AU/ACSC/OLSONML/AY09

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

TACKLING CYBERSPACE FORCE DEVELOPMENT ISSUES

by

Matthew L. Olson, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Lieutenant Colonel Brian Landry

Maxwell Air Force Base, Alabama

April 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
APR 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Tackling Cyberspace Force Development Issues	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Command And Staff College Air University Maxwell Air Force Base, Alabama**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

The Air Force (AF), Force Development (FD) construct is currently too limited in scope and implementation to effectively tackle cyberspace FD issues. The perceived gap between establishing a solid cyber culture and its professionals negatively affects the overall ability to integrate effects at the strategic and operational levels. A broader FD approach must exist to synchronize its institutional culture in concert with development of its professionals. The greater result will yield an environment that is cohesive and complementary to utilize and prioritize limited cyberspace resources and capabilities. The disparity of a unified culture and development of its professionals is manifested by fundamental cyberspace identity issues, namely: understanding the general nature of cyberspace (basic purpose, concepts and mission elements); understanding the notional force development strategy to professionalize a cyber field and most importantly understanding how to integrate cyberspace in joint operational planning. Ongoing discussions regarding task-organization, force structure and roles of the 24th Cyberspace Numbered Air Force (NAF) could make some information in this paper quickly obsolete as its future is still being written. A significant amount of source references derive from draft AF cyberspace doctrine, AF Cyber roadmap and various SAF/XC functional way ahead briefings. This paper adopts a problem-solution methodology to address cyberspace identity issues stated above while proposing broad FD recommendations to better link development of its force and culture to meet long term cyberspace demands.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**37**	

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

List of Illustrations

Page

Abstract

The Air Force (AF), Force Development (FD) construct is currently too limited in scope and implementation to effectively tackle cyberspace FD issues. The perceived gap between establishing a solid cyber culture and its professionals negatively affects the overall ability to integrate effects at the strategic and operational levels. A broader FD approach must exist to synchronize its institutional culture in concert with development of its professionals. The greater result will yield an environment that is cohesive and complementary to utilize and prioritize limited cyberspace resources and capabilities.

The disparity of a unified culture and development of its professionals is manifested by fundamental cyberspace identity issues, namely: understanding the general nature of cyberspace (basic purpose, concepts and mission elements); understanding the notional force development strategy to professionalize a cyber field and most importantly understanding how to integrate cyberspace in joint operational planning.

Ongoing discussions regarding task-organization, force structure and roles of the 24th Cyberspace Numbered Air Force (NAF) could make some information in this paper quickly obsolete as its future is still being written. A significant amount of source references derive from draft AF cyberspace doctrine, AF Cyber roadmap and various SAF/XC functional way ahead briefings. This paper adopts a problem-solution methodology to address cyberspace identity issues stated above while proposing broad FD recommendations to better link development of its force and culture to meet long term cyberspace demands.

Introduction/Roadmap

Draft, AFDD 2-11, *Cyberspace Operations* states: While not everyone requires the depth of expertise maintained by cyberspace professionals, every Airman should have a general understanding of the cyberspace domain.[1] Although the term cyberspace is incorporated in Air Force (AF) doctrine, advertisements, slogans, and briefings, it would appear very few Airmen understand what it is and more importantly how it contributes towards achieving operational effects.

It was through this research and discovery process, I concluded the AF view of cyberspace Force Development (FD) is currently too limited in scope and implementation to effectively tackle key cultural identity issues facing Airmen today. The AF must broaden its view towards a holistic approach to synchronize the development efforts of its professionals and mature its culture to best employ its effects across the spectrum of conflict.

This paper roadmap addresses: strategic and operational planning via a framing construct; Communications and Information (C&I) primers which set the conditions for cyber transformation; defining the general nature of cyberspace; charted career path of its professionals and provide broad FD recommendations to yield a mature and cohesive culture for long term mission sustainment. Devoid of a means to provide operational relevance, cyberspace will remain ambiguous, or worse yet, ineffective and improperly employed.

The moment of arrival for cyberspace maturity is when every Airman (eventually all Joint) can articulate its mission capabilities and limitations, and treated on parity with its cross domain counterparts such as air, space, land, and sea. Until this state has been achieved, the AF must lead its Airman to infuse its mission capability to realize its full potential to the joint fight.

The Necessity of Framing

Strategic Framing: Ends-Ways-Means

As indicated by its mission statement, the Air Force objective is to attain superiority in air, space and cyberspace domains. Military planning is the critical link to employ tactical capabilities to achieve operational and strategic objectives. Military planning is inherently interlaced with complexity and confusion across all levels of warfare. One has less control over environmental complexities but can reduce confusion by applying a logical framing approach. In his book, *Campaign Planning: Tools of the Trade,* Dr. Jack Kem poses three questions: what is the problem?; what is the solution?; and does the solution solve the problem?[2] Despite its simplicity, there is immense value as they frame a context to visualize the linkage and relationships in a strategy to objective analysis.

Framing provides a reference point to focus thereby analyzing its individual and related components. As with all types of warfare, cyberspace fits within a strategic ends-ways-means construct. The ends involve understanding the strategic end state of what you wish to achieve. Strategic guidance is generally broad in nature yet communicates specified objectives (goals) that must be attained to achieve the desired end state. The means imply the given resources and capabilities one has to expend towards its intended objectives. Cyber resources consist of physical elements of a man-made domain such as: infrastructure, architecture, electronics and human capital. The ways indicate an employment methodology of limited resources within given constraints of space and time. Cyberspace methodologies include offensive and defensive warfare competencies to achieve cyber superiority. The most popular form of cyber warfare is Computer Network Operations (CNO) comprised of net attack, net defense and net exploitation that may achieve direct and indirect effects in cyber and cross domains such as air, land, space

and sea. Every viable strategy must be founded on sound planning and a means of continuous assessment to indicate progress towards a Measurement of Effectiveness (MOE); potential Decision Points (DP); and if a strategy to task alignment was based on faulty assumptions.

The ends-ways-means construct provides an overall strategic campaign view, the Joint Operational Planning Process (JOPP) provides cyber planners an operational framework to conduct a coherent and logical decision analysis of Course of Action (COA) recommendations. Timeless planning constants must have flexibility; must be shared (collaboration) and must have understood logical relationships and linkages. Ill-defined plans without proper vetting are destined for failure. The very essence of military planning is to provide clarity, scope of purpose, logic in strategy and minimal risk during employment.

Operational Framing: Joint Operational Planning Process (JOPP)

The Joint Forces Air Component Commander (JFACC) is the senior AF representative to the Joint Force Commander (JFC) charged with integration and employment of air, space and cyberspace capabilities in theater operations. The JFACC will typically have an inadequate knowledge of cyberspace and therefore rely on embedded cyber liaisons within the Joint/Air Operations Center (JAOC/AOC) to represent cyberspace capabilities, effects and limitations.

