CYBERSPACE MISSION FOCUS: NW OPS VS. NETOPS

GRADUATE RESEARCH PROJECT

Travis J. Hawker, Major, USAF
AFIT/ICW/ENG/10-03

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

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

AFIT/ICW/ENG/10-03

CYBERSPACE MISSION FOCUS: NW OPS VS. NETOPS

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Travis J. Hawker

Major, USAF

June 2010

AFIT/ICW/ENG/10-03

CYBERSPACE MISSION FOCUS: NW OPS VS. NETOPS

Travis J. Hawker
Major, USAF

Approved:

//Signed//	9 Jun 2010
Robert F. Mills, PhD (Chairman)	Date
//Signed//	9 Jun 2010
Michael R. Grimaila, PhD (Member)	Date

Abstract

This research outlines a method of reasoning for understanding warfighting domains, defining operations within a warfighting domain (primarily offensive, defensive and security) and correlating that operational understanding into mission requirements within the Air Force in order to better answer the questions, "How do we fly, fight and win in cyberspace?" In doing so, this research will attempt to show that what is currently coined as defensive operations on the network are in fact more properly aligned with the doctrinal definition of security in the air and land domains. Furthermore, this research will focus on the inherent differences between the Air Force specific missions of Network Warfare Operations and Network Operations, primarily operations vs. maintenance, and how this different mission focus is misrepresented in terms of personnel and organizational structure. Finally, it will, in response to this misrepresentation, provide brief examples of personnel and organizational changes, using the air domain as a model, which may better align Air Force cyberspace efforts with the ever pressing unique mission requirements resident within the domain.

Acknowledgements

I would like to first thank my advisor Dr. Robert Mills, as well as all my professors and classmates here at the Air Force Institute of Technology, for providing me the guidance required and the necessary knowledge over the last year to succeed in this program. It is truly through your efforts and mentorship that a student may reach their potential.

Additionally, I would like to thank my fellow Cyber Warfare classmates of class ICW-10J. It is through the unique and differing backgrounds and perspectives we have shared, argued and often laughed that I will look back on this experience with fond memories. It has been a blast; look forward to seeing great things from each of you!

- Travis

Table of Contents

Table of Figures

CYBERSPACE MISSION FOCUS: NW OPS VS. NETOPS

I. Introduction

Background

Cyberspace is a new and ever changing warfighting domain. The Air Force has shifted focus to this domain over the last five or ten years with a watchful eye to the importance this domain plays on its ability to execute its mission in support of national security objectives. It has instituted such transformation as a new career field and vast changes in organizational structure with relation to its networks. However as this domain continues to grow and develop, so too must the willingness of the service to meet this challenge and carry out its 2008 mission statement of *"The mission of the United States Air Force if to fly, fight and win in Air, Space and Cyberspace."* With this increased focus on the cyberspace warfighting domain, Air Force leaders and Airmen alike, have asked the question, "How DO we fly, fight and win in cyberspace?"

Purpose

The purpose of this research is to provide a brief discussion on how the service can answer this question. It will offer a short background on the current state of the Air Force's cyberspace efforts and some apparent shortfalls with respect to mission focus. It will begin by outlining the principles of warfighting domains and a brief summary of how operations are conducted within them, primarily comparing and contrasting offensive, defensive and security operations within the air, land and cyberspace domains. Through this, it will attempt to show that what is currently coined as defensive operations on the

network are in fact more properly aligned with the doctrinal definition of security as seen in the air and land domains. Furthermore, this research will focus on the inherent differences between the Air Force specific missions of Network Warfare Operations and Network Operations, primarily operations vs. maintenance, and how this different mission focus is misrepresented in terms of personnel and organizational structure. Finally, it will, in response to this misrepresentation, provide brief examples of personnel and organizational changes that may better align Air Force cyberspace efforts with the ever pressing unique mission requirements resident within the domain. The overall objective of this research is provide a basic outline for how to further understand the domain, define operations within it and project this understanding to mission requirements and the resources needed to meet them within the cyberspace domain.

Scope

This research takes a broad to narrow approach. Initially, it discusses the factors that define environments and domains in a broad sense and then narrows this discussion to the domains of air, land and cyberspace as defined in *Joint Publication 3-0 Joint Operations, Army Field Manual 3-0 Operations, Air Force Doctrine Document 2 Operations and Organization* and *Air Force Doctrine Document 3-12 (Draft) Cyberspace Operations,* for the purpose of understanding operational art within warfighting domains. Focus then shifts to how the Air Force currently operates within the cyberspace domain through its missions of Network Warfare Operations and Network Operations as defined in Air Force Doctrine Document 2-5 Information Operations and the 2006 Warfighter

Integration Plan with the intention of defining the differences between these unique missions and identifying how those differences affect the Air Force's cyberspace efforts.

II. Principles of a Warfighting Domain

Defining the Environment

When discussing concepts such as warfighting domains and the force applications a military service will use to operate within those realms, it is wise to define the parameters of the discussion to avoid confusion. Each domain carries unique environmental factors and definitions that provide for one's conceptual understanding of the physical space an environment consists of. *Merriam-Webster Dictionary* defines an environment as: "the complex of physical, chemical and biotic factors that act upon an organism or an ecological community and ultimately determine its form and survival". Each environment (air, land, sea, space and cyberspace) is unique from the others due to the physical characteristics that set them apart (Figure 1):

- **Air**: the mixture of gases that surround the earth
- **Land**: the solid part of the earth
- **Sea**: great bodies of salt water that cover much of the earth
- **Space**: The region beyond the earth's atmosphere
- **Cyberspace**: energies and properties of electronics and the electromagnetic spectrum

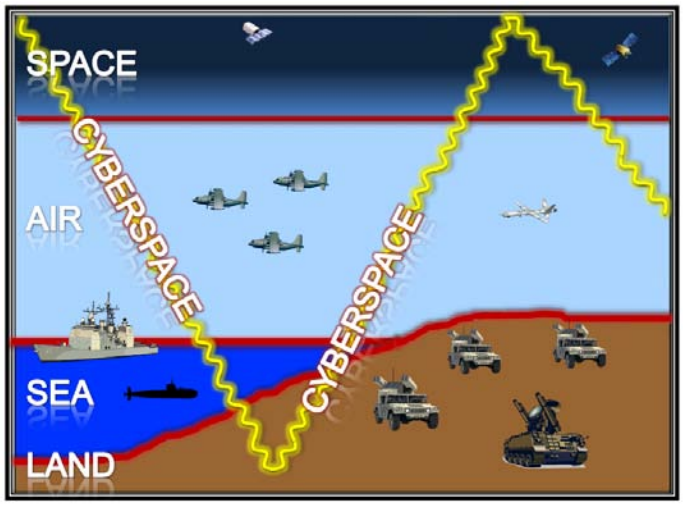


Figure 1: Physical Environments

Each environment is subject to various factors and scientific principles beyond the physical space outlined above making their utilization and exploitation unique. For example, within the air environment, there are four enduring environmental forces that must be understood and studied in order to operate and exploit this environment: weight, lift, drag and thrust. If there is more thrust than drag and more lift than weight, then flight is possible. However in order take advantage of these forces and how they relate to each other, continuing scientific breakthroughs with respect to those forces have led to technological advances focused on the exploitation of the air environment. The Bernoulli Principle, developed by Daniel Bernoulli, for example states that the faster air moves, the less pressure it exerts. This principle ultimately led to the development of the modern airplane wing. As shown in Figure 2, the air traveling over the curved top portion of the wing has farther to go, and therefore moves faster, creating lift. If lift is sufficient, flight is possible.

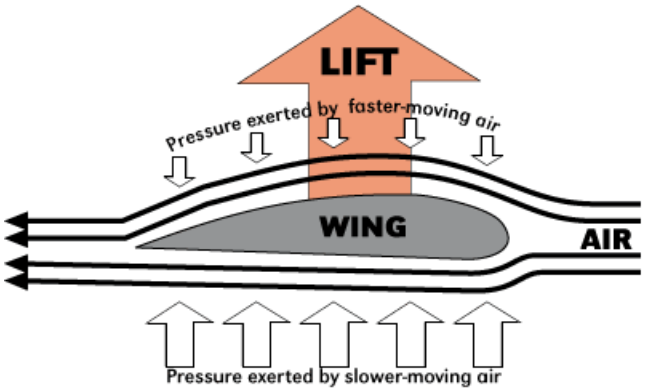


Figure 2: Bernoulli Principle (Yes Mag, 1996)

Cyberspace is similar when it comes to possessing unique environmental factors and scientific principles which define it as a distinctive environment for use and exploitation. It is primarily defined by the underlying properties of electronics and the electromagnetic spectrum, both of which allow for energy and information to traverse

through the environment. Wavelength, frequency and amplitude for example, are three underlying factors that govern how signals are propagated through the cyberspace environment. Through the understanding and manipulation of the relationship between these factors and the traits each possesses, mankind has learned to exploit various portions of the electromagnetic spectrum (Figure 3) for the purpose of transmitting information. Much like Bernoulli's Principle led to the exploitation of air through flight, Heinrich Rudolf Hertz's experiments proving that signals could be transmitted via electromagnetic waves paved the way for the eventual exploitation of the cyberspace environment through the development of radios and wireless telegraphs; thus the Hertz designation seen today in radio and electrical frequencies.

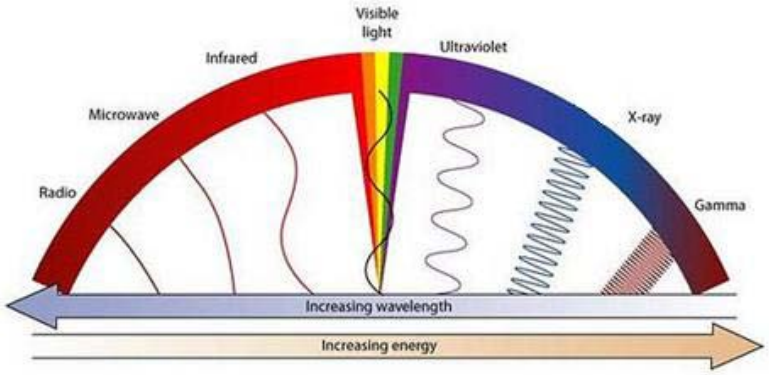


Figure 3: Electromagnetic Spectrum (U. of Waikato, 2007)

Domain Evolution

As understanding of these environments progresses, technologies continue to evolve for utilization within and exploitation of these physical environments (vehicles on land, powered ships at sea, airplanes in air, satellites in space and computers in cyberspace to name a few). And as these technologies evolve, so do the reliance on them and the capabilities they provide. As reliance morphs to dependence on the capabilities,

the result is an economic, social and political security issue resulting in the necessity to ensure use of those environments as a function of national security and the ability to guarantee unfettered access to them as goal of military strategy. Therefore, the broad environmental definitions of land, air, sea, space and cyberspace have been scoped based on these dependencies and coined warfighting domains for the purpose of securing and defending them as a national security imperative. For example, the cyberspace warfighting domain has been defined in *Joint Publication 3-0* and echoed in the draft of *Air Force Doctrine Document 3-12* as:

> *Cyberspace consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers. Within cyberspace, electronics and the electromagnetic spectrum are used to store, modify and exchange data via networked systems.*

As a result, it can be seen that the environment of cyberspace, has been drastically tailored focusing only on the portions of the electromagnetic spectrum that are utilized for the purpose of storing, modifying and exchanging data through networked systems (the Internet, telecommunications and computer networks and the embedded processors and controllers of which they are comprised) as depicted in Figure 4. So for the purpose of flying, fighting and winning in the cyberspace domain, it is obvious that the focus is only on those portions of the environment defined within the domain,

Figure 4: Environment Scoped to Domain

excluding large portions of the electromagnetic spectrum used today such as radio (examples can be seen in the Department of Defense (DoD) Joint Spectrum Center Electromagnetic Chart, Figure 5).

