilities across all domains. The system must be able to rapidly receive indications/warnings from information collection, then detect, identify, track, and assign weapons systems, and then engage and assess the effects upon the adversary.

3.3.8 Emphasize Force Development

Force structure must evolve to operate and support the real-time integrated command and control system in all environments. Personnel must be trained in specified skills and competencies to conduct real-time integrated command and control air operations. At a minimum, these forces must be able to operate in three dimensions and from an agile network perspective.

3.3.9 Infuse real-time integrated command and control in military and academic thinking

Real-time integrated command and control of air operations shall be incorporated into military and academic thinking. This will include new military strategy, processes, concepts, and doctrine. It will allow real-time integrated command and control perspectives and ideas to be given the necessary attention in out training and schools. Border geographers and fellow social scientists in academia not typically associated with the military will be called upon to help develop this command and control system thinking. Border geographers deal extensively with understanding and mapping spaces and will be able to provide fresh perspective to this three-dimensional and network-oriented system.

Conclusion

Informed by the geography concepts of networked space, borders as gradients, and vertical geographies, the goal of this thesis is to call for a new approach to integrating command and control in the context of joint air operations Chapters one through three address a specific research question in a sequential orders: 1. How has the creation and evolution of military aviation, space, and cyber networks affected how the military interprets space and time? 2. What policies and doctrines guide military air, space, and cyberspace and how do they help or hinder development? 3. How does the integration of the air, space, and cyberspace domains affect the execution of joint air operations? From the theoretical and doctrinal foundations of airpower, to the policy and doctrinal guidance, to the threats faced from potential adversaries such as China, and to the current integration issues that all culminate in the need for a real-time integrated command and control system for air operations.

Chapter one addressed the question how has the creation and evolution of military aviation, space, and cyber networks affected how the military interprets space and time? It asserts that strategic attack against command and control structures has worked previously. The chapter discussed the history of air power and associated theories that were advanced by early air power advocates such as General Billy Mitchell. General Mitchell advocated for strategic attack of the enemy that prioritized destruction of the enemy's physical industry and infrastructure. As technology progressed, Colonel Warden and Colonel Boyd developed approaches designed to cause strategic paralysis of the enemy by destroying command and control structures. Colonel Warden advocated for the physical paralysis while Colonel Boyd advocated for psychological paralysis of the enemy. Discussion then transitioned to the military understanding of air, space, and cyberspace domains. The chapter described the specific domain characteristics and then the

military's understanding of technologies, capabilities and effects. Brief sections outlined the interconnected relationships of humans and machines, followed by the doctrinal foundation of air operations, information operations, command and control.

Chapter two answers the question, what policies and doctrines guide military air, space, and cyberspace and how do they help or hinder development? It found that the United States perceives the modernization of Chinese and Russian as a threat that must be addressed from the strategic to the tactical level. It further found that the United States military must maintain overmatch capabilities to win against peer-adversaries like China and Russia. The necessary policy and doctrinal guidance at the strategic and operational level has been given to support the real-time integrated command and control system for joint air operations. The section covered three strategic policy documents, The National Security Strategy, The National Defense Strategy, and The National Military Strategy. The chapter then discussed a doctrinal document, Joint Operating Environment: 2035.

Chapter three addresses how integration of the air, space, and cyberspace domains affect air operations and calls for the need for real-time integrated command and control for air operations to be actualized. The chapter is grounded in the theoretical and doctrinal foundations from chapter one and the policy and doctrinal guidance from chapter two. With this understanding, the current and future threat is discussed. Emphasis is placed on the modernization efforts of China and Russia's militaries for anti-access/area-denial operations that harness advanced command and control, cyberspace/information operations, space operations, hypersonic missiles, and missile defense systems. The next section of chapter three emphasizes the current level of integration of the command and control of air operations. It finds that the current level of integration falls way short of what is required and that the air operations center is

thus less survivable in high intensity conflict. With this notion, the chapter finally calls for the actualization of the real-time integrated command and control system to assure overmatch capabilities against peer adversaries and provides the foundations needed to develop this new capability and capacity.