Strategic framing spans the entire campaign architecture through a cognitive map incorporating Operational Design (OD) and Operational Art (OA) planning elements. The JOPP is an operational-level problem framing concept referenced in Joint Publication (JP) 5-0, *Joint Operational Planning*, which allow planners to frame the problem, present options in the form of Courses of Action (COAs), and provide a systematic approach to flesh out and document its proposed Concept of Operations (CONOPs). Once approved, the CONOP will be published as an Operational Plan/Order (OPORD/OPLAN).[3] The JOPP accomplishes the fundamental task of

providing clarity on presented COA options as well as the decision analysis used to support COAs. The JOPP process validates task analysis and instills confidence that the proposed options offer the highest probability of success with the least amount of risk within the given constraints.

There are seven principal steps which make up the JOPP process. The first two steps Initiation and Mission Analysis (MA) utilize OD elements to centralize efforts in framing Dr. Kem's question: what is the problem? Steps three through five utilize OA elements to centralize efforts in framing Dr. Kem's second question: what is the solution? Built within these steps include validation measures to answer his last question: does the solution solve the problem? Steps six and seven reflect the selection, approval and publishing of the CONOPs. The following is a look at the JOPP and highlights opportunities where cyberspace planners should consider during operational planning.

Step 1. Initiation: Joint planning is generally initiated at the strategic level of war by the President, Secretary of Defense and CJCS to convey strategic guidance and specified U.S. interests or designated an end state. Perfect guidance will provide clear objectives, purpose and identify what constitutes success.[4] Planners can often expect less than perfect guidance which may require military leaders to obtain further clarity with civilian authorities.

J5, Plans and J3, Operations directorate often conduct strategic-level translation of national guidance into operational military objectives. The end states are dictated standards and conditions as approved by the President or Secretary of Defense which must be met prior towards the commencement of joint operations.[5] Clarity of a military end state includes a termination criterion which specifies conditions under which the military no longer should serve as the primary Instrument of Power (IOP).[6] The military may continue in a supportive role (i.e.

security and humanitarian assistance) but it is the diplomatic and economic IOPs that must gain the priority of effort to ensure a civil stability during post-conflict operations.

Step 2. Mission Analysis (MA): MA is the most analytically involved step. It requires a CONOPs baseline to convey situational awareness for civilian leadership, subordinate commanders and their staffs. The goal of MA is to frame the problem and communicate initial guidance to subordinate commands. Specified activities include: Joint Intelligence Preparation of the Environment (JIPOE); initial development of Commanders intent; Initial Planning Guidance (IPG); initial development of Commanders; Critical Information Requirements (CCIRs); and initial assumptions and limitations.

Based on strategic guidance, cyber planners conduct a logical task analysis of its supported/supporting links and relationships to produce a task determination (implied and specified). This rigorous process of task analysis is to produce the mission essential task list which serves as the baseline of the commanders mission statement and objectives. During this step, cyber planners have the greatest responsibility and influence to translate how cyberspace may best effect a commanders intent across all levels of warfare to include operational limitations, risks and assumptions.

Cyber activities play a tremendous role in shaping and enabling operations throughout all campaign phases and may follow through conflict termination. Achieving unified action through continuous coordination and cooperation is the utmost priority of the JOPP. Partnerships may reside outside service level and include joint, interagency, and coalition partners. Planners must remain critically aware of risks and implications that can unintentionally counter other national IOP or coalition efforts. Interagency and joint synchronization remains a complex and difficult challenge but a proven necessity to permit unity of effort.

Draft, AFDD 2-11, *Cyberspace Operations* states that cyber planners participate in tactical and strategic level planning: At the tactical level, they employ cyberspace warfare tools and weapon systems from land-based or airborne platforms. They maintain proficiencies in Tactics, Techniques and Procedures (TTP) designed to create a range of effects (e.g., deny, disrupt, collect, defend). At the operational and strategic levels, they are well versed in a broad range of cyberspace capabilities and joint processes, permitting the effective integration of cyberspace assets with other national and military capabilities.[7]

Step 3. COA Development: The purpose of this step is to ensure the JFC has viable COA options. All COA's must meet Chairman Joint Chief of Staff (CJCS) five basic validity criteria: Adequacy, is the COA built within the JFC guidance?; Feasibility, is the COA designed within the given time, space and resources? Acceptability, does the COA balance cost and risk associated?; Distinguishable, is the COA a distinct option from the other proposals? and Complete; how well does the COA document and comply with joint doctrine, format and intent?

Step 4. COA Analysis and Wargaming: Cyber planners conduct preliminary validation of initial assumptions i.e. non-kinetic strikes against an adversary's Command and Control (C2) nodes. Assumptions often prescribe limitations to gauge what a plan can or cannot do. It is vital commanders incorporate assumptions in planning estimates and consider branch or sequel plans as an appropriate means to reduce associated risks and answer the "what now" in case assumptions are proven false. Planners may wargame proposed actions through various methodologies such as modeling and simulation to increase predictability of success in attaining objectives. Planners may devise a Decision Support Template (DST) which records ongoing battle events and matches them to a proposed counter action matrix built as a soft "play book". JP 5-0, *Joint Operations Planning*[8] states that planners will identify governing factors to aid in

comparing courses of action. Governing factors are aspects of the situation, imposed by external factors or those the commander deems critical to mission accomplishment. Potential governing factors include specified elements of the commander's intent and planning guidance; wargaming results; selected principles of war'; external constraints or any criteria the commander desires.

Step 5. COA Comparison: In this step, cyber planners test methodologies against governing factors to ensure COA options meet specified JFC guidance. It is important to note that the JOPP is an iterative process. The commander's estimate and OPORD/OPLAN will remain in a continuous state of refinement throughout until final publication. Planners must remain adaptable and consider broad implications across other domains and IOPs. An example of stove-pipe planning would be a directed cyber attack against an adversary's civilian radio and television broadcasting stations with the intent to neutralize state propaganda. This action could unintentionally counter Information Operations (IO) objectives designed to encourage citizen understanding of coalition intent or hamper humanitarian efforts to guide fleeing refugees to medical and food shelters.

Step 6. COA Selection: The Plans division chief will present all fleshed out COAs in a decision brief for selection and approval by the President or Secretary of Defense. It is the cumulative, rigorous and continuous analysis of all steps which evokes confidence that the JFC has a winning and attainable strategy with the least amount of risk.