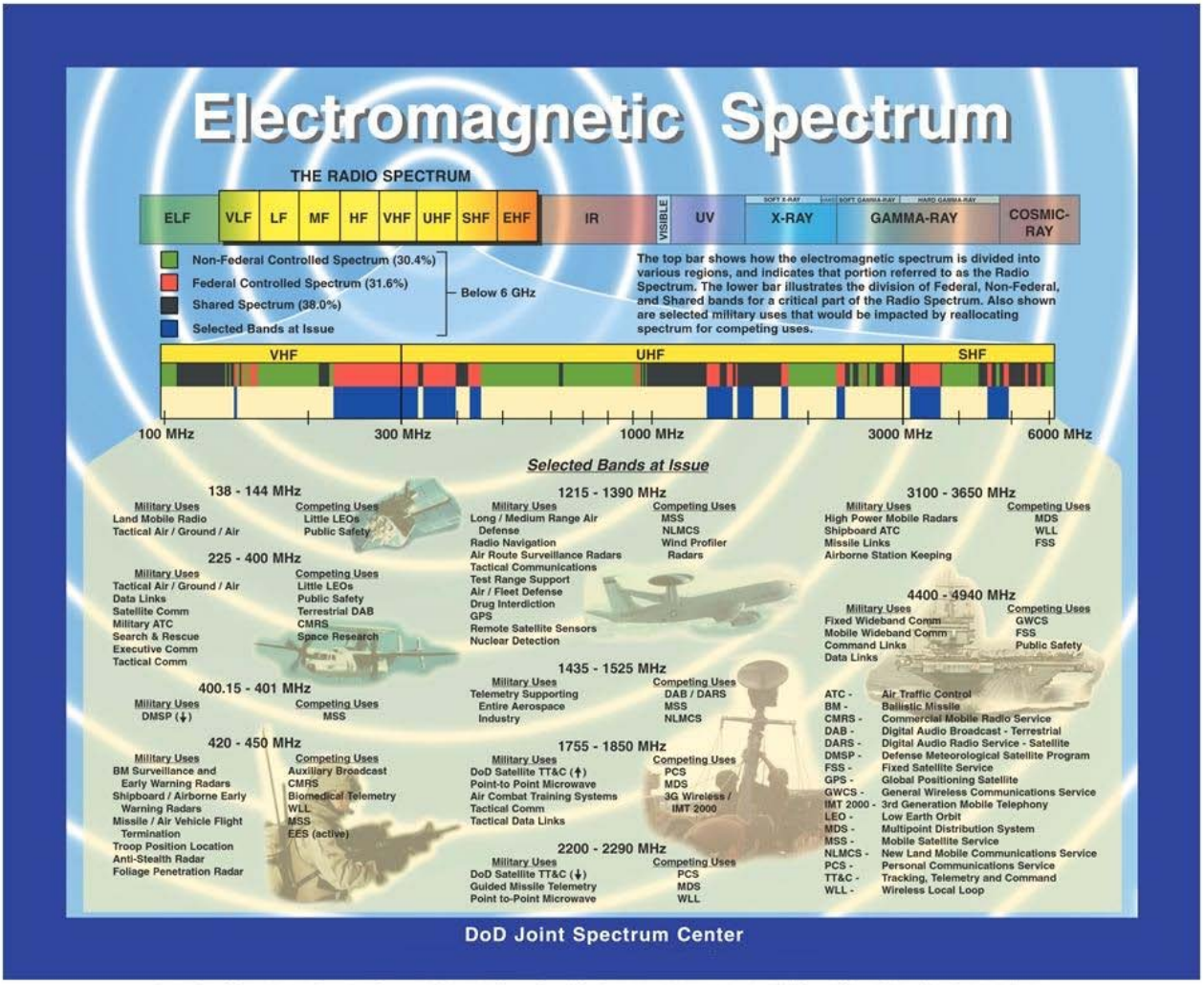


Figure 5: DoD Joint Spectrum Center Electromagnetic Spectrum Chart (DISA, 2010)

This tailoring of environment to domain results in two unique definitions which are in some respects drastically different. It is this distinction between environment and warfighting domain definition must be understood to ensure clear and accurate focus

when defining operations within a domain and the forces that will be charged with carrying out those operations. Lack of understanding will result in a confused operational picture of what must be accomplished within the battlespace. For this reason, this research will focus on the cyberspace warfighting domain (not environment) as defined above and the forces and missions associated with that domain.

Factors Influence Domain Operations

Just as the overarching environments of air, land, sea and cyberspace have basic properties which define them as unique physical environments and allow mankind to exploit them, warfighting domains also possess factors that influence operations within them as unique domains. These significant factors determine how a commander may apply operational art to achieve overall strategic objectives within the domain. They can utilize the ends (desired end state of operations), ways (the effects created to achieve the ends), means (tools/resources used to achieve the ends) and risk (amount of uncertainty/vulnerability commanders are willing to accept) and combining them with operational level effects for the purpose of determining what will be accomplished within that domain's battlespace (*AFDD 2*, 2007). In other words, there are unique characteristics, as a function of operating within a domain that commanders must consider when conducting operational planning. For instance, when developing campaign or contingency plans for operations within the air domain, commanders must understand and account for factors of air space, borders, weather and time, as they affect their ability to operate and accomplish the mission. Commanders must consider that there are international rules of airspace which principally state that a country owns the

airspace above it as dictated by its borders and will likely require flight plans to be filed for flight into that airspace and diplomatic clearance will need to be received in the case of military operations flown over/through that airspace; effectively creating borders in what was once considered a domain of free movement. This may or may not prevent certain types of air missions, the ways and means for achieving an objective, depending on if a country or countries do not allow use of their airspace. Additionally, the concept of airspace as a form of three dimensional terrain, with relationship to ground terrain, must be understood for planning purposes to de-conflict flight routes/patterns for safety of flight and ensure precise loiter and air refueling locations as keys components to mission accomplishment. The concept of "air terrain" can be seen in the attached United Airlines flight route map (Figure 6) showing flight routes de-conflicted in terms of altitude, longitude and latitude:

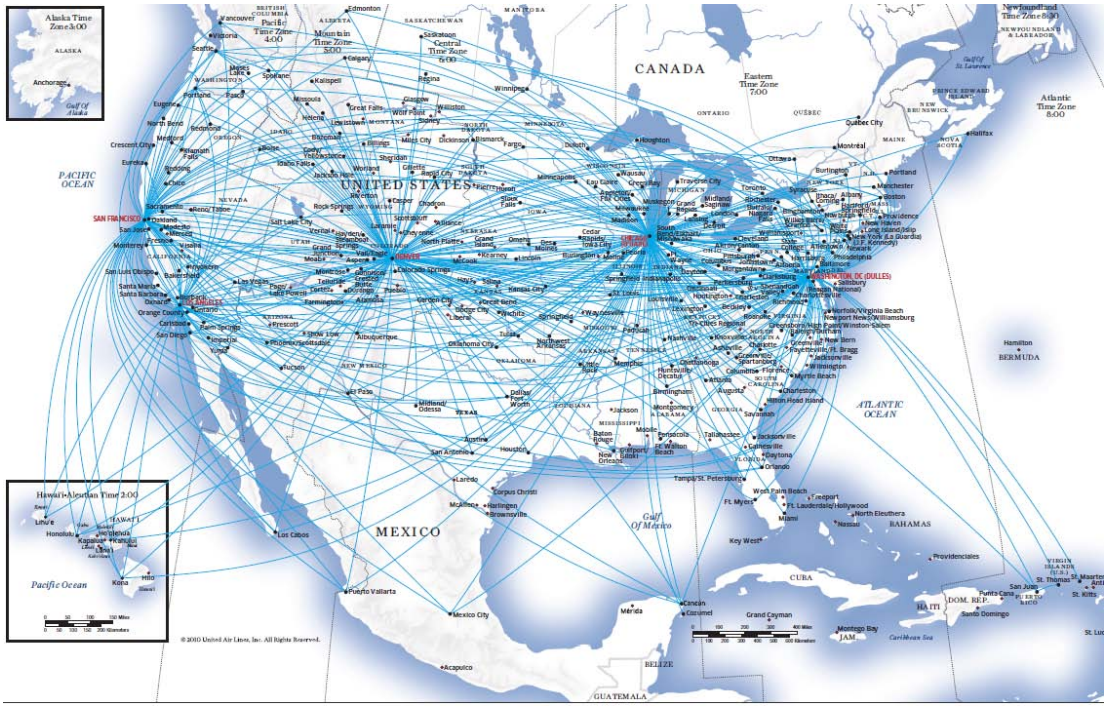


Figure 6: United Airlines Flight Route Map (United, 2010)

Weather or celestial factors also affect a commander's planning for air operations as certain types of missions/aircraft cannot succeed in inclement weather or certain celestial conditions. Too much moonlight, for example, brings increased risk of detection for certain types of special operations air missions and those missions will typically not be flown at times of high moonlight. Conversely, there is also an element of time with respect to reach associated with operating in the air domain.

> *Because of its independence of surface limitations and its superior speed the airplane is the offensive weapon par excellence.*
>
> *General Giulio Douhet*

Primarily that airpower can provide effects against a target (ends) in a much faster method (means) than possibly sea or land power and therefore can lead to far superior objective accomplishment in terms of speed or time; a pace much quicker than land or sea forces may be able to mass, maneuver and attack; a belief portrayed, to the dismay of many, by early airpower visionary Billy Mitchell when publicly advocating that strategic airpower would dominate the future of warfare. He believed, after witnessing the trench warfare of WWI, that airpower would provide a quicker way to wage war as it could swiftly strike at an enemy's vital centers affecting the hearts and minds of the enemy. It was for this reason, consequently, that he also advocated for a separate air service as he believed the Army and Navy to be too traditional (surface oriented) and would not recognize the strategic capabilities inherent in the air domain.

The advent of air power, which can go straight to the vital centers and either neutralize or destroy them, has put a completely new complexion on the old system of making war. It is now realized that the hostile main army in the field is a false objective, and the real objectives are the vital centers.

Brigadier General William 'Billy' Mitchell

There are some interesting parallels between the environmental factors affecting a commander's operational artisanship within the air domain and the cyberspace domain. The factor of terrain within the cyberspace domain, while not three dimensional based on altitude, longitude or latitude, is one based on a vast web of telecommunications and computer infrastructures that also provides global routing paths determining usable terrain much like the flight paths shown in the United Airlines flight route map shown above; many different routes to get from location A to location B within the domain. Compare the United Airlines route map and this UUNET network map below (Figure 7) and see how they resemble one another graphically.

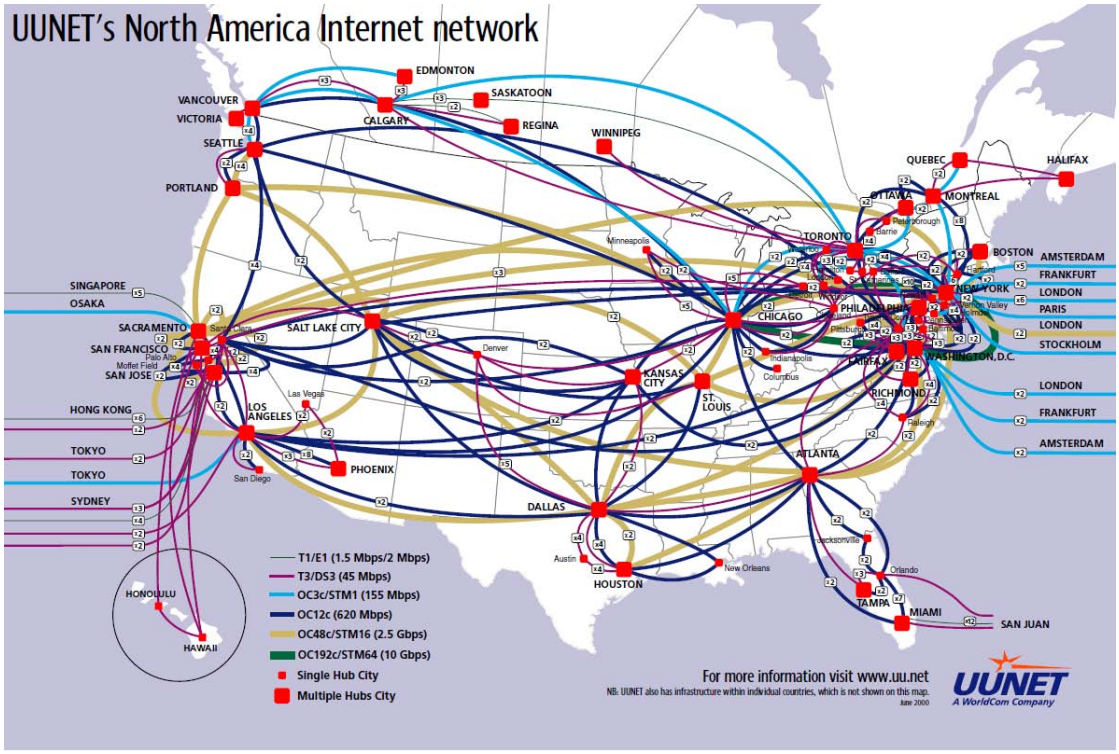


Figure 7: UUNET North America Internet Network Map (UUNET, 2000)

UUNET is one of largest fiber optic networks, if not the largest, carrying over 50% of all Internet traffic (Webcore, 2010). The graphical representation of these routes illustrates a similar terrain picture for both the air and cyberspace domains; the constrained operational space that both must understand and plan for in order to execute their mission with success. There is an obvious difference in that air routes are procedural in that they are agreed upon and can change quickly out of necessity while the UUNET fiber network is a constructed infrastructure making change difficult. However, like air, the cyberspace terrain can be quickly changed (reconfigured in a time of need) using technologies such as satellite and wireless. Additionally, like airspace over flight issues in the air domain that can halt air operations before they begin, commanders in the cyberspace domain are faced with a similar situation. Network infrastructure and

equipment residing in other countries might be viewed as "off limits" for military operations without consent of that country, making the cyberspace domain "over flight" constrained much like airspace. Furthermore, cyberspace also includes commercially owned infrastructure making the "over flight" concerns increasingly complicated from a legal standpoint. As no one really "owns" air other than the arbitrary vertical borders that have been drawn to protect a nation's sovereignty in the name of air space, the infrastructure and equipment that makes up the cyberspace domain is in fact "owned" and operated by someone, often a private/public company with no ties to government. Thus garnering approval and providing operational effects in support of strategic objectives within this domain is increasingly more complicated from that of the air domain.