Fielding the real-time integrated command and control system for air operations is complex, but must be actualized to maintain the United States military's overmatch capability in the air operations environment. The real-time integrated command and control capability needs to be fused in military science, doctrine, and air operations given the vital functions it provides for joint air operations. The real-time integrated command and control system is less about the past command and control structures accomplishments, but more about real-time display and execution of command and control functions in domains and spaces that have highly fluid boundaries. The system must effectively account for rapid and dynamic changes to boundaries in the battlespace. The challenges and opportunities of actualizing the real-time integrated command and control system warrant extreme innovation and transformation in military operating concepts, distributed network structures, rapid processes, and advanced technologies so that the United States will be able to counter the high intensity threats of today and of tomorrow.

Bibliography

"AFDD-1 Air Force Basic Doctrine." *U.S. Air Force Doctrine > Home*, Curtis E. LeMay Center for Doctrine Development and Education, 27 Feb. 2015, www.doctrine.af.mil/Core-Doctrine/Vol-1-Basic-Doctrine/.

AFDD 3-1, Air Warfare. Curtis E. LeMay Center for Doctrine Development and Education, 22 Jan. 2000, www.globalsecurity.org/military/library/policy/usaf/afdd/3-1/afdd3-1_2011.pdf.

"AFDD 3-13, Information Operations." *U.S. Air Force Doctrine > Home*, Curtis E. LeMay Center for Doctrine Development and Education, 28 Apr. 2016, www.doctrine.af.mil/Doctrine-Annexes/Annex-3-13-Information-Ops/.

"AFI13-1AOCV3, OPERATIONAL PROCEDURES-AIR OPERATIONS CENTER (AOC)." *Air Force E Publishing*, USAF, 2 Nov. 2011, static.e-publishing.af.mil/production/1/af_a3_5/publication/afi13-1aocv3/afi13-1aocv3.pdf.

"ASPC." *ASPC*, College of Aerospace Doctrine, Research and Education, www.iwar.org.uk/military/resources/aspc/text/theory/obj.htm.

Brunet-Jailly, Emmanuel. "Theorizing Borders: An Interdisciplinary Perspective." *Taylor & Francis*, 2005, www.tandfonline.com/doi/abs/10.1080/14650040500318449.

Buckley, John. *Air Power in the Age of Total War*. UCL Press, 1998.

"DIA China Military Power." *Defense Intelligence Agency*, 2019, www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf.

"DIA Russia Military Power." *Defense Intelligence Agency*, 2017, www.dia.mil/portals/27/documents/news/military%20power%20publications/russia%20military%20power%20report%202017.pdf.

Eagar, Mari. "What Is the Difference between Decentralized and Distributed Systems?" *Medium*, Pathfinder Leadership, 4 Nov. 2017, medium.com/distributed-economy/what-is-the-difference-between-decentralized-and-distributed-systems-f4190a5c6462.

Eurofit, https://in.pinterest.com/pin/208502657724769485/?amp_client_id=CLIENT_ID(_)&mweb_unauth_id=&simplified=true

Fadok, David S. *John Boyd and John Warden Air Power's Quest for Strategic Paralysis*. Air University Press, 1995, media.defense.gov/2017/Dec/27/2001861508/-1/-1/0/T_0029_FADOK_BOYD_AND_WARDEN.PDF.

"Five Rings." *Five Rings*, 12 Dec. 2014, militaryanalysis.blogspot.com/2014/12/five-rings.html.

Harris, Andrew. "Vertical Urbanisms: Opening up Geographies of the Three-Dimensional City." *Progress in Human Geography*, vol. 39, no. 5, Oct. 2015, pp. 601–620, doi:10.1177/0309132514554323.

"JOE 2035, Joint Operating Environment: 2035." *Joint Chiefs of Staff*, Department of Defense, 14 July 2016, www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917.