Step 7. OPLAN/OPORD: Once COAs have been approved by the appropriate authority, the Execute order (EXORD) is published for Geographic Combatant Commanders (GCC) to execute the designated CONPLAN as specified by an OPLAN/OPORD. It is not enough to view cyberspace as a stagnant set of capabilities. One must carefully align and employ cyber professionals and capabilities to produce operational relevance in a joint fight. In order to

appreciate what cyber is trying to build, it is also important to appreciate the historical context from which C&I evolved.

C&I Evolution – Cyberspace Primers

The evolution of C2 communications eventually led to the modern paradigm of netcentric models of operation. The AF netcentric model would be forced to adapt or go extinct by multiple factors such as: Operationalize the Network (OPTN), Knowledge Centric Operations (KCO), and Presidential Budget Decision (PBD) 720.

Operationalize the Network (OPTN): In late 1997, OPTN was an initiative which changed the cultural image of C&I. OPTN de-emphasized its prized networks and emphasized the operational capabilities it supported. The fundamental strategy to re-associate networks as a weapons system garnered wide-support from the operational community. C&I Airmen articulated operational risk relative to their associated mission(s). OPTN elevated C&I's stature to obtain quality training, selective management, equipment block upgrades, and Wing cooperation to meet the glaring necessities of requiring a sound (network) defense in depth strategy. OPTN successfully wrestled operational control of base networks away from the host Wing Commander and solidified its oversight under the Department of Defense's, integrated Global Information Grid (GIG) architecture.

The AF response to pervasive network threats such as network intrusion and malicious code (worms or virus's) resulted in the centralization of all base network management functions to MAJCOM, Integrated-Network Operating Support Centers (INOSC). The INOSCs hierarchy reported to an AF service component under the purview of U.S. STRATCOM's, Joint Task Force-Global Network Operations (JTF-GNO). As part of the OPTN initiative, the C&I community redefined its leadership duty positions to emulate those of an aircrew.

Knowledge Centric Operations (KCO): The next push came from the EUCOM commander, Lt Gen. Tom Hobbins who stated in the Aug 2007, C4ISR Journal: Today's operator is drowning in information, yet starved for knowledge[9] General Hobbins promoted the concept called KCO and declared: Knowledge-centricity focuses on people and information first and hardware second. It requires a level of operational rigor to focus on how to present the information and develop a seamless way for the operator to make it discoverable, regardless of format or location.[10] KCO articulated that IT systems were to provide relevant warfighting effects in terms of delivering the right information at the right time.

Presidential Budget Decision (PBD) 720: The most distinguished event that expedited the C&I transformation was the Presidential Budget Decision (PBD) 720. In late 2006, the Air Force began implementation of PBD 720, which targeted personnel capital of the military, civilian and defense contractors in order to offset needed recapitalization and modernization priorities at large. PBD 720 was executed through force shaping means and it reduced active duty AF wide authorization end strength by 32,440 in order to meet congressionally authorized levels[11]. The C&I community took a substantive hit from this initiative affecting ~ 8,179 billets including: 6,927 Enlisted reductions and 1,252 Officer reductions. The reduction forecasted a dismal and challenging future. The C&I functional leadership responded with a transformation plan and multiple initiatives to counteract post PBD-720 effects. The transformation of C&I to cyber was a natural evolution.

This paper, has reflected that cyberspace is not merely a set of stagnant capabilities but offers significant relevance to the joint planning process in achieving operational and strategic effects. It qualifies as a legitimate FD issue when the scope of FD does not adequately look at integrating its professionals and capabilities in the joint process. Many of the C&I primers

evolved as technology drove the need to transform data processing into relevant information power. The following discusses the basic nature of cyberspace definition, objectives and key elements.

Defining The Nature of Cyberspace

It is my assertion that a contributing factor towards the cultural identity issues lie in a misperception. On several occasions I observed a recurring theme echoed by Airmen of all ranks that: if they didn't grow up with it, they don't understand it. This theme infers to the inability of self-identification with cyberspace which results from a cultural gap or experience during its ongoing developments. Some feel the word "cyberspace" invokes a technological culture and language of its own and only understood by communicators. Although cyberspace has unique characteristics, capabilities and limitations conveyed by a specific vocabulary, the same is true about any domain and is not exclusive. Simply put, cyberspace is a conceptual manmade domain in which we strive to integrate its various elements to enhance warfighting effects in and across other cross-domains. The following sections broadly addresses cyberspace domain elements comprised of: strategic (guidance, objectives) and operational (cyber warfare, cyber operations, and competencies) to help frame the cyberspace nature.

Strategic Element

Strategic Guidance: Once the root problem has been identified, one can begin to ask Dr. Kem's questions to initiate a strategy to task development. Strategic guidance emanates from national levels such as the President, National Security Council (NSC), Secretary of Defense (SECDEF) and CJCS. Strategic guidance can be delivered by formal and informal means to articulate national interests.

Defining Cyberspace: The National Military Strategy of Cyberspace Operations (NMS-CO) defines cyberspace as: A domain characterized by the use of electronics and the electromagnetic spectrum to store modify, and exchange data via networked systems and associated physical infrastructures.[12]

On 30 Oct 2008, Vice Chairman, Joint Chief of Staff, General, James E. Cartwright published the official DoD definition of cyberspace as: The employment of cyber capabilities where the primary purpose is to achieve military objectives and effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid (GIG).[13] The DoD definition, although welcomed, adds complexity by competing with the NMS-CO definition. The key distinction is that the DoD definition removes both electronic and electromagnetic elements and re-centers cyberspace to focus on netcentric operations and defense of the GIG. General Cartwright's cyberspace letter additionally states: operations that may cause effects in cyberspace (e.g. electronic warfare, psychological operations) that do not employ cyber capabilities should not be considered cyberspace operations.[14]

Draft, AFDD 2-11, *Cyberspace Operations* is the primary AF doctrine and defines cyberspace as: A global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.[15] Although its definition can be construed to align with the DoD definition, its implied elements as further outlined in AFDD 2-11, *Cyberspace Operations* support the NMS-CO definition.

Cyberspace Objectives: Objectives are essential operational goals that bridge the gap between strategy to task. The 2003 *United States National Strategy to Secure Cyberspace* is a

key document which lists the following defensive-oriented strategic objectives in nature: prevent cyber attacks against America's critical infrastructures; reduce national vulnerability to cyber attacks, and minimize damage and recovery time from cyber attacks that do occur.[16]

The Air Force Cyberspace Command (Provisional) incorporated specified objectives of the National Military Strategy (NMS) but also added offensive-oriented objectives: deter and prevent cyberspace attacks against vital US interests; prevent and rapidly respond to attacks and reconstitute cyberspace operations; integrate cyberspace power in the full range of global and theater effects, and defeat adversaries operating through cyberspace[17] The identified strategic objectives set the operational framework for which the services are to Organize, Train and Equip (OT&E). A fundamental challenge still exists in settling and resolving the definition which will impact standardization of OT&E across the services.