Much like the air domain's advantage over sea and land in providing effects upon enemy's vital centers with speed and reach, the cyberspace domain also benefits from this time factor. Cyberspace enables the delivery of rapid effects, much quicker than the air domain in fact, with near global reach--assuming an enemy's vital centers have the telecommunication and computer network infrastructure required to provide the domain. In fact, much of what has been said about air power's ability to provide quick and flexible global reach can also be said about operations within the cyberspace domain.

> *As the aeroplane is the most mobile weapon we possess, it is destined to become the dominant offensive arm of the future.*
>
> *Major General J. F. C. Fuller, British Army*

> *The future of our nation is forever bound up in the development of Air Power.*
>
> *Colonel William 'Billy' Mitchell*

While the air domain is strategic in nature and therefore the most similar to cyberspace (barring space), the need is present for further research of all domains for parallels in operations. The purpose of proving insight into the environmental factors that affect the operational art within the air domain for comparison to the cyberspace domain is to provide a better grasp of the cyberspace domain as a true warfighting domain. The cyberspace domain has a physical environment in which it resides, encompassing unique physical parameters and sciences to define its existence and its exploitation just as the land, air, sea and space domains. Additionally, through the evolution of this exploitation, the necessity for unfettered access has become a goal of military strategy and a risk to national security. Because of this, cyberspace has become a warfighting domain, not unlike the others, with unique characteristics that may influence the ends, ways, means and risk factors that commanders use in planning for operational effects within battlespace. It is by all definition a warfighting domain through which an understanding of military operations must be spawned, nurtured and evolved.

III. Military Operations in a Warfighting Domain

Understanding the Battlefield

Once an understanding of what the domain is and what it looks like is had, one can begin to compare domains for the purpose of recognizing how to conduct military operations. This research will parallel operations (primarily offensive, defensive and security) for the land, air and cyberspace domains and determine if current "defensive operations" conducted in cyberspace are in fact defensive operations as defined in land and air or if they resemble some other type of operations (security). While it has virtual objects within it, cyberspace is seen as a physical environment not unlike land, air, sea and space. Determined by its unique physical attribute of electronics and the electromagnetic spectrum, operations within the other warfighting domains can provide historical perspectives and insight as to how we may choose fight within the new warfighting domain of cyberspace. The cyberspace domain provides some challenges as the technology exploiting this environment changes quickly (computer technology seems to advance almost daily while the B-52 has been in service since 1955). However, for the sake of making progress toward military objectives, the domain can be narrowed down to a subsections of the cyberspace warfighting domain, for example: the NIPRNET/SIPRNET portions of the DoD GIG (from the Internet facing routers inward) for defensive operations and the whole of the Internet for offensive operations. By doing this, a battlefield (not unlike that of land or air) is seen--one in which forces must learn operate and leadership focus must be shifted for the purpose of fighting and winning within that domain, Network Warfare (NW) in this case. Variations over time of the

military utility and requirement for fighting within the cyberspace domain will lead to multiple functions of offensive and defensive NW operations much like the operational functions of strategic attack, airlift and counterair the Air Force uses for the purpose of achieving specific effects through the air and space domains in direct support of desired military objectives (*AFDD 1*, 2003). To get there however, we must first understand the underlying principles of military operations (more precisely, what are offensive and defensive operations) and then attempt to apply them to the cyberspace battlefield and NW operations.

Army Field Manual 3-0: Operations in the Land Domain

Army Field Manual 3-0, Operations, is a great place to gain a perspective of military operations as formulated for the land domain. The Army's operational concept of full spectrum operations outlines how the service will conduct itself during conflict. It combines offensive, defensive and stability or civil support operations simultaneously in an attempt to seize, retain and exploit the initiative (setting or dictating the terms of action throughout an operation) within the land domain, as shown in Figure 8. Operational initiative is something all ground commanders aim to seize, retain and exploit in an attempt to achieve decisive results (*FM 3-0*, 2008).

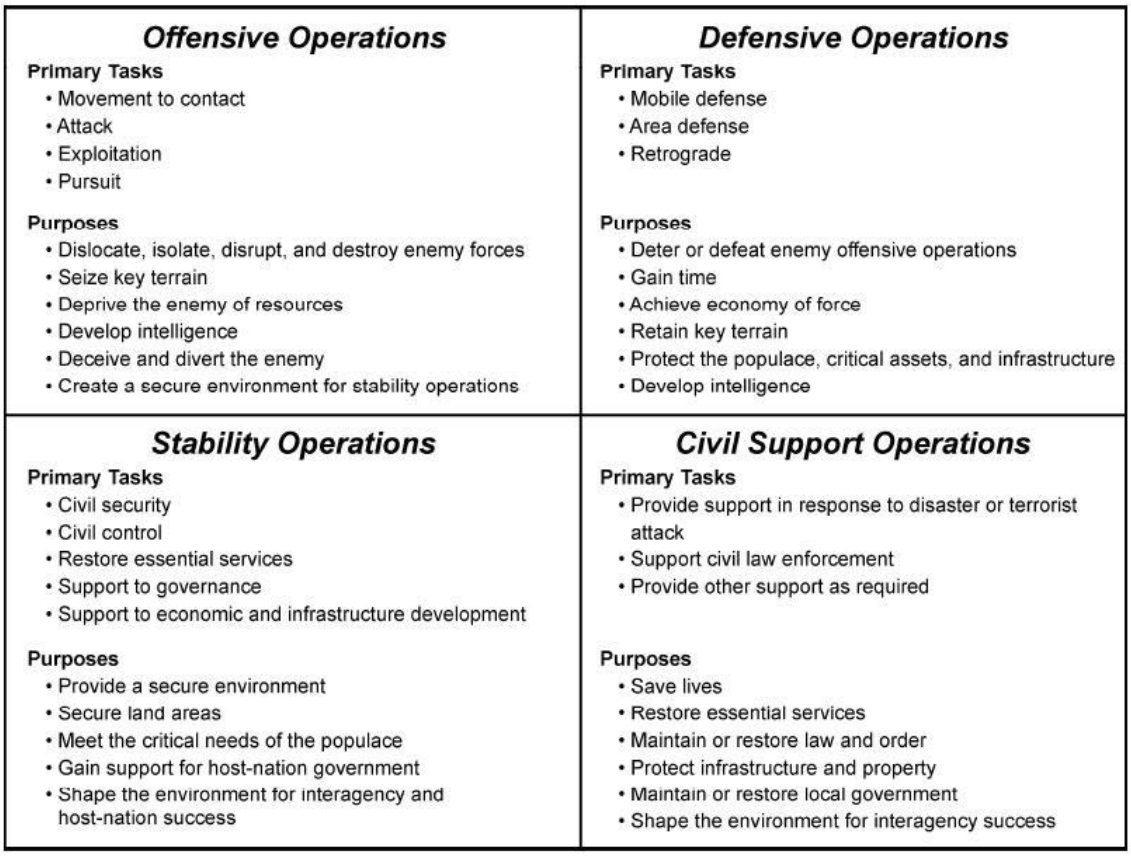


Figure 8: Army Field Manuel 3-0 Operations Matrix (HQ Dept of the Army, 2008)

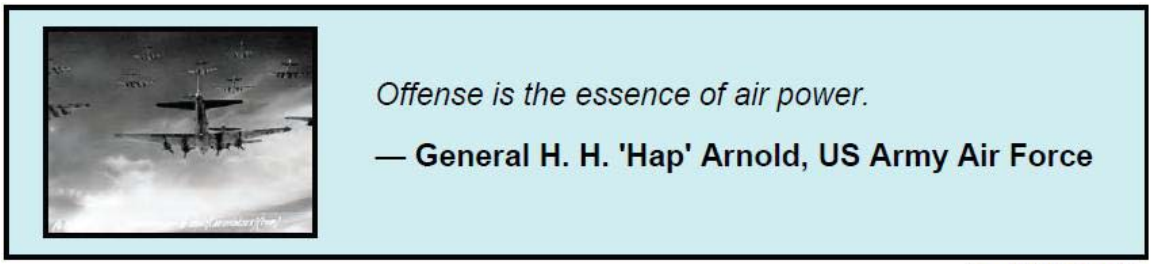
The Army employs offensive and defensive operations to defeat the enemy in the land environment while employing stability or civil support operations to interact with the populace and civil authorities for the purpose of improving civil conditions while applying combat power to prevent any situation from deteriorating. Offense is defined as taking the fight to the enemy by overwhelming their capabilities, disrupting their defenses and ensuring their defeat. Defensive operations are conducted to defeat an enemy attack and create the conditions for a counteroffensive operation, allowing forces to regain the initiative.

On the surface, the principles of military operations outlined in Army doctrine seem transferable to the current operational construct we see within the DoD for NW operations within the cyberspace domain. Computer Network Attack (CNA) is used independently or in conjunction with other offensive operations with the purpose of taking the fight to the enemy much in the same manner as offensive operations are defined for land. While there are no formal terms associated with the cooperation with civil authorities and concern for civil conditions within the NW realm (e.g. stability and civil support operations), there are vast protections in place in the form of coordination layers (military and civilian), legal reviews and limited operating authorities to ensure the same result; promoting social well-being and public safety for the purpose of maintaining the initiative in operations. Computer Network Defense (CND) however, is not currently conducted in the same approach the as defensive operations defined in *FM 3-0*. Instead, CND resembles a subsection of defensive operations (passive defenses or security) more than the fluid maneuvering of defensive forces outlined above; manipulating from defensive posture to counterattacking in a semi-offensive maneuver for the purpose of seizing the initiative. Security or passive defensive measures are only a portion of the defensive operations required to ensure the Army's operational initiative within land operations.

Air Force Doctrine Document 1: Operations in the Air Domain

The above discussion provided a brief overview of the Army's doctrinal definition of military operations within the land warfighting domain and some brief insight to how that might apply to operations within cyberspace. However, another

perspective on military operations from the point of view of fighting within a different domain may be useful in gaining a broader definition of military operations as not all domains are the same. The USAF, as outlined in *AFDD 1*, defines air and space forces as inherently offensive in nature: "control of air and space is offensive in execution … even highly successful defensive air campaigns such as the World War II Battle of Britain were based upon selective offensive engagements" (*AFDD 1*, 2003).



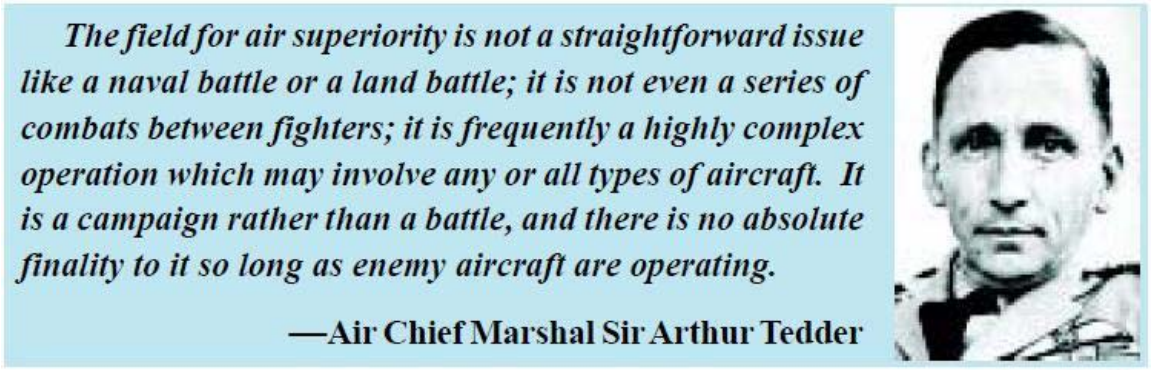
from AFDD 2-1.1, pg 18

The Air Force defines offense as an action rather than to reaction for the purpose of seizing, retaining and exploiting the initiative; a definition much in the same light as that of the Army and one that correlates well to current offensive operations within the cyberspace domain. That said, the Air Force, through its definition of operational functions (counterair specifically) has given a glimpse into its ideal for defense within these subsections of the air domain. Operational functions are defined in *AFDD 1* for the purpose of describing operational constructs that can be used to achieve military goals and those focused on utilizing the air domain (aircraft) are listed in Figure 9.