Jones, Reece. "Placing the Border in Everyday Life." *Google Books*, Google, 2014, books.google.com/books?hl=en&lr=&id=BiYHDAAAQBAJ&oi=fnd&pg=PP1&dq=info%3Axvn4jBw-61oJ%3Ascholar.google.com&ots=C7X1A41X9z&sig=s1J9DpMLuzK14-8TyV2fjCfiVqI#v=onepage&q&f=false.

"JP-1 Doctrine for the Armed Forces of the United States." *Joint Chiefs of Staff*, Department of Defense, 25 Mar. 2013, www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf.

"JP 1-02 Department of Defense Dictionary of Military and Associated Terms." *Joint Chiefs of Staff*, Department of Defense, 8 Nov. 2010, fas.org/irp/doddir/dod/jp1_02.pdf.

"JP 3-30 Joint Air Operations." *Joint Chiefs of Staff*, Department of Defense, 25 July 2019, www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf.

Keaney, Thomas A., and Eliot A. Cohen. *Gulf War Air Power Survey*. For Sale by the U.S. G.P.O., Supt. of Docs., 1993.

"Modern War Domains." *MODERN WAR DOMAINS*, www.angelfire.com/games2/warpspawn/MWD.html.

Nail, Thomas. "Book Review: Theory of the Border by Thomas Nail." *LSE Review of Books*, 21 Mar. 2017, blogs.lse.ac.uk/lsereviewofbooks/2017/01/31/book-review-theory-of-the-border-by-thomas-nail/.

"NMS Description of The National Military Strategy." *Joint Chiefs of Staff*, Department of Defense, 2018,www.jcs.mil/Portals/36/Documents /Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf.

"NSS National Security Strategy of the United States of America." *The White House*, 2017, www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

"NDS Summary of The National Defense Strategy." *Department of Defense*, Department of Defense, 2018, dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

"OSD, ANNUAL REPORT TO CONGRESS Military and Security Developments Involving the People's Republic of China 2019." *Department of Defense*, Office of the Secretary of Defense, 2019, media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

Pearson, Taylor. "The OODA Loop: How to Turn Uncertainty into Opportunity." *Taylor Pearson*, 30 July 2019, taylorpearson.me/ooda-loop/.

"RAND The Source of Basic Doctrine: Fundamental Characteristics of Airpower." *RAND Corporation*, RAND Corporation, www.rand.org/content/dam/rand/pubs/monograph_reports/MR927/MR927.chap2.pdf.

Rogoway, Tyler. "Listen To This Highly Interesting Radio Recording Of The F-117's Latest Flight Over Nevada." *The Drive*, Action Media Inc., 30 July 2018,

www.thedrive.com/the-war-zone/22515/heres-a-highly-interesting-radio-recording-from-the-f-117s-latest-flight-over-nevada.

Strang, Joshua. “Combined Air Operations Center.” *Home Page of Hanscom Air Force Base*, United States Air Force, www.hanscom.af.mil/News/Photos/igphoto/2001777213/.

“The Odds on a Conflict between the Great Powers.” *The Economist*, The Economist Newspaper, 25 Jan. 2018, www.economist.com/special-report/2018/01/25/the-odds-on-a-conflict-between-the-great-powers.

Walters, William. “Live Governance, Borders, and the Time–Space of the Situation: EUROSUR and the Genealogy of Bordering in Europe.” *Academia.edu*, 2016, www.academia.edu/35751809/Live_governance_borders_and_the_time_space_of_the_situation_EUROSUR_and_the_genealogy_of_bordering_in_Europe.

Woodcock, William A. “The Joint Forces Air Command Problem.” *Naval War College*, Naval War College Review, 2003, digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2181&context=nwc-review.

“7 Amazing Maps of the Internet.” *Daily English Global Blogkasperskycom*, 3 Nov. 2015, www.kaspersky.com/blog/amazing-internet-maps/10441/.