Operational Element

Cyber Warfare: Cyber warfare describes information and signals used to deliver effects against military systems. During an ACSC cyberspace lecture, the senior scientist for Information Assurance (IA), Information directorate, AFRL, Dr. Kamal Jabbour specified that the signal must have an influence on the intended system; meaning the destruction of an adversarial system alone does not constitute cyber warfare.[18] Dr. Jabbour stated that the influence can come in the form of direct or indirect influences. An example of a direct influence is an action taken to directly disrupt or deny an information system through a malicious code attack, while an example of an indirect influence would be to create a condition by which the system is altered, affecting the adversary's "trust factor" or system integrity.

Pyramid Framing: Despite differing definitions, the AF adopted the NMS-CO concept to accept cyberspace domain elements which comprised of the following components: electromagnetic spectrum (signals); electronics and infrastructure (physical), and logical (network). All elements are capable of providing offensive and defensive effects from each respective component. This concept is best illustrated in AFDD 2-11, Fig 1 below.

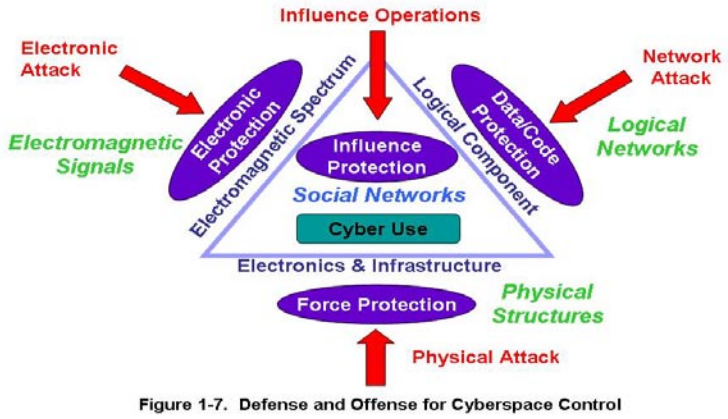

Figure 1: Defensive and Offensive for Cyberspace Control

This figure serves as an operational level frame, illustrating offensive/defensive domain elements to attain and preserve freedom of action. This paper will not cover all elements in depth but illustrate net warfare as the most common example of cyberwarfare.

Network Warfare: Net warfare contains three core capabilities: Network Attack (NetA), Network Defense (Net-D) and Network Warfare Support (NetS). Network Operations (NetOps) describe operations containing either NetA and NetD activities. NetA employs network-based capabilities to destroy, disrupt, corrupt, or usurp information residing in or transiting through networks. NetD employs network based capabilities to defend friendly information residing in, or transiting through networks against adversary efforts. Finally, NetS is the collection and production of network related data for immediate decision involving Network

Warfare (NW) Ops. NetS is critical to NetA and NetD actions in order to find, fix, track and assess both adversaries and friendly sources of access, as well as vulnerabilities for the purpose of immediate defense, threat prediction and recognition.[19]

Cyber Core Competencies: Cyber missions are essential towards achieving information superiority and seen as crucial enablers, particularly shaping operations to establish the needed superiority in and across other domains. The Air Force Cyber Roadmap presents the following cyber competencies:

1. Establish the Cyberspace Domain: In order to have the ability to establish portions of the domain, forces must be expeditionary and independent of host nation support to provide global reach.
2. Control the Domain: This demands robust situational awareness and ability to prepare the battlespace; requires strong defensive capabilities, and means to ensure positive C2.
3. Leverage the Domain: This is the ability to establish and control portions of cyberspace at our time of choosing while denying the same advantage to the adversary. [20]

Enabling Cyber Competencies:

C&I professionals will provide the backbone of cyber forces, yet its success is mutually shared across multiple functional skills who provide equally supporting competencies. Additional competencies as identified in the AF cyber roadmap are: responsive and coordinated engineering and acquisition; dedicated Cyberspace Technical Center of Excellence (CTCoE) in shaping future education, training, and research, and intelligence that provides complete and

integrated commander situational and battlespace awareness necessary to plan and conduct cyber operations in tandem with air and space operations.[21]

Force Development

The cyber force development construct is developed under the authority of HAF A3 (Ops)/A5 (Plans). The force development of its professionals is designed to fulfill specified roles and competencies necessary to attain national and strategic cyber objectives identified above. Cyber Airman can expect to execute operations support across a wide array of AF missions spanning air, space, and cyberspace organizations.[22] The very nature of cyber operations demands an increased technical capability of its enlisted force, led by officers who understand the operation and can recommend best options to achieve the intended effect.

Cyberspace Roles: Based on anticipated realities of PBD 720, C&I leaders developed an aggressive path for cyber transformation. A fundamental task was to identify core cyber roles which would encompass implied Knowledge, Skills and Abilities (KSA) that would then shape and build specified cyber Air Force Specialty Codes (AFSCs). The Air Force cyber roadmap identifies key cyber professional roles for enlisted and officer:

1. Cyberwarfare Operators: Offensive arm which exploits vulnerabilities, develop operational TTPs and lead overall planning, and execution in and through cyberspace.
2. Cyberwarfare Specialists: Technical arm of cyber to establish, provision and sustain the blue cyberspace enterprise with IA measures; under defensive auspices.
3. Cyberwarfare Analysts: Members of the AF Intelligence Community (IC) who enable defensive, surveillance, reconnaissance, access, or offensive operations. Analysts recognize adversary trends, technologies, and TTP in support of defensive operations.

4. Cyberwarfare Tool/Weapon Developers: Blended mix professionals who focus on development design and software-hardware solutions. It will be their task to develop and employ long and short term combatant commander requirements.[23]

Enlisted Development

As briefed by SAF/XCT, the Force Development for Cyber Transformation, Fig 2. demonstrates convergence of 17 C&I enlisted AFSCs into KSAs. The gray shaded area on the left illustrates the current C&I career field skills and how they are converted into the planned cyber career fields (right-side column). The dark shade of blocks represent the 1B0 AFSC series which focus on operational aspects of the enterprise and the white blocks represents the 1B1 AFSC series which provides a hardware "centric" set of skills. The model establishes the baseline matrix to translate and hone the current C&I work force to the new relevant cyber KSAs.[24]