- Strategic Attack
- Airlift
- Air Refueling
- Special Ops
- Combat Search & Rescue
- Counterair
- Counterland
- Countersea
- Intelligence, Surveillance and Reconnaissance

Figure 9: *AFDD 1* Operational Functions (Air Domain Focused)

The operations function of counterair, by definition, is "operations to attain and maintain a desired degree of air superiority by the destruction, degradation or disruption of enemy forces" and is split into two sub-functions, offensive and defensive counterair. It is recommended that both offensive and defensive efforts be controlled together as one continuum of operations for the purpose of economies of force and concentrations of effort as opposed to completely separate stovepipes of offense and defense. Offensive counterair operations entail hunting and killing enemy air power near its source when and



from AFDD 1, pg 42

where the USAF chooses while defensive counterair operations encompass the "detection, identification, interception and destruction of attacking enemy air and missiles", generally in or around friendly territory (*AFDD 1*, 2003). Defensive counterair, according to *AFDD 1*, is what the Air Force outlines as its doctrinal air defense definition and encompasses a full range of defensive operations from passive to active; part of which, the passive portion, can be seen in the service's focused understanding of security centered on the ideas of force protection, staying beyond enemy's reach and defeating enemy intrusion to reduce vulnerabilities to friendly forces. With this understanding, the Air Force and the Army are not that far off on their doctrinal

understandings of defense and security as well. And as such, our approach to CND continues to resemble passive defenses or security more than the fluid maneuvering of defensive forces outlined for both the air and land domains, as shown in Figure 10 (this personal view of current cyberspace operations will be supported in subsequent sections).

	Air Air Force (AFDD 1)	Land Army (FM 3-0)	Cyberspace Current operating status
Offensive Ops	Offensive action is to seize, retain, and exploit the initiative. Offensive is to act rather than react and dictates the time, place, purpose, scope, intensity, and pace of operations.	Combat operations conducted to defeat and destroy enemy forces and seize terrain, resources, and population centers.	**Yes, primarily in support of kinetic ops.**
Defensive Ops	Detection, identification, interception, and destruction of attacking enemy air and missiles and normally takes place over or close to friendly territory.	Combat operations conducted to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations	**No, minimal active defense at best.**
Security	Friendly forces and their operations must be protected from enemy action that could provide the enemy with unexpected advantage. This principle also enhances our freedom of action by reducing the vulnerability of friendly forces.	Protection: tasks and systems that preserve the force so the commander can apply maximum combat power. Protection determines the degree to which potential threats can disrupt operations and counters or mitigates those threats.	**Yes, primary form of current NetD posture.**

Figure 10: Air, Land and Cyberspace Operations Comparison Matrix

Defense vs. Security

To posture our CND efforts for increased integration in full spectrum operations with respect to NW, we must first understand the true definition of military defense as opposed to confusing or interchanging it with the definition of security. As of today, the term defense with respect to NW operations is generally used when in reality, the technologies, TTPs and organizational structures are predominantly geared toward security. Successful defensive operations, as outlined in *FM 3-0* and *AFDD 1*, have

distinctive characteristics that set them apart from security and make them vital to the spectrum of operations. For example:

- Destroy as much of the attacking enemy as possible
- Are aggressive
- Are flexible
- Transition to offense at every opportunity

These characteristics highlight the primary differences between defense and security. Defensive forces are active maneuver forces, with maneuver being defined as "the employment of forces in the operational area through movement in combination with fires to achieve a position of advantage in respect to the enemy" in *Joint Publication 3-0 Operations* (*JP 3-0*, 2010). Thus active defense operations require dedicated forces to find, fix, engage and defeat adversarial attacks with the focus resting on their ability to actively maneuver within the battle space for this purpose.

Conversely, security:

> "enhances force protection by identifying and reducing friendly vulnerability to hostile acts, influence, or surprise. Physical security includes physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. Functions in physical security include facility security, law enforcement, guard and patrol operations, special land and maritime security areas, and other physical security operations like military working dog operations or emergency and disaster response support. Measures include fencing and perimeter stand-off space, land or maritime force patrols, lighting and sensors, vehicle barriers, blast protection, intrusion detection systems and electronic surveillance, and access control devices and systems." (*JP 3-0, 2010*)

Security is a first-line passive defensive measure employed throughout the force for the purpose of deterring adversarial offensive operations. Ideally, security efforts will eliminate lower-level adversarial attacks allowing defensive maneuver forces to focus on the more advanced, larger scale threats that bypass security measures. Security is a subset of defense supporting the continuum of operations. Defense on the other is emulated through force projection by maneuver forces within the continuum of operations which can quickly shift from defensive to offensive operations for the sake of gaining and maintaining the operational initiative, as shown in Figure 11. Forces conduct defensive operations not solely for the purpose of protecting themselves from adversarial attack, but also to create the conditions for a counteroffensive operation (possibly utilizing the same forces for both the defensive and offensive ends of the continuum), and are therefore are fundamentally different than security.

Figure 11: Continuum of Operations

IV. Air Force Perspective, NetOps vs. NW Ops

AF Mission

Once operations within warfighting domains have been defined, a service can then take those overarching definitions and utilize them as a possible framework for specific operations within a specific domain. The Air Force, in December 2005, deemed cyberspace as a warfighting domain in parallel with its existing domains of Air and Space. In a joint letter to Airman, then Air Force Secretary Michael W. Wynne and Chief of Staff General T. Michael Moseley stated that "Our mission is our guiding compass" and outlined this mission statement as:

"The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests – to fly and fight in Air, Space and Cyberspace."

This 2005 mission statement, for the first time, focused the concept of cyberspace outside the traditional support role it had played for years (and continues to) in the Air Force's ability to take the fight to its adversaries. It shifted, even if no more than in word only, the focus of senior leaders toward this new warfighting domain which was now portrayed at the same level of significance as domains of air and space--a domain in which we as a service must be able to "fly and fight". Air Force leaders realized the service must excel within the cyberspace domain to maintain a competitive advantage and ensure its relevancy as a fighting force in support of national military objectives in this new era of modern warfare; much as has been done in air and space before. As a result, Air Force

leaders and Airmen alike, across the service were asking the question, "How do we fly, and fight in cyberspace?" As it should have been, this evolution in mission was taken head on by some, and this new cyberspace push was evident through such actions as the establishment of the 67th Network Warfare Wing for the purpose of executing network operations, defense, attack and exploitation to create cyberspace effects and the re-designation of the Air Force Information Warfare Center to the Air Force Information Operations Center to better reflect the center's increased focus on network warfare through Tactic, Technique and Procedure (TTP) development, Operational Testing and Vulnerability Assessments. The Air Force Mission statement was later changed in August 2008 under new Air Force Secretary Michael Donley and Air Force Chief of Staff General Norton Schwartz to read:

"The mission of the United States Air Force if to fly, fight and win in Air, Space and Cyberspace."

This new mission statement was key in two aspects. First, it made the mission statement "simple and easy to understand" as noted by Gen Schwartz in an Aug 2008 speech at Bolling AFB. Second, it added the term "win". No longer was it accepted verbiage to AF leadership to just be competitive and relevant in air, space and cyberspace--instead the service was making a committed effort to say it will win in those domains as well. This is not really a far stretch in the air and space domains, but cyberspace still remains a big question.

As time has gone on there have been discussions and planning for a new cyberspace command which have come and gone, ultimately resulting in the standup of a

new cyber Numbered Air Force (24 AF) for execution within this warfighting domain while additionally placing the cyberspace mission on par with the space domain within Space Command (the Space of the Air, Space and Cyberspace in the mission statement) for Major Command advocacy. New/modified enlisted and officer career fields with cyberspace emphasis have been developed and implemented. Additionally, various cyber focused training programs, whether they be modules to be taught at Basic Military Training and Reserve Officer Training Corps and Officer Training School or full training tracks at the Service Academy, Cyber Tech Schools or Professional Military Education, have been or are being developed. All of this time, effort, money and posturing conveys one clear message if nothing else: the cyberspace mission is here to stay for the foreseeable future, and the Air Force must continue this evolution toward ensuring a competitive advantage in this domain.

Of course now that evolution has begun, what does it mean? How does one "fly, fight and win" in cyberspace? What are the pertinent missions resident within the domain and how do one assure their success? In this relatively new warfighting domain a foundation has been set, as stated above, albeit with a limited understanding of the domain with respect to what the domain really is, its defining parameters and who or what falls within the domain. Despite these difficulties with definition, the Air Force continues to move forward, although maybe not as fast as one may like, with identifying organizational change chartered with tackling this domain. One fact has become apparent as the service has attempted to answer some of these questions: It is certain that NW Operations (NW Ops) defined as "the integrated planning, employment and

assessment of military capabilities to achieve desired effects across the interconnected analog and digital network portion of the battlespace" (AFDD 2-5, 2005) will be a primary mission of the Air Force's cyberspace domain efforts. The threat facing warfighting capability in terms of NW, if left unchecked, would be paramount as the Air Force in the era of modern warfare seen today has become largely net-centric and if a competitive advantage is not had in this area, it could be catastrophic not only for fighting within the cyberspace domain, but within the other domains as well (air and space). As a result, the service must continue moving toward operationalizing our NW capabilities while continually shaping the cyberspace equation.

Threat to AF Mission

It can be speculated that it will take a catastrophic cyber event such as a "cyber Sept 11th" before the cyberspace warfighting domain actually receives the attention and resourcing it requires to ensure this competitive advantage. An advantage that ensures the service's ability to "fly, fight and win" in all of its warfighting domains of air, space and cyberspace while engaging in true warfare in the cyber battle space. Is there some intrinsic truth to this speculation? The service has seen over the last few years a large number of Communications Officers released from duty by the Air Force while at the same time, this career field has been identified as the primary source for transition to the 17D Cyberspace Operations Officer career field. Additionally, key cyber warfare organizations such as 24th Air Force, the 67th Network Warfare Wing and the 688th Information Operations Wing, while relatively new in some respects, continue to be drastically undermanned and underfunded. All of this sends a mixed message that while

cyberspace is deemed significant enough to add the term to the USAF mission statement the reality is that nothing easily visible and precisely catastrophic enough has happened as a result of a cyber type attack to warrant the reaction of widespread focus and resourcing seen after Sept 11th. For example, there was a sweeping push for Special Operations Forces and the long term sustainment resourcing to support which resulted in response to the shift in modern warfare which was experienced as a result of that attack-- an increase from $3.7 billion in FY 2001 to $6.5 billion in FY 2006 (Lane, 2006).

Understanding that the attacks of Sept 11th were a horrific event on U.S. soil resulting in the loss of nearly 3000 human lives, and to say a cyber attack may or may not be capable of a parallel in physical destruction and human loss is debatable, the underlying principle to this speculation is still valid. Should it take a catastrophic cyber event such as a "cyber Sept 11th" to occur before USAF cyber forces see the attention and resourcing they require to become dominant within this warfighting domain?

First, is this the right question to ask? If the Air Force and the nation have learned anything from that fateful day, it is that all must remain vigilant and proactive in searching out and destroying any and all adversaries who may be planning such attacks to avoid future tragedy. It could be argued that by the time a catastrophe on par with Sept 11th in terms of sudden and widespread disaster in this domain is experienced, it is too late. The competitive advantage at that point is lost. Shouldn't the focus be on proactive cyber practices as opposed to waiting for one defining event to force the reaction?

Secondly, catastrophic results in terms of widespread destruction or disaster may not be the primary effect desired as a result of attacks through the cyber domain; however

they may be as devastating to the Air Force's ability to support National Security objectives. The USAF Scientific Advisory Board, in their 2008 report on Defending and Operating in a Contested Cyber Domain, concluded "that if and when tensions escalate between the US and its adversaries … there is a reasonable projection of conflict behavior in which an adversary does not attempt to deny network services, but instead uses compromised mission applications and/or data to distort and confuse or control the decision-aiding process" (USAF Scientific Advisory Board, 2008). Barring full blown kinetic conflict between net-savvy nations or attack from a cyber capable terrorist organization, the Air Force may never see a cyber attack that results in large scale, sudden devastation.

That does not mean however that the Air Force and the Defense Industrial Base that supports it is not under cyber attack every day. The fact is that vital intellectual property and mission data has been and is currently lost through cyber espionage at an alarming rate. While actual cumulative numbers are hard to determine, one incident alone can prove to be a distressing blow to National Security. For example, a U.S.-China Economic and Security Review Commission's 2009 Annual Report to Congress, outlined how a 2007-2008 attack on a defense contractor allowed intruders to siphon several terabytes of data related to the design and electronics systems of the F35 Lightning II (U.S.-China Economic and Security Review Commission, 2009). For comparison's sake, 10 terabytes of data is roughly equal to the printed collection of the U.S. Library of Congress in digital form. That same report projected a total of 87,570 Incidents of Malicious Cyber Activity against the Department of Defense for 2009, up from 54,640

for 2008 while a Joint Task Force-Global Network Operations' Cyber Threat Briefing states there are approximately 120 nations with cyber warfare capability or intent, not including the vast number of terrorist groups, extremists and cyber criminals (JTF-GNO, 2009). This makes for a daunting yet critical challenge for cyber defenses to overcome as they function today.

