

**Strategy to Task
for
Twenty-Fourth Air Force
Cyberspace Operations**



30 March 2009

Table of Contents

I.	Forward	1
II.	Executive Summary.....	2
III.	Assumptions.....	7
IV.	Purpose	8
V.	Overview	9
	A. C-NAF (24 AF) Mission and Vision.....	9
	B. Commander’s Intent	9
	C. USSTRATCOM’s UCP Assigned Cyber Mission	10
	D. USJFCOM’s UCP Assigned Mission as Joint Force Provider	10
VI.	Component-NAF Operations	11
	A. Objectives	11
	B. Desired Effects	14
	C. Required Capabilities	15
	D. Cyber Tasks and Critical Actions	17
VII.	Capability Development Considerations	20
	A. Capabilities Review and Risk Assessment Incorporation.....	21
	B. Inject AF Cyber Equities and Input into JCIDS Process.....	21
	C. Determine Appropriate Panel for POM	21
VIII.	Key Cyber Relationships.....	21
	A. Service and Joint Partners and Relationships	22
	B. Interagency Partners and Relationships	22
	C. Public-Private Partnerships and Relationships	24
	D. Partnership Summary	24
IX.	JOpsC Analysis/Concept Integration.....	25
	A. Concept Analysis and Shortfall Determination.....	25
	B. Gap Determination	25
	C. Concept Prioritization	26
X.	Commander’s Critical Information Requirements.....	27
	A. Priority Intelligence Requirements	27
	B. Friendly Forces Information Requirements.....	28

C. Essential Elements of Information (classified)..... 28

XI. Commander’s Estimate (SWOT Analysis) 29

 A. Internal Factors 29

 B. External Factors 29

XII. Summary 30

XIII. Annex A, Implementation Tasks 31

XIV. Annex B, Family of Concepts Tasks 42

XV. Annex C, Perform AF Cyberspace Force Management (AFCyMA Task 1.0)..... 54

XVI. Annex D, Establish AF Cyberspace Domain (AFCyMA Task 2.0) 64

XVII. Annex E, Operate the AF Cyberspace Domain (AFCyMA Task 3.0)..... 74

XVIII