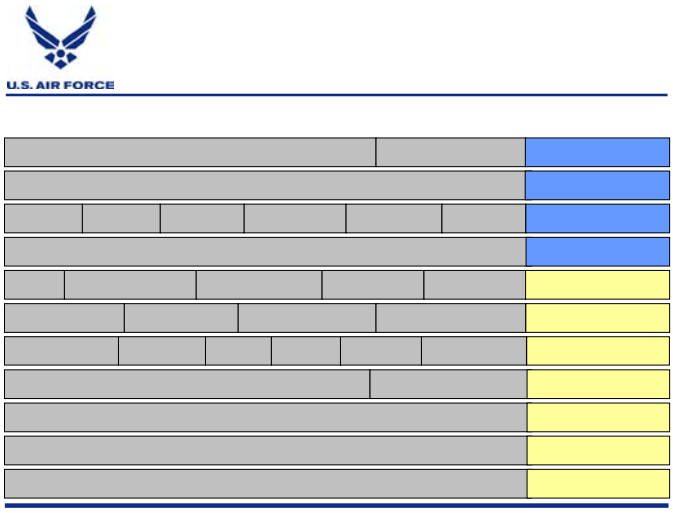

Figure 2: Enlisted Skills Convergence to KSAs[25]

As a general note, the notional enlisted career development construct has not changed from its current paradigm. The enlisted force will provide the technical depth to execute both the cyberspace functions and tactical missions required for cyberspace dominance.[26] Fig 3 illustrates

that AB-SrA will continue to focus on obtaining cyberspace fundamentals and specific tactical level training, SSgt-TSgts will continue to complement their knowledge with Advanced fundamentals. SNCOs are expected to assume enlisted leadership positions such as Superintendent duties where they can take their gained experience and apply an operational perspective.

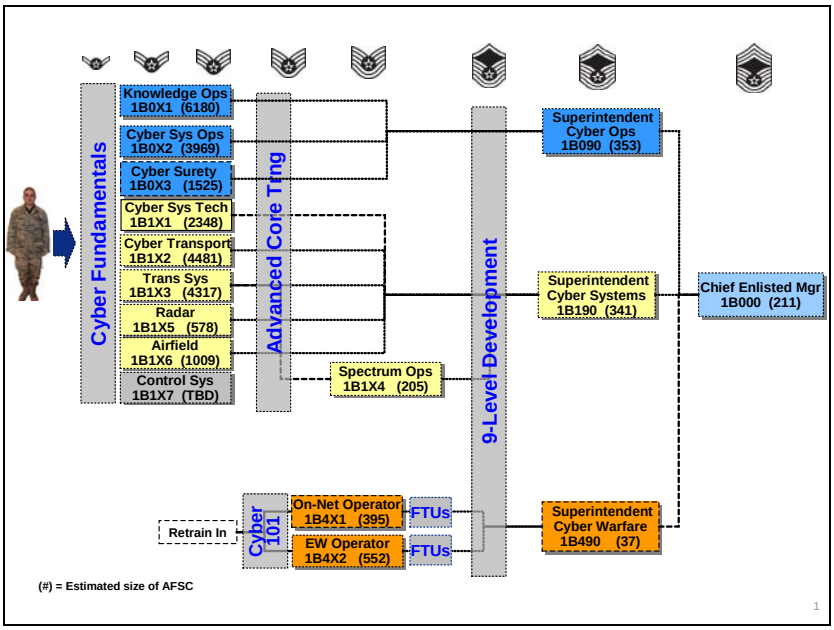

Figure 3: Enlisted Cyber Career Progression[27]

Enlisted Cyberspace Air Force Specialty Codes (AFSCs)

There are ten designated cyber enlisted AFSCs (four undecided) in three borad cyb. There are three broad cyber mission categories: Cyber operations (1B0XX's), Cyber Systems (1B1XX's) and Cyberwarfare Operators, (1B4X's) and NetOps, (1B4X2's). Cyber Analyst will be provided out of the IC. Per the AF Cyber Roadmap, the breakout of projected cyber enlisted force AFSCs is:

1. 1B0X1, Knowledge operators possess content info management, retrieval, and presentation skills. Activities may include: web, COP and collaboration mgt.

2. 1B0X2, Cyber Systems operators focus on server ops, data storage and appropriate software apps. In a deployed environment, this may include exchange and sys admin.
3. 1B0X3, Cyber Surety operators employ IA measures: COMSEC, COMPUSEC and EMSEC. They are essential to ensure a defensive posture of friendly networks.
4. 1B1X1, Client Systems Technicians (CST)s provide client support and integrate approved client-level voice, data, and video devices to the base infrastructure.
5. 1BX2, Cyber Transport Systems focus on airborne and net infrastructure availability.
6. 1BX3, RF Transmissions Systems operators focus on transmission assurance and possess understanding of space, radio, satellite systems technologies to integrate and sustain airborne and terrestrial multi-mode, multi-band radio frequency systems.
7. 1B1X4, Cyber Spectrum Specialists assure base level, electromagnetic spectrum.
8. 1B1X5, C2 Radar Systems Ops provide airfield radar ops mgt and sustainment.
9. 1B1X6, Airfield Systems Specialists provide airfield C2 and nav. systems support.
10. 1B1X7, Cable/Antenna Systems Specialists install wired/wireless infrastructure.

Proposed AFSCs (unapproved/under consideration):

1. 1B1X8, Control Systems Specialists conduct industrial monitoring and control systems of Supervisory Control and Data Acquisition (SCADA); i.e. distribution systems.
2. 1B1X9, Mission Systems Maintenance troubleshoot/repair airborne C2 systems.
3. 1B4X1, On Network Warfare operators provide network attack, defense and exploit capabilities to disrupt, deny, degrade, or destroy adversary information systems.
4. 1B4X2, Electronic Warfare Operators provide electronic protect, electronic attack, jamming, deception, and theater level spectrum management[28].

Officer Development

Ongoing efforts will convert the standard 33S, AF communications officer, to 17D, AFSC series and establish the 12X series to comprise the Airborne Cyber Warrior Officers (ACWOs). As field grade officers, CWOs will be qualified to work at MAJCOM-level or as a planner in the Air Operations Center (AOC), with a leadership follow on in an AOC or a cyber organization as the DO or CC.[29] As with the enlisted development, there is no career development departure from the current 33S development model. Figure 4. Cyber Officer Force Development, illustrates a similar accession to retirement approach for officer development as we saw in the enlisted development plan. The progressive cyber courses (100-400) are a specified series of functional cyber training to keep CWOs in tune with developments, commensurate to ones anticipated career progression.