Based on this information, it is evident that the far reaching cumulative effects of cyber espionage could foreseeably result in collective catastrophic effects on National Security far greater than that of the Sept 11th attacks if proactive measures are not taken to prevent it and ensure a competitive advantage in the cyber domain. The effects of countless dollars of research and development information essentially given away coupled with the insight provided about military advances before they are even presented as operational capabilities provides potential adversaries a significant advantage at an extremely low cost. The Air Force does not need to, nor should it, wait for a "cyber Sept 11th" before it ensures the cyberspace warfighting domain receives the attention and resources it requires as the nature of modern warfare continues to shift toward the cyber domain. The midst of that event is upon us, and future outcomes will depend on the proactive actions taken today.

"Operationalize the Network"

Faced with this realization, the Air Force over the last few years has begun its move to truly "operationalize" its networked capabilities as a result of the perceived threat and shift in mission statement briefly mentioned above. The idea or term "operationalize the network" has been around the communications community for some

time now. However, this has been more of a catchphrase for streamlining network maintenance capabilities and personnel as opposed to using the network as a function of warfighting capacity or a maneuver force with the ability to bring or deny effects in concert with other kinetic capabilities for the ultimate goal of supporting COCOM objectives.

If, however, the Air Force is to "operationalize" networks with the purpose of flying, fighting and winning in cyberspace, some distinctions need to be made with respect to how the network is perceived, utilized and managed as the phrase Network Operations (NetOps) has been used loosely and randomly across the service to describe various aspects of AF network management depending on who is using the term. Through the interchanging and misuse of this term, confusion has resulted not only among the communities reliant on networks for net-centric mission accomplishment, but within the cyber community charged with providing and operating the domain as well. What is NetOps, what are its responsibilities and how are they different than those of NW Ops? This confusion creates a fog of war or battle directly mired in an atmosphere of indecision and non-responsibility. When talking about securing the network or NetD (USAF term for CND), who owns responsibility and what authorities do they have in carrying out those missions? Conversely, who is accountable for providing the network and ensuring its availability to those reliant upon it? The confused mission space and command and control have led those within and as a result outside the cyberspace domain reeling to answer those questions. What responsibilities does a local wing commander

have to the fighting forces in cyberspace to ensure an unwarranted advantage is not given to the adversary?

By developing a common understanding of terms--i.e. doctrine--their functions and how they fall within the service's vast network management and operations missions the Air Force can begin to move past the confusion and focus mission development aimed at persecuting cyber threats service-wide (air, space and cyberspace domains collaboratively working together) while continuing to provide the agile combat support they all rely on. To do this, Network Warfare operations (NW Ops) and Network Operations (NetOps) must be defined. Are they the same? If not, how do the differences affect how the Air Force should move to apportion it cyber resources, and how does this apportionment affect its ability to ensure mission success in all domains?

NetOps Defined

The 17 April 2006 *Warfighting Integration Plan*, when defining NetOps, discusses these networks as a method to deliver the necessary infrastructure to support Decision Superiority; essentially looking at the networks as a mission enabler and force multiplier providing a robust globally interconnected network environment in which data can be shared among users and platforms (Secretary of the Air Force Office of Warfighter Integration and Chief Information Officer, 2006). It for all intents and purposes defines Air Force Networks as the underlying support platform which allows other Air Force capabilities to complete their mission and NetOps as the function through which these networks are maintained and provided in the Air Force. It is a manmade (constructed) domain that must be available at all times as to ensure the Air Force's

warfighting proficiency. There is an enormous task when realizing the scope of the necessary network infrastructure requirement to support a 300K+ person fighting force coupled with the requirement to provide this domain anywhere in the world. The thousands of pieces of network equipment (routers, switches, encryption devices, servers, patch panels, etc.) to the multitude of circuits maintained to provide worldwide communication to the countless servers, desktops and laptops used daily must be maintained in operational status to make this network support possible. Maintenance personnel must keep these networks functioning at a high fully mission capable (FMC) rate, to use an air operations term, to ensure any hope at a competitive advantage in any Air Force warfighting domain in this ever increasing net-centric atmosphere. This mission enabling capability is the underlying focus behind the term NetOps as defined in the 17 April 2006 *Warfighting Integration Plan*. This document defines NetOps as the AF subset of the DoD Global Information Grid (GIG), including everything except information content, operations support and **warfighter application**. It states that the underlying goal of NetOps is to promote net-centricity allowing the AF to transform itself to meet the DoD vision of net-centric operations and warfare. It is through this definition and specifically the exclusion of **warfighter application** where the distinction between NetOps and NW Ops lies.

NW Ops Defined

AFDD 2-5, Information Operations, defines NW Ops as the integration of network attack (NetA), network defense (NetD) and network warfare support (NS) to ensure forces operate in a protected information environment, allowing other Air Force

capabilities (air and space) to operate in an uninterrupted fashion. *AFDD 2-5* continues to discuss that NW Ops can also be used to independently or in conjunction with other operations to create effects upon an adversary. Specifically, NetA is the employment of network-based capabilities to destroy, corrupt or usurp information resident in or transiting the network. NetD is the employment of network-based capabilities to defend friendly information resident in or transiting through networks against adversary efforts to destroy, disrupt, corrupt or usurp it. *AFDD 2-5* states that NetD actions include analyzing network activity to determine the appropriate course of action to protect, detect and react to internal and external threats to Air Force networks. This definition implies a continuous monitoring and movement on the net to detect react and counter act adversary attack and movement on Air Force networks, while NS is the support necessary to complete NetA and NetD operations (primarily intelligence) (*AFDD 2-5*, 2005). NW Ops is deeply rooted in warfighter application and focused on the idea of maneuver forces operating on the network to engage the adversary.

NW Ops Supported and NetOps Supporting

Based on the doctrinal definitions outlined above, NW Ops is in essence the operational movement of forces on the network (cyberspace domain) provided by NetOps for the purpose of either offensive, defensive or battle space preparation operations. NW Ops, like air and space operations, can be integrated with the other warfighting capabilities for the purpose of providing effects to the combatant commander as opposed to NetOps which is not focused on warfighting effects, but rather providing support to or enabling capabilities. In this sense, NW Ops is supported by and reliant on NetOps as an

agile combat support function in the same way as air and space personnel for projecting warfighting capability (a caveat being possible NetA operations that may or may not take place on AF networks), as shown in Figure 12. So to simplify the discussion using terms those in the Air Force are traditionally familiar with, NW Ops can be seen as the pilot (operator) charged with flying, fighting and winning in cyberspace so that others may realize freedom of movement in utilizing the domain while NetOps is the maintenance function charged with providing (ensuring Fully Mission Capable (FMC)) the tools, and in this case the domain, operators in all domains need to operate; ideally, this is no different than the B-2 maintenance crews charged with ensuring that aircrews have FMC aircraft to execute their Global Strike mission.

Figure 12: Supported vs. Supporting

Mission Distinction

Unfortunately, there is overlap between the definitions outlined above which help to exacerbate the misunderstanding between NW Ops and NetOps mission characterization, specifically when discussing NetD. Under *AFDD 2-5*'s definition of NW Ops, it is stated that the mission of NW is to ensure forces operate in a protected information environment, allowing other Air Force capabilities (air and space) to operate in an uninterrupted fashion (*AFDD 2-5*, 2005). On the surface, this would seem no different than the enabling function garnered by NetOps. However, the difference lies in

the underlying methods by which they both seek to ensure this protected information environment, probably a small, and often blurred distinction, but one nonetheless. NetOps, as an enabling function, attempts to secure its enabling network capabilities in support of mission assurance (whatever mission it is supporting at the time) and operational requirements through Information Assurance controls (see Figure 13).

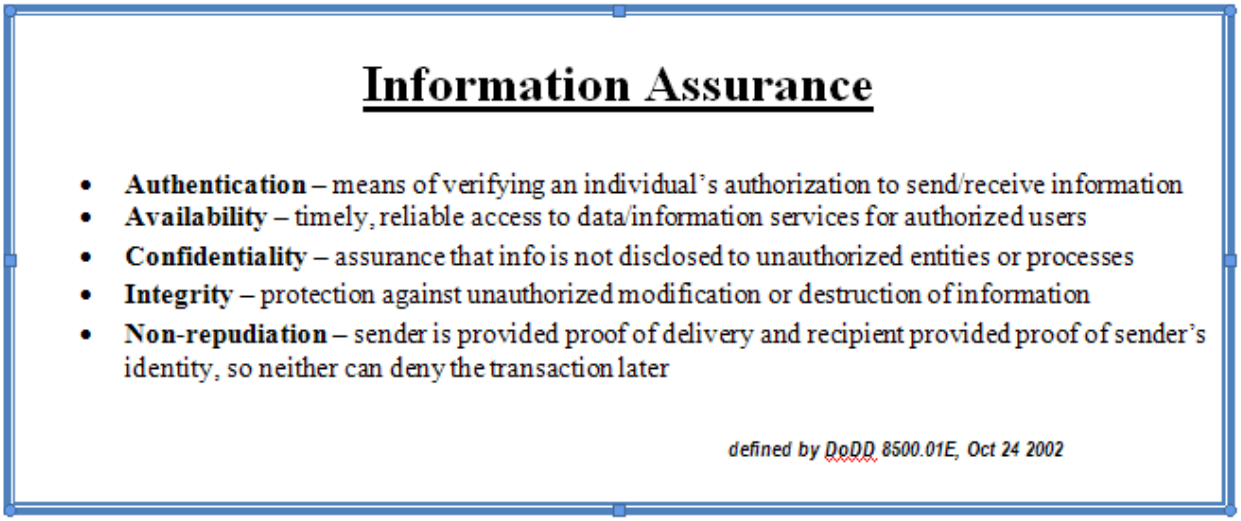


Figure 13: Information Assurance (DoDD 8500.01E, 2002)

That is, it seeks to ensure the domain through focused efforts to ensure that the information passed across the network is available and authentic while maintaining its confidentiality, integrity, and the ability for non-repudiation. NetOps primarily executes these protective measures through their maintenance actions (i.e. downward directed network patching or configuration changes) or new equipment/technology installations. However, ultimately the primary mission of the NetOps community remains providing network capability to the operator and often times, the two (network security and desires of the operator) conflict as security usually comes at some cost to the operator in terms of usability. The USAF Scientific Advisory Board (2008) stated "it is clear that Information

Assurance is a necessary element or measure or defending cyberspace, but it is equally clear that it is insufficient. There is a need for a more broad-based perspective, if effective defense against disruptive cyber attacks is to be achieved." The reality is that IA, and through its use NetOps, provide a mode of passive basic security as a subsection of what should be a defense in depth network posture; much in the way the gate, fencing and identification cards present these functions around any Air Force installation, keeping the lower level threat neutralized while allowing trained defenders to find, fix, track, target and engage the more technically proficient or persistent threats (see Figure 14). Additionally, it is noteworthy that many network configuration changes and patches originate as NetD tactics directed by NW Ops units for NetOps implementation.