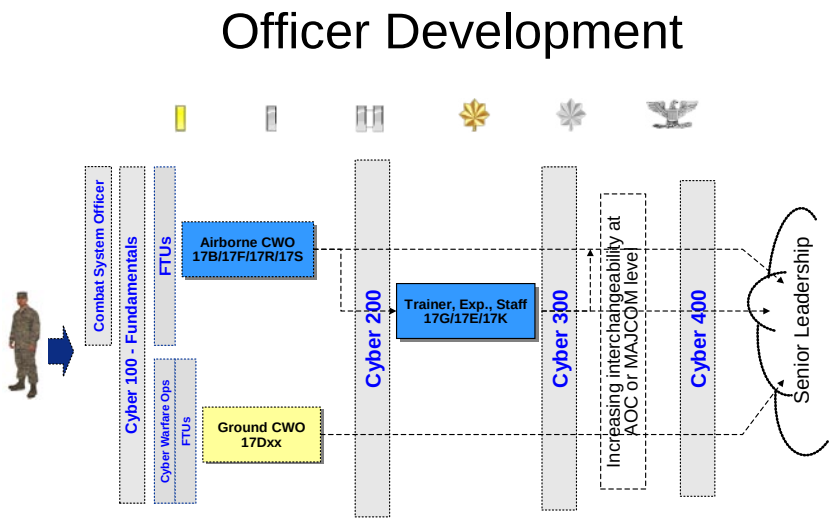

Figure 4: Cyber Officer Force Development[30]

Airborne Cyber Warfare Officer (ACWO): According to the *AF Roadmap for the Development of Cyberspace Professionals* , the rated CWO will be developed for technical depth in their major weapon system platform and later targeted for appropriate non-flying, cyber-

broadening assignments (NETOPS units, Network Warfare units, Space Warfare units, etc). ACWO specialty centers on the use and understanding of the electromagnetic spectrum (EMS). ACWOs are assigned to designated airframes and may provide electronic countermeasures to conduct electronic attack/defense or information operations, or perform as a Weapons Systems Officer (WSO). The ACWO careerfield comprises of the following 12X series:

1. 12B, Bomber CWO assigned to either a B-52 or B1.

2. 12F, Fighters CWO assigned to either an EA-6B or F15E.

3. 12R, Reconnaissance CWO assigned to either an RC 135, EC 130 H/J. The RC-135 EWO is responsible for ELINT, SIGINT and MASINT collection and mission reporting.

4. 12S, Special Operations CWO assigned to either an AC 130H/U or MC 130E/H.

5. 12E, Experimental Test CWOs assigned to plan, direct and report on design development and modification of aircraft, aerospace vehicles and flight simulator.

6. 12G are Generalist ACWOs qualified in another airborne CWO AFSC and performs staff functions for EW and Cyberwarfare programs and issues.

7. 12K are Trainer CWOs qualified in another airborne CWO AFSC and conducts training students in EW and navigation. [31]

Ground, Cyber Warfare Officer (CWO)

Additionally, Ground, CWO AFSC 17D (replaced 33S) will be armed with a broad range of expertise. Proficiencies will include: network systems operations, IA, Computer Network Defense (CND), electronic protection, Computer Network Exploitation (CNE)/ Attack (CNA); expeditionary communications; data links management; spectrum management; knowledge based operations, including chief information officer (CIO) duties; systems engineering and

architecture design; telecommunications, space, command and control, and flight-line systems maintenance. [32]

Ground CWO training will provide junior officers cyberspace fundamentals as 2Lts. Depending upon follow on assignment, they will receive appropriate specialty training as determined by the assigned unit mission.

All CWOs will be required to complete Cyber 100 to be awarded the AFSC training badge. New accessions in 2012 will receive Initial Qualification Training (IQT) in AFSC awarding courses. Many C&I individuals transitioning to cyberspace AFSCs from today until 2012 will require some amount of retraining. Much of the retraining takes place through Formal Training Units (FTUs) as individuals move into assignments in cyber warfare units. FTUs provide the final initial training needed by the cyber career force to achieve IQT status. FTU examples include: Garrison Communications to prepare officers destined for fixed base communications organizations, Network Attack to prepare individuals destined for cyber attack organizations, and Network Defense to prepare individuals destined for cyber defense organizations.[33]

A Holistic FD Approach – Mean What You Say

In Draft, AFDD 2-11 *Cyberspace Operations*, General Norton A Schwartz, CSAF provides initial guidance to "view cyberspace as a whole".[34] The cultural issues specified in this paper reflect evidence of a limited FD scope. It is natural to view force development within a limited scope of establishing and growing a dedicated functional careerfield. However, if cyberspace is to be embraced as a separate but equal domain, then its FD scope needs to expand and synchronize both its institutional culture and maturing force to meet Gen. Schwartz's holistic intent.

A way to illustrate the nature of this problem is to analyze the following statement: Cyberspace is a distinct domain requiring superiority and thus equal to other distinguished domains (air, land, space and sea). If accepted at face value, this statement implies that cyberspace development and sustainment should therefore have equal footing and importance to that of its counterparts. The concept and reality poses expectation management concerns.

Cultural acceptance of cyberspace FD is key to tackling and resolving the identity issues head on and will increase the overall potential of cyberspace to achieve unified actions. Cyberspace must have mission relevance and an equal place at the head of the table in mission relevance across Wing, MAJCOM, HQ and Defense levels in order to attain the designated objectives as determined by strategic policy. This very strategy is necessary to employ that unified strategy to task concept.

Recommendations

A method of closing the gap between its culture and professionals is to apply broader, force development measures. Measures to develop the next generation cyber warriors and stimulate cultural growth will improve overall warfighting effectiveness across all domains. Broad measures must not be limited to front loading education, but also employ continuous measures spanning an entire career (accessions to retirement) to meet long-term requirements. Cyberspace is now a permanent fixture of warfare that affects the entire joint spectrum. The following are a few recommended measures:

1. Resolve the definition of cyberspace: Both national strategic and operational objectives as defined by multiple agencies have created a key issue for the Service components to have a standard set of elements to conduct the OT&E mission. The impact of having a clouded definition of cyberspace detracts from the unified efforts needed to marshal resources,

collaborate and establish cooperative relationships to be effective and responsive in a volatile environment.

2. Create a Cyberspace Road Show: A cyber road show designed to educate and inform basic concepts, FD strategy and operational relevance is a small investment for a high anticipated return. Spread-the-word campaigns are intended to increase visibility and permanence. Greater awareness and permeation of cyberspace in AF culture will facilitate its stature, evoke greater greater understanding and encourage operational integration as a result of building institutional coherence and confidence. It is ideal to ensure that some team members have someone with operational planning experience to relate how cyberspace capabilities fit in planning at each level of warfare. They will be essential to articulating to Wing leadership (via framing) the tactical to strategic chain and why each link is required to support the overall effort. Another objective would be to dispel lingering cultural misperception(s) plaguing senior leaders and convert them to knowledgeable stewards, confident and familiar with cyberspace capabilities and effects as they are with air and space.

3. Create a Cyberspace Inspector General (IG) program. During an ACSC, AP 800 lecture, the guest lecturer spoke on Cyberspace and Information Operations (IO). A question he posed (paraphrase) why C&I determines its success or failure based on whether its services are operational.[35] He indicated C&I professionals should measure operational success based on an effectiveness criteria rather than a platform-based approach. Cyber planners face similar challenges as their counterparts who employ non-kinetic effects i.e.: Information Operations (IO); intelligence and Special Operation Forces (SOF). Quantifiability can not only be difficult to measure, but at times is inapplicable to non-kinetic effects which may only provide qualitative effects. During ACSC, JP-515 lecture, Lt. Col. Linschoten best illustrated this challenge with an

IO example (paraphrase): how does one ensure (with certainty) that an enemy who turned right at a T intersection, turned right as a result of a directed psyop pamphlet drop? How do we prove that the desired action was made based on a factor we introduced or whether it was resultant of an unknown factor?[36] Attribution of cause and effect relationships may be more difficult to validate than an observable kinetic effects; i.e.: counting tanks, killing radar sites, and interdiction of enemy supply lines (all physical).

There are many effects cyber planners should consider and determine Measures of Performance (MOP) and Measures of Effectiveness (MOEs) to qualify as indicators and can be institutionalized in the form of an IG cyber program. Institutionalizing a cyber program will help assist cyber professionals and operational customers remain focused on key capabilities and effects that cyberspace can achieve or contribute to. The key is to relook at strategic objectives and develop associated logical strategy to tasks and effects alignment as discussed earlier in framing. Developing and linking offensive and defensive MOPs and MOEs to designated objectives are the best way to relate mission relevance to operators. This approach will relate the operational mission risk and impacts that OPTN did for C&I in its earlier years.

4. Program budgeting for increased personnel and training: Resource constraints are the biggest challenge towards developing world class professionals. It is not a lack of will as much as ensuring those tasked with the mission have the required authority and resources needed to accomplish it. Most people would agree with the realist view: you get what you pay for. This approach applies in developing a cyberforce. SECAF Wynne stated: We must aggressively dedicate appropriate resources to further develop the intellectual and technical prowess that is a hallmark of today's Airman.[37] However the latest DoD memo, dated 12 Nov 08, Defense Secretary, Gates states: It is imperative that the Services are able to provide the required forces

trained for Computer Network Operations (CNO)…In the near term we will not increase the Service's end strength or the associated travel funds to meet this requirement.[38] The memo clearly stresses the importance of CNO by tasking the Services to go-do without providing additional resources or mention of future program commitments. The DoD and all Service components should remain consistent with their message and actions to better manage operational expectations and mission risks.

5. Reassess Cyberspace in PME programs and incorporate/expand accordingly: During my research evaluation, it would appear Air University (AU) offers limited basic cyberspace instruction outside of Air Command Staff College (ACSC) and Air War College (AWC). Furthermore, a review of curriculum demonstrates the Squadron Officer College (SOC) and Air and Space Basics Course (ASBC) do not have any course curriculum instruction of cyberspace basic doctrine or concepts. From an institutional approach, evidence would suggest wide-gaps exists in education. Therefore, AU should consider conducting a cyberspace assessment of all PME programs, spanning enlisted and officer, residence and distance learning programs in order to better assess where instruction gaps or deficiencies lie that need to be bolstered or established. If left unresolved, the institution may unintentionally send a message which downplays its own mission statement.

Additionally, AU should consider the level of effort to teach senior leaders and operational planners with the art of cyberspace integration. As previously stated, the JFACC is ultimately responsible to advise the JFC on how best to integrate air, space and cyber capabilities. It would be incumbent that AU team with JFCOM as the joint trainer determine if its leaders and planning staffs are adequately prepared to employ cyber in the joint fight. It is unanimous that no one service owns or controls cyberspace. Cyberspace Tactics, Techniques

and Procedures (TTPs), doctrine and training must be considered at the Joint level as it is a joint enabler. Currently there is no cyberspace joint doctrine or joint training.

6. Implement a Cyber Retention strategy/program: Lt. Col. Joe Trector, SAF/XC, 33S functional manager[39] confirmed in a telephone interview that currently there is no discussion of career incentives such as a bonus or other incentive to retain cyber professionals.[40] The AF Road Map says: Well planned retention strategies must be developed to help retain these skilled professionals.[41]

Having a lack of retention program in a profession that requires specialized skillsets could present risks to managing expectations of meeting long-term mission goals and prove unrealistic to its long term accessions to retirement. Draft, AFDD 2-11, *Cyberspace Operations* states: This evolving era of cyberspace operations requires that individuals possess high standards of technical competence, robust analytical skills, and an intimate understanding of warfare application in cyberspace. To be successful in an evolving era of cyberspace, continuous learning is paramount.[42] This statement implies that a significant and continuous investment is required in terms of training cost and time to develop proficiency across an operational environment. Cyberspace, unlike its domain counterparts will evolve at an unprecedented pace. Modernization, research and development costs are necessary to keep pace with the rapid developments of new threats and actors. SAF/XC leaders, education leaders and functional managers must team to view force development from a holistic approach and consider how its current retention strategy (or lack thereof), promotion and continuous education requirements impact the overall long-term mission success.

A viable retention strategy should also consider the concept of ensuring the right force mix of active military, Air Reserve Component (ARC), civilian and contractor forces. Cyber

leaders will need to closely consider the mission and its requirements to determine if a particular force might be better suited than another. As an example, certain positions and missions would not be well suited for an active duty officer, on a standard three year tour. Particular cyberskills require a significant amount of investment time to train and develop. Cyber leaders and functional managers should consider if contractors, ARC or civilians might be a better fit to reduce mission impact by assuring uninterrupted longevity and seasoned experts for various cyber missions at home station while contractors or civilians may be limited or unable to fulfill operational deployment requirements. Cyber leaders, education institutions, and functional managers must collectively assess, and synchronize the right force mix to meet long-term cyber requirements while ensuring that cyber professionals are afforded opportunities for assignment breadth and promotion.