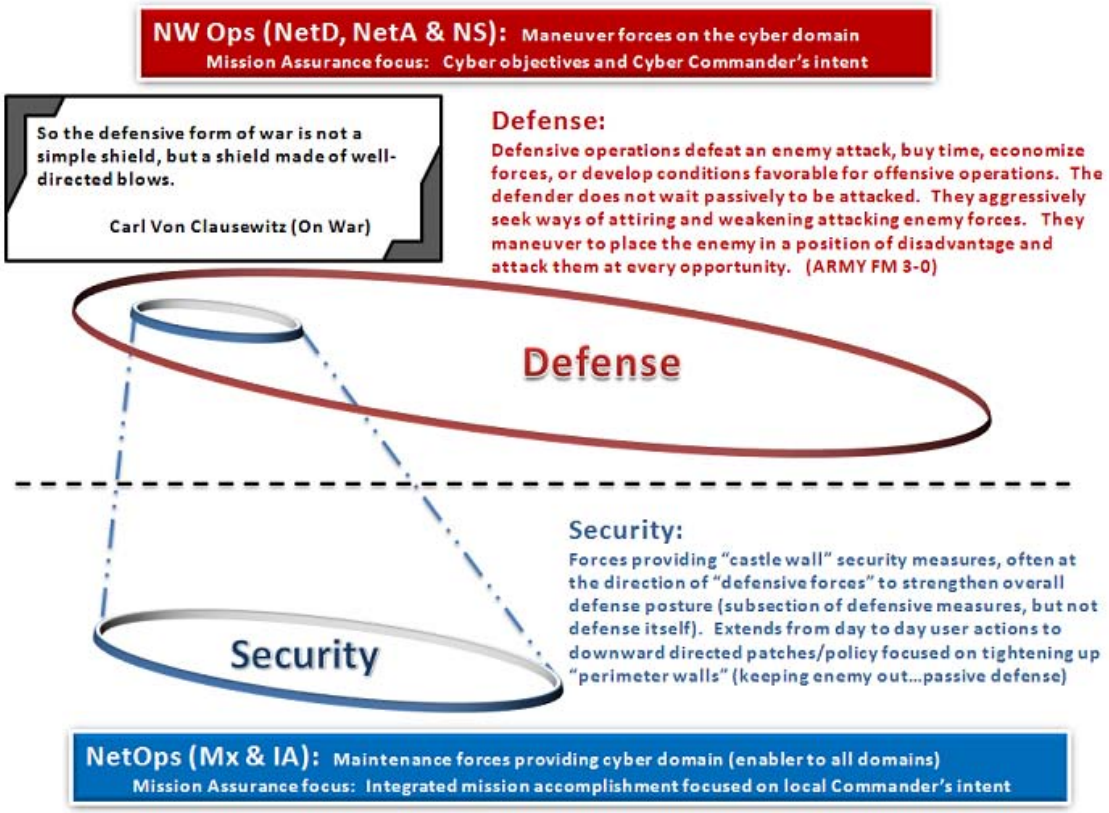


Figure 14: Defense vs. Security

NW Ops, and in this case primarily NetD forces, also attempt to provide this protected environment as defined in *AFDD 2-5,* however their focus is primarily on adversarial threat to networks, continuous monitoring of network sensors and maneuver on the network to detect, react and counteract to adversary attack/movement on Air Force networks. NetD operators often determine and downward direct network security postures for NetOps maintainers to execute as a fortification of first line security measures while inversely, when anomalies are detected at the security parameters, NetOps forces often report them to NW Ops forces for further action. While these are two distinct mission areas within the domain, the necessity for integration is present as with operations in other domains. NW Ops' primary mission focus is on the defense of networks, not necessarily desires and wishes of other operators (air and space) using the network as an enabling function to complete their mission. The reality is that Air Force networks must reside somewhere in the middle in terms of defending the networks while doing so in such a fashion where they still enable the users to accomplish their missions.

As outlined above, the preponderance of network forces fall into two clear mission paths. Operations (NW Ops) and Maintenance (NetOps) and find themselves on different ends of the network defense operations continuum in terms of how they provide for NetD, see Figure 15. One using IA measures predominantly as a focused passive security effort (NetOps) while the other focuses on active defense through maneuver and employment of forces (NW Ops) focused on adversarial threat. While the underlying knowledge of baseline technology used to operate within the domain (in this case Internet Protocol (IP) networks) is the same, the required depth of understanding of that

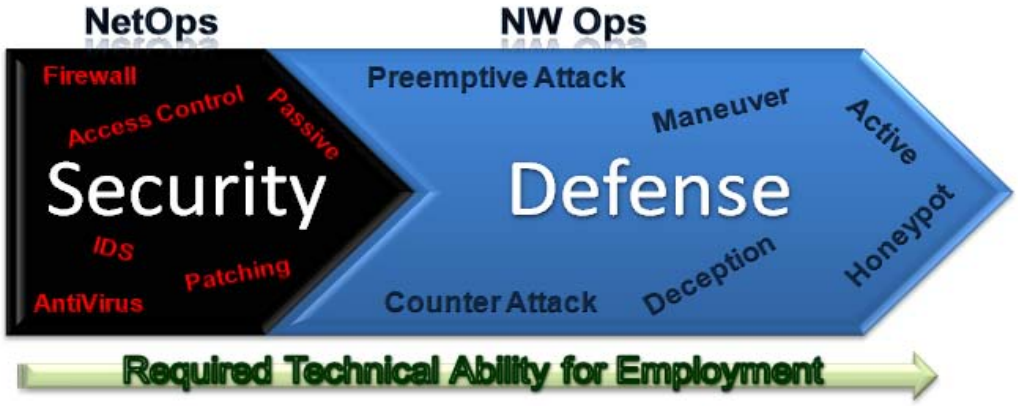


Figure 15: Defensive Operations Continuum

technology coupled with the vast differing mission employment focus related to each result in what can only be described as two completely separate mission areas, maintenance/sustainment (NetOps) and operations (NW Ops) whom share the same domain and at times may converge for the purpose of providing a tiered network defense continuum within the cyberspace domain battle space.

V. Air Analogy

Operational Function, Mission Focus

As the distinction between operations/defense (NW Ops) and maintenance/security (NetOps) has been made in the two preceding chapters, an interesting parallel (or lack thereof) can be made with relation to how the Air Force has proceeded with operations in the cyberspace domain as opposed to its more historical domain of air.

The air domain, as defined in *AFDD 2-1.1, Counterair Operations*, is "the area beginning at the Earth's surface, where the atmosphere has a major effect on the movement, maneuver and employment of joint forces"; it is a warfighting domain which resides within a physically definable environment (*AFDD 2-1.1*, 2008). There are many different technologies or weapon systems--aircraft, missiles, etc--that take advantage of this domain for the overall goal of national security. As stated previously in this document, cyberspace, like air, consists of the shaping principles which define it as a warfighting domain. Because of this, the IP network can be looked at as being analogous to the airplane, a technology or weapon system for exploiting the cyberspace domain as defined by being within the cyberspace environment and utilizing the physical properties of that environment; electronics and the electromagnetic spectrum. Much in the same way that airplanes are not the only weapon system utilizing the air environment, IP networks are not the only system within cyberspace. So the focus will be on the comparison of the airplane and its use within the air domain to that of the network and its use within the cyberspace domain. While the principles of flight are pretty much the

same--lift versus weight and thrust versus drag--vast improvements and modifications on this science have occurred since the December 17, 1903 Wright Brothers exploits at Kitty Hawk, North Carolina (Smithsonian, 2010). This ultimately lead to the array of operational uses for aircraft described in *AFDD 1*'s Operational Functions, used by the service to execute national security objectives within the air domain. Only those operational uses, of the 17 Operational Functions within *AFDD 1*, primarily using aircraft for mission accomplishment were outlined in Figure 16:

- Strategic Attack
- Airlift
- Air Refueling
- Special Ops
- Combat Search & Rescue
- Counterair
- Counterland
- Countersea
- Intelligence, Surveillance and Reconnaissance

Figure 16: *AFDD 1* Operational Functions (Air Domain Focused)

These functions all use the domain for individual mission accomplishment, however not all are responsible for operations focused on securing freedom of movement, the ability to fly, fight and win, within the domain. Likewise, there are multiple operational uses for the network which utilize it for mission accomplishment but are not definitively responsible for its ultimate defense, Figure 17 for examples:

- NW Ops
- Ops Planning
- Acquisitions
- Personnel
- Admin
- Logistics
- Communications
- Finance
- Intelligence, Surveillance and Reconnaissance

Figure 17: Network Operational Functions (Examples)

Notice that the NetOps mission is not included in this list of network operational uses because NetOps, like combat support which was not listed above (yet is one of the 17 Operational Functions of Air and Space), is not reliant on the network for mission accomplishment. It ensures sustainment of the network for use by those whom are reliant upon it, much like combat support is "the essential capabilities, functions, activities and tasks necessary to create and sustain air and space forces" (AFDD1, 2003). In reality, while NetOps does represent a means used for ensuring mission accomplishment through their maintenance actions and security measures (IA), they do not "fly" missions on the network in the same way counterair force maneuver air; they are providing the network for those whom need it for mission accomplishment; NetOps is combat support. Conversely, NW Ops are operational forces not unlike that of the flying corps in the air domain; maneuvering the battle space as an operational user of the domain.

Operator vs. Combat Support Focus (Personnel Perspective)

Once the difference in mission is understood, an interesting difference in how operational missions are organized as opposed to combat support should be discussed. The various operational functions or missions within the air domain above require uniquely skilled and technically sound personnel operating within their specific operational realm in order to ensure their distinctive mission is accomplished. For example, the skills required to complete KC-135R Stratotanker aerial refueling missions at altitude are completely different than those required to fly F-22 Raptor air superiority missions. The basics tenets of flight and airmanship are the same; however the TTPs are vastly different as are the technical parameters which surround each aircraft. The KC-

135 and F-22 will at times integrate with each other for the purpose of completing a task, but, they have different mission objectives within the air domain and varied mechanisms for ensuring success of those missions. The service has recognized the need to foster these specialized operational mission sets in order excel in the air domain and does so through the organization of its operational force; one example being seen in the variations of the pilot Air Force Specialty Code (AFSC) (although there are many operational AFSC's operating within the air domain). All have the same baseline foundation in operations within the air domain (garnered through undergraduate pilot training (UPT)) but employ it through specifically different mission sets:

11AA C-5	11AB C-9	11AC C-12	11AD C-17	11AE C-20/C-37
11AF C-21	11AG VC-25	11AH C-26	11AJ C-27	11AK C-130
11AL C-135/C137	11AM C-141	11AN T-43	11AR T-3/T-41	11AS T-37
11AT T-1	11BA B-1	11BB B-2	11BC B-52	11BM T-37
11BN T-38	11FA A-7	11FB A-10	11FF F-15	11FG F-15E
11FH F-16	11FJ F-22	11HA HH-1H	11HB UH-1H	11HC HH-1N
11HD HH-3	11HE HH-60	11MA C-5	11MB C-130E/H	11MC C-130J
11MD c-141	11ME VC-25	11MF KC-135	11MG KC-10	11MH C-9
11MJ C-12	11MK C-17	11ML C-20/C-17	11MM C-21	11MN C-26
11R3 EC-130	11RA E-3	11RB E-4	11RC EC-130	11RD HC-130
11RE WC-130	11RF EC-135	11RG RC-135	11RH WC-135	11RJ U-2
11RL E-8	11SA MH-53	11SB MH-60	11SC AC-130H	11SD AC-130U
11SE HC-130	11SF MC-130E	11SG MC-130H		

Figure 18: Example Pilot AFSCs

These separate mission areas all exploit the air domain for the purpose of securing their individual mission success which ultimately supports overarching Air Force goals and

objectives. In order to execute these missions however, they all rely on another function, combat support. Combat support is defined in *AFDD 1* as "the essential capabilities, functions, activities and tasks necessary to create and sustain air and space forces" and is "the science of planning and carrying out the movement, maintenance and protection of forces"; a completely different mission perspective than that of operations. They are the forces designated with the responsibility of fielding and ensuring military capability is ready for full spectrum operations whereas operations are the employment of those capabilities. Combat support is organized much differently as a result of this differing mission focus as seen in a completely different series of AFSCs within the Air Force:

21A Acft Main/Muns	21B Maintenance	21G Log Plans	21M Muns & Mis Main
21S Supply	21T Trans	32EA Architect	32EB Readiness Eng
32EC Civil Eng	32EE Electrical Eng	32EF Mechanical Eng	32EJ Environmental Eng
33S (17D) Comm			

Figure 19: Combat Support AFSCs

It is interesting to note that these combat support forces, in terms of officer AFSCs, are much broader in skill (with the possible exception of Civil Engineers (32X)) as they function more as management forces ensuring the specialized enlisted AFSCs within their purview provide the necessary combat support function for employment of that military capability. There has been no apparent need for specialization within the combat support officer force as technical expertise in these fields' lies within the enlisted force. The officer corps is focused on the broader macro issues of providing combat support in

today's high operations tempo environment (again, with the possible exception of Civil Engineers).

It is through the combination of these two, operations and combat support that the Air Force projects combat capability through the air domain, understanding that they each have their own specific mission requirements to fulfill and distinct processes and skills to accomplish them. That said, only the counterair operational function has the ultimate mission responsibility of guaranteeing air superiority to ensure "friendly use of contested airspace and disable the enemy's offensive air and missile capabilities to reduce threat posed against friendly forces" (*AFDD 1*, 2003). All others, whether they are the additional users of the domain (the other air platforms charged with missions other than counterair) or broad ranging combat support missions that provide air capabilities for all on the domain, are merely consumers or providers of the domain's capabilities at this point. Counterair forces are charged with the operational mission to "attain and maintain a desired degree of air superiority by the destruction, degradation or disruption of enemy forces" (*AFDD1*, 2003) for the purpose of allowing friendly forces freedom of movement within the domain to complete their operational missions, not unlike the mission given to NW Ops forces with respect to IP networks in the cyberspace domain. It has been seen in the realm of the air domain that there is a desired level of specialization within the operations officer corps focused on unique mission accomplishment while that of combat support function is broad, focused on macro issues and the management of enlisted technicians.