7. Train as you Fight: We've all heard the concept of "train as you fight". It's one of the very redundant lessons learned theme from most every major operation and exercise. It holds true that we should have in place a system and mechanism to ensure the proficiency and quality of our cyber experts remains the highest in the world. During a telephone interview with Lt. Col. Trector, SAF/XCT, best described the training end-state of cyberspace professionals as (paraphrase): we somehow need to get cyberspace operators to a point they become no different than pilots who train, conduct mission planning, go to the range to execute the mission, return to base for an analysis, conduct an outbrief, return home and do it again the very next day.[43]

Let's suppose we take the action to formalize an IG cyber program which identifies and evaluates Mission Essential Task List (METL)s as determined by functional managers and GCCs who know first-hand, the relevant, operational KSAs and capabilities needed in theater. In theory, the bases should then train and practice to meet those required capabilities and integrate

proficiency checks as a graded instrument within the Wing, Operational Readiness Inspection (ORI). It would be advisable to incorporate a systematic approach which employs a continuous training mission at home related to operational objectives and then conduct the evaluation of cyberspace readiness through institutionalized programs such as an IG and Wing ORI. This systematic approach should ensure a ready force, capable of delivering those relevant METL capabilities to its operational customer. It is only by these established means and thinking that cyberspace will advance to attain operational mission parity at all levels as AF doctrine envisioned.

Conclusion

This paper proposed that the current scope of AF cyberspace FD is too limited. As a consequence of that result, this paper addressed key cultural identity challenges related to the synchronizing development of its force to a well established culture. Those issues were: understanding the general nature of cyberspace; understanding the force development strategy, and integrating cyberspace in the joint operations planning.

To counter those issues, a framing construct relayed how cyberspace fit within a strategic and operational level construct. Furthermore, this paper provided information to convey its basic domain nature (cyber concepts and elements), notional force development of cyber Airman and the importance of the JOPP to incorporate cyberspace capabilities in operational planning.

By considering General Schwartz's "holistic" concept of cyberspace requires a broad scope to focus many components of its FD which includes policy and relationships in support of the ultimate goal of attaining cyber superiority.

Americans can no longer underestimate the adversary as we did in Korea, Vietnam, Iraq and Afghanistan. Our battlefield is now a virtual plane as real as a geographical one. The

constant that applies to both is that our confidence cannot rest alone in our military might or technical superiority. Our enemy is cunning, adaptive, and capable of countering US might by leveraging asymmetric warfare in cyberspace to gain the advantage. Cyber warriors equipped, educated and trained to conduct shaping or enabling operations in the virtual battlefield are a necessity across all campaign phases. The assurance of mission success does not lie in technology, but the commitment to develop a capable and prepared cyber force and a dedicated culture who are as cyberminded as they are airminded.

Notes

[1] Draft, AFDD 2-11, *Cyberspace Operations*, 21
[2] Dr Jack Kem, Campaign Planning, 13
[3] JP 5-0, III-1
[4] JP 5-0, III-5
[5] Ibid
[6] Ibid
[7] Draft, AFDD 2-11, *Cyberspace Operations*, 45
[8] JP 5-0, III-31
[9] Gen Tom Hobbins, C4ISR Journal, 1 Aug 2007
[10] Ibid
[11] *XC-PBD 720 FOA Cyber Brief*, Powerpoint brief, SAF/XCTF, January 2009
[12] National Military Strategy – Cyberspace Operations (NMS-CO)
[13] VCJCS letter, dated 29 Sept 08, Subj: Definition of Cyberspace Ops
[14] Ibid
[15] AFDD 2-11, Cyberspace Operations, 9
[16] National Strategy for Cyberspace
[17] National Military Strategy - Cyberspace Operations (NMS-CO)
[18] ACSC Lecture, AP 800, 27 Jan 2009
[19] Jabbour, 50 Cyber Questions, 10
[20] AF Cyber Roadmap, 5
[21] Ibid, 6
[22] Ibid, 10
[23] Ibid- 26
[24] Force Development for Cyber Transformation Brief, Oct 08
[25] Ibid
[26] AF Cyber Roadmap, 10

Notes

[27] Ibid, 11
[28] Ibid, 22
[29] Ibid, 13
[30] Ibid, 23
[31] Ibid, 26
[32] Ibid, 26
[33] Ibid, 31
[34] AFDD 2-11, Cyberspace Operations, foreword
[35] ACSC Lecture, AP 800, 27 Jan 2009
[36] ACSC Lecture, JP 516, 2 Feb 2009
[37] AF CyberRoadmap iii
[38] OSD memo, dated 12 Nov 08, Subj: Developing Trained Cyberspace Forces
[39] Lt Col Joe Trector, telephone interview, 24 Oct 2008
[40] Ibid
[41] AF Cyber Roadmap, 18
[42] AFDD 2-11, 44
[43] Lt Col Joe Trector Phone interview

Bibliography

1. ACSC Cyberwarfare Lecture, AP 800, 27 Jan 08 (unattributed guest speaker)
2. ACSC Information Operations Planning Considerations Lecture, JP 516, Lt Col Michael Linschoten, 2 Feb 08
3. (Draft) Air Force Doctrine Document (AFDD) 2-11. *Cyberspace Operations*, 31 Nov 2008.
4. AFRL publication, Document number: WPAFB 08-3194, Jabbour, Kamal T. *50 Cyber Questions Every Airman Can Answer*,
5. *Force Development for Cyber Transformation* Powerpoint brief, SAF/XCTF, Oct 2008
6. Gates, Robert M., OSD memorandum to all secretaries of military departments, Subj: Developing Trained Cyberspace Forces, dated 12 Nov 2008,
7. General James Cartwright, VCJCS memorandum to Deputy Secretary of Defense, Subj: Definition of Cyberspace Ops, 29 Sept 2008,
8. General Tom Hobbins, C4ISR Journal, 1 Aug 2007, http://integrator.hanscom.af.mil/2007/August/08302007/08302007-22.htm
9. "Joint Operational Planning Process," *Operational Art and Campaigning Primer*, Joint Advanced Warfighting School. In *Joint Campaign Planning: Volume 6* course book, edited by Sharon McBride, 1-7. Maxwell AFB, AL: Air University Press, Jan 2009.
10. Joint Publication (JP) 5-0. *Joint Operation Planning*, 26 Dec 2006.
11. Kem, Jack D. *Campaign Planning: Tools of the Trade*, *Second Edition*. US Army Command and General Staff College, Fort Leavenworth, KS, Jun 2006.
12. Lt Col Joeseph Trector, SAF/XCTF, telephone interview by author, 24 Oct 2008
13. Pace, Peter. *National Military Strategy for Cyberspace Operations*. Washington DC: Department of Defense, 2006.
14. Reilly, Jeffrey M. *Operational Design: Shaping Decision Analysis through Cognitive Vision.* Air Command and Staff College, Maxwell AFB, AL, Oct 2008.
15. The National Strategy to Secure Cyberspace, Feb 2003.
16. The Air Force Roadmap for the Development of Cyberspace Professionals 2008-2013, Washington, DC, 15 Apr 2008.
17. *XC-PBD 720 FOA Cyber Brief*, Powerpoint brief, SAF/XCTF, Jan 2009