So how does this analogy equate to the cyberspace domain (IP networks)? The list of users whom rely upon the cyberspace availability is larger than that of those relying on the air domain for their mission success. However, only a small portion of those utilizing the cyberspace domain are charged with the mission of ensuring our forces operate in a protected information environment thus allowing Air Force capabilities to operate in an uninterrupted fashion on the network (*AFDD 2-5*, 2005). NW Ops' mission is to create effects upon an adversary whether they are offensive or defensive for the purpose of providing freedom of movement within the domain, not unlike that of counterair's mission in the air domain. Therefore, they should be a uniquely skilled and mission focused force. Tailored to the highly technical aspects of this domain and focused on the development of the specialized TTP required to ensure their mission success; not on network sustainment. It is not feasible to expect a KC-135 pilot to maintain their aircraft, nor should we expect cyberspace operators to function outside their NW Ops mission set if the service it to expect success in the domain.

On 30 Apr 2010, the service implemented the 17D career field as authorized under the 2008 Air Force Roadmap for the Development of Cyberspace Professionals for the purpose of filling the mission void felt by not having an NW operational force. This however, essentially consisted of taking all 33S Communications and Information officers and changing their Air Force Specialty Code (AFSC) from 33S to 17D to emphasize the new focus on operations (Trechter, 2010). Within this implementation, there were two categories (or shreds):

Title	Description
17DXA:	Plans, organize and performs active network defense, exploitation and attack in support of joint, national and AF objectives
17DXB:	Plans, organizes and performs Net Ops to include establishment, operations and passive defense in support of joint, national and AF objectives

from SAF/XCTF 6 Jan 2010 AFSC Conversion Process Background paper

As can be seen, the NW Ops mission accomplishment is to be executed by the 17DXA shred of the 17D career field as shown in the description above outlining "active defense" as opposed to the 17DXB description of "passive defense"; see defense vs. security previously discussed. However, unlike the air domain where combat support forces are purposefully left separate in order to account for the differences in mission focus, the Air Force has taken what was essentially the combat support (NetOps) force for this domain (33S AFSC) and converted it to the operations force. While there is some emphasis and understanding placed on the inherent mission difference between operations and combat support within this AFSC conversion (A and B shred), is there enough separation to allow for what is the vast mission difference between NetOps and NW Ops as outlined previously? Or is the perception that if it is a computer or network there is no variation between operations and combat support missions, unlike the air domain, one that the service should continue?

According to a 17D/33S Career Field Update brief dated 25 Feb 2010, a decision point from Corona South 2010 made SAF/A6 the functional authority for the 17D career field while SAF/A6 will appoint HQ AFSPC/A3 as the 17D Development Team chair

(Abel, 2010). These steps seem to only exacerbate the confusion of operations vs. combat support by attempting to combine the two mission sets instead of understanding the differences and organizing accordingly. Will the battle of overpowering operational requirements in support of all Air Force net-centric operations continuously overshadow the need to provide active operations on the network as long as we continue to attempt both, often competing missions, with the same personnel? Much like the counterair pilot mentioned above, the 17DXA should be highly proficient and specialized in his/her craft as an operator. Conversely, the 17DXB really has no mission change from that of the 33S: maintain and provide the cyber domain for all operational users of the domain, which is focused on management as much if not more than the technical aspect of the domain.

So if there is to be cross-utilization of manpower for the A to B shred and vice versa, how do we ensure the expertise, and equally important, the mission perspective is there to guarantee the NWOps mission? The USAF doesn't take maintenance officers off the flightline to fly counterair missions without sending them through extensive pilot training. Is this the plan for a move from the combat support B shred to the operations A shred? However, this is done within the air domain through a selection board process where non-pilots can apply for UPT. But when selected, the individual is essentially starting over from scratch in terms of training for operations in the air domain as a pilot. A maintenance officer selectee is not just given a limited crash course on air operations because he/she may have an understanding of aircraft as a former maintenance officer for example; they are functionally moved from a combat support mission perspective to the

operations one and completely retrained in this new perspective. So like air, shouldn't the cyberspace domain take a similar approach in force development and employment? If so, why have the same AFSC and functional manager? Additionally, as increased recognition of the vast differences between these two missions in cyberspace is seen, a move to a more air centric model will only make sense. Where two completely separate career fields with separate functional management chains cultivate the mission differences of operations and combat support within the domain for the purpose of providing combat capability for all uses within the domain. We will come to understand that, as doctrine states, combat support is vital to the full spectrum of operations within the Air Force. And the 17DXB mission set (NetOps) of providing that combat support will continue to grow as the service moves toward increased net centricity. This leads to an increased chasm between the missions of NW Ops and NetOps as their focus will be squarely placed on providing capability.

Conversely, the 17DXA NW Ops mission set is one that will evolve, like that of air operations, as continued formalization and categorization of true operational mission requirements are realized. If the cyberspace domain is studied with the same outlook as the air domain, a subset of a physical environment with various technologies/weapon systems used for exploiting the domain (or more precisely, the counterair operational function for the purpose of ensure domain dominance), protocols or technical network types (for example) can be seen in the same light at the various counterair platforms in the air domain; unique and specialized operational sub-mission sets based on exclusive

technological differences requiring differing TTP in order execute their portion of the NW Ops mission. Possibly requiring additional emphasis on specialization within the 17DXA operational force to increase exploitation of the domain, such as:

- 17DXA IP Data Networks Ops
- 17DXB Telephone Networks (PSTN) Ops
- 17DXC Supervisory Control and Data Acquisition Networks Ops
- 17DXD Air Traffic Control and Landing Systems Ops
- 17DXE Integrated Air Defense System Ops
- 17DXF Airborne Network Ops
- 17DXG Space Network Ops

Merely an example to show a possible evolution of the NW Ops mission space, this move toward an increased specialization of skills would only exacerbate the need to separate the operations (NW Ops) forces from the combat support (NetOps) forces as singular functional management leads to conflicting mission focus ultimately damaging the success of both in the long run. As combat support provides the domain for all whom use the network, their focus will lie on maintenance and capability provision, not on combating the adversarial threat within the battle space and vice versa. For further analysis into the network classification and possible 17DXA AFSC classification, reference an AF Institute of Technology Thesis by Lt Col (then Major) Timothy Franz entitled "*IO Foundations to Cyberspace Operations: Analysis, Implementation Concept and Way-ahead for Network Warfare Forces* (Franz, 2007)

Operator vs. Combat Support Focus (Organizational Perspective)

The same rationale that unique mission focus should drive to the realization that separate operational and combat support forces within the cyberspace domain carries over to organizational structure as well. The same confusion in mission perspective and competing objectives seen at the personnel level can also be seen on an organizational one. The current structure under 24AF (NAF for cyberspace) shows tactical level organizations, the 67NWW primarily, attempting to operate as both an operational and combat support organization just as the conversion of to the 17DX career field does above. Additionally, the 689 Combat Comm Wing (689 CCW) is organized as a separate NetOps wing not under the purview of the AF NetOps C2 process when in reality, much of what they do is little different than that of CONUS Network Control Centers (base level networks) other than it is done in austere locations. They still focus on providing and maintaining the domain for all operational users. The 24AF organization chart below (Figure 20) outlines the unsystematic way in which these two unique mission sets are matrixed throughout the organization:

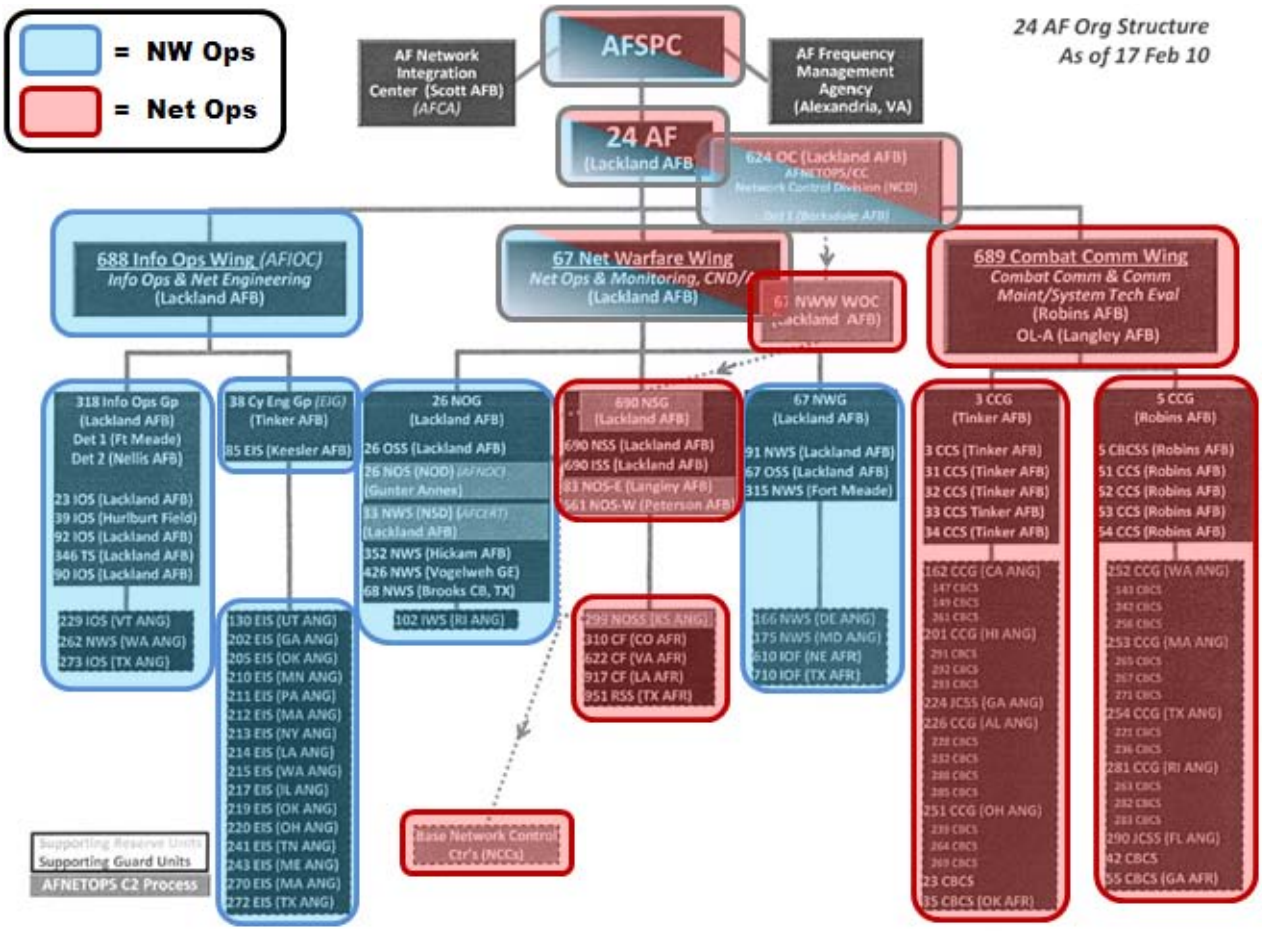


Figure 20: Current 24 AF Organizational Structure

As can be seen, the primary wing for tactical level NW Ops, 67NWW, is also the organization for tactical level control of combat support across the Air Force. This inevitably places leadership in the unenviable position of having to deconflict between the two missions when they should be focused on one or the other. Integration and prioritization of these two should happen at higher level such as 24AF through the 624 Operations Center for operational deconfliction while 24AF and AFSPACE should deconflict issues such as long term funding and strategic direction. Thus allowing wing leadership and down to focus on tactical level mission objectives; see Figure 21:

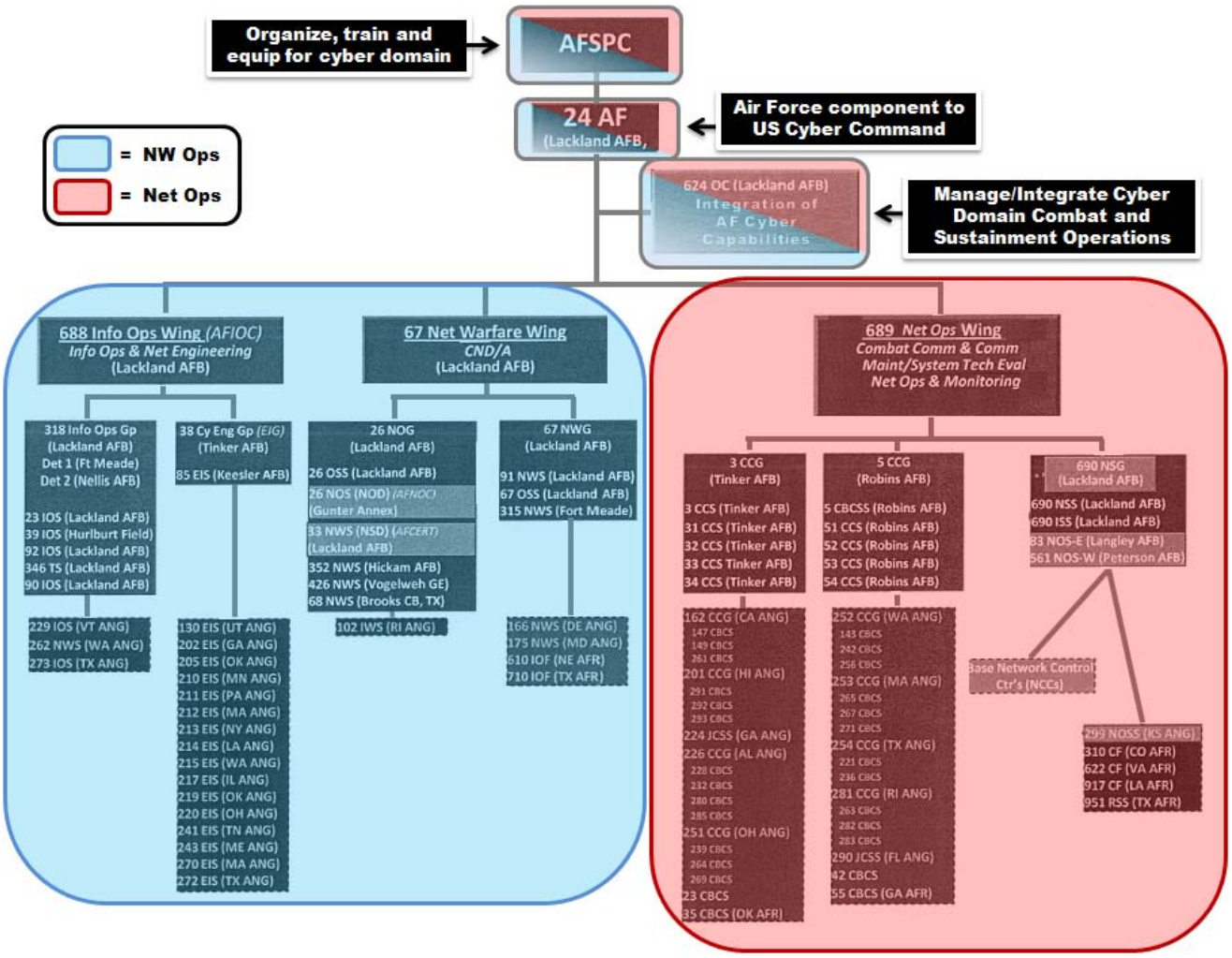


Figure 21: Example Mission Focused 24 AF Organizational Structure

Much like the separation of AFSCs, this organizational split based on mission perspective allows focusing of resources toward one definable mission at the organizational level possible--a step that has been taken in the air domain and a step forwards toward the ultimate goal of flying, fighting and winning in cyberspace.

VI. Conclusion and Discussion

Summary

Cyberspace is a new and ever changing warfighting domain, and the Air Force has shifted focus on this domain over the last five or ten years with a watchful eye to the importance this domain plays on its ability to execute its mission is support of national security objectives. It has instituted such transformation as a new career field and vast, if not ever changing, organizational structure with relation to its networks. However, as this domain continues to grow and develop this change must continue. Operations in the air domain and how we execute them didn't evolve overnight nor do they remain stagnant. It is important, as the Air Force moves forward in cyberspace, that the unique characteristics that define it as a domain and shape operational art within it are understood and utilized in developing the service's domain presence. These significant factors determine how a commander may apply overall strategic objectives and combine them with operational level effects for the purpose of determining what will be accomplished within that domain's battlespace. The land, air, sea and space domains provide great perspectives on proven principles in military operations for possible integration into the cyberspace. Once operations are understood and defined for use, operational function and mission space definition can provide a clearer picture of roles and responsibilities at the organizational and personnel levels for execution of these operations within the cyberspace domain. While the steps taken to date have shown progress, the evolution and focus based on mission perspective must continue if the Air Force is to ensure its mission of flying, fighting and winning in air, space and cyberspace.

Further Research Questions

This research report discussed entities within in the Air Force which focus organizational and personnel resources toward the cyberspace domain, NetOps and NW Ops. Based on an understanding of the domain and operational understanding of offensive, defensive and security operations within the domain, continued research should be applied in the following to aid in the evolution of this domain:

- Focused mission definition: is there a difference between operations and combat support in cyberspace like there is in the air domain, if so, what is it?
- If *operations* is a unique mission in cyberspace, separate from *combat support*, is there a need to split the 17DX AFSC into two as a result? If so, is there a need to evolve the operational AFSC into specialized sub-mission sets based on specialization (pilot model)? For example:
    - 17DXA IP Data Networks Ops
    - 17DXB Telephone Networks (PSTN) Ops
    - 17DXC Supervisory Control and Data Acquisition Networks Ops
    - 17DXD Air Traffic Control and Landing Systems Ops
    - 17DXE Integrated Air Defense System Ops
    - 17DXF Airborne Network Ops
    - 17DXG Space Network Ops

- If *operations* is a unique mission in cyberspace, separate from *combat support*, is there a need for organizational reorganization based on mission? If so, is there further reorganization that must happen to focus on network specialization (see previous)?
- If *operations* is a unique mission in cyberspace, separate from *combat support*, and mission differences drive the recommendation for organizational reorganization and separate career fields, how does recent force shaping of the 33S career field affect this recommendation, is it plausible?

Bibliography

United States Air Force Scientific Board. (2008). *Defending and Operating in a Contested Cyber Domain.* Andrews AFB, MD 20762: Department of the Air Force.

AIA Public Affairs. (2006, Jul 5). *Air Force Stands up First Network Warfare Wing*. Retrieved Mar 31, 2010, from The official web site of the U.S. Air Force: http://www.af.mil/news/story.asp?id=123022799

Air Force Association. (2008, Aug 29). *New Mission statement*. Retrieved Mar 31, 2010, from Airforce-Magazine.com, Online Journal of the Air Force Association: http://www.airforce-magazine.com/DRArchive/Pages/2008/August%202008/August%2029%202008/NewMissionStatement.aspx

Air Force Association. (n.d.). *Quotations on Airpower*. Retrieved May 16, 2010, from http://www.afa.org/quotes/quotes.pdf

Assistant Secretary of Defense (Networks and Information Integration). (23 April 2007). *Department of Defense Directive, 8005.01E, Information Assurance.* Washington, D.C.: Assistant Secretary of Defense (Networks and Information Integration).

Chairman of the Joint Chiefs of Staff. (2010, March 22). Joint Publication 3-0, Joint Operations. Washington, District of Columbia, United States: Charman of the Joint Chiefs of Staff.

Clausewitz, C. V. (1882). *On War.* New York, NY 10014: Penguin Classics.

DISA. (n.d.). *Electromagnetic Spectrum*. Retrieved May 15, 2010, from Joint Spectrum Center: http://www.disa.mil/jsc/speccht.html

Franz, T. P. (2007). *IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-Ahead for Network Warfare Forces.* Wright-Patterson Air Force Base, Ohio: Air Force Institute of Technology.

Gettle, M. M. (2005, Dec 8). *Air Force Releases New Mission Statement*. Retrieved Mar 31, 2010, from The Official web site of the U.S. Air Force: http://www.af.mil/news/story.asp?storyID=123013440

Headquarters Department of the Army. (2008, Feb 27). Field Manual 3-0, Operations. Washington, District of Columbia, United States.

Heckert, P. A. (2007, Nov 20). *The Electromagnetic Spectrum*. Retrieved May 15, 2010, from Suite101.com: http://atomic-molecular-optical-physics.suite101.com/article.cfm/the_electromagnetic_spectrum

Joint Task Force-Global Network Operations. (2009). *Threat Brief.* Joint Task Force-Global Network Operations.

Lane, L. W. (2006, Mar 15). Resourcing for Special Operations Forces (SOF): Should Responsibilities Be Passed From USSOCOM Back To The Services? Carlisle Barracks, Pennsylvania, United States.

LtCol Trechter, S. (2010, Jan 6). Bullet Background Paper on AFSC Conversion Process. Washington, District of Columbia, United States.

Maj Abel, U. 3. (2010, Feb 25). Career Field Update, Training Future Cyber Professionals. Ramstien, Germany.

Meilinger, C. P. (n.d.). *American Airpower Biography.* Retrieved May 15, 2010, from Air and Space Power Journal: http://www.airpower.maxwell.af.mil/airchronicles/cc/mitch.html

Merriam Webster. (2010). *Dictionary and Thesaurus*. Retrieved May 13, 2010, from Merriam-Webster: http://www.merriam-webster.com/

Secratary of the Air Force. (2008, Oct 1). Air Force Doctrine Document 2-1.1, Counterair Operations. Montgomery , Alabama, United States.

Secratary of the Air Force. (2005, Jan 11). Air Force Doctrine Document 2-5, Information Operations. Montgomery , Alabama, United States: Air Force Doctrine Center.

Secretary of the Air Force. (2003, Nov 17). Air Force Doctrine Document 1, Basic Doctrine. Mongomery, Alabama, United States.

Secretary of the Air Force. (2007, Apr 3). Air Force Doctrine Document 2, Operations and Organization. Montgomery, Alabama, United States.

Secretary of the Air Force. (2010, Mar). Air Force Doctrine Document 3-12, Cyberspace Operations (Draft). Montgomery, Alabama, United States: Secretary of the Air Force.

Secretary of the Air Force Office of Warfighter Integration and Chief Information Officer. (17 April 2006). *Warfighter Integration Plan.* Washington, D.C.: Secretary of the Air Force Office of Warfighter Integration and Chief Information Officer.

Smithsonian National Air and Space Museum. (n.d.). *Milestones of Flight*. Retrieved May 12, 2010, from Smithsonian National Air and Space Museum: http://www.nasm.si.edu/exhibitions/gal100/wright1903.html

The Great Idea Finder. (2006, Oct 10). *Heinrich Hertz*. Retrieved May 15, 2010, from The Great Idea Finder: http://www.ideafinder.com/history/inventors/hertz.htm

The University of Waikato. (2007, Jul 30). *The Electromagnetic Spectrum*. Retrieved May 15, 2010, from Science Learning: http://www.sciencelearn.org.nz/Contexts/See-through-Body/Sci-Media/Images/The-electromagnetic-spectrum

U.S.-China Economic and Security Review Commision. (2009). *2009 Report to Congress.* Washington D.C.: U.S.-China Economic and Security Review Commision.

United Air Lines, Inc. (2010). *Route Maps*. Retrieved May 15, 2010 , from United Airlines: http://www.united.com/page/article/0,6823,1019,00.html?navSource=Dropdown07&linkTitle=routemaps

UUNET. (2000, Jun). *UUNET's North American Internet Network.* Retrieved May 15, 2010, from NTHELP: http://www.nthelp.com/images/uunet.pdf

Webcore Technologies. (2010). *Infrastructure - Network Providers*. Retrieved May 15, 2010, from Webcore Technologies: http://www.webcoretech.com/infra/net_providers.cfm

Yes Mag. (1996, Jun 12). *The Science of Flight*. Retrieved May 15, 2010, from Yes Mag: http://www.yesmag.ca/focus/flight/flight_science.html

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
17-06-10	Graduate Research Project	Jun 2009 – Jun 2010

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberspace Mission Focus: NW Ops vs. NetOps	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	**5d. PROJECT NUMBER** N/A
Hawker, Travis J., Maj, USAF	**5e. TASK NUMBER**
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)	8. PERFORMING ORGANIZATION REPORT NUMBER
Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765	AFIT/ICW/ENG/10-03
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Stan G. Cole, LtCol, USAF Student, National War College in route to Commander, Air and Cyberspace Analysis Group NASIC/ACG Comm: (937) 257-2859 stan.cole@wpafb.af.mil cole3@ndu.edu	**10. SPONSOR/MONITOR'S ACRONYM(S)** NASIC/ACG **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States

14. ABSTRACT

This research outlines a method of reasoning for understanding warfighting domains, defining operations within a warfighting domain (primarily offensive, defensive and security) and correlating that operational understanding into mission requirements within the Air Force in order to better answer the questions, "How do we fly, fight and win in cyberspace?" In doing so, this research will attempt to show that what is currently coined as defensive operations on the network are in fact more properly aligned with the doctrinal definition of security in the air and land domains. Furthermore, this research will focus on the inherent differences between the Air Force specific missions of Network Warfare Operations and Network Operations, primarily operations vs. maintenance, and how this different mission focus is misrepresented in terms of personnel and organizational structure. Finally, it will, in response to this misrepresentation, provide brief examples of personnel and organizational changes, using the air domain as a model, which may better align Air Force cyberspace efforts with the ever pressing unique mission requirements resident within the domain.

15. SUBJECT TERMS

NetOps, NW Ops, Cyberspace, Domain, Operations

16. SECURITY CLASSIFICATION OF: Unclassified			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
REPORT	ABSTRACT	c. THIS PAGE			Robert F. Mills, PHD, ENG
U	U	U	UU	68	19b. TELEPHONE NUMBER *(Include area code)* 937-255-3636 x4527

Standard Form 298 (Rev: 8-98) Prescribed by ANSI Std. Z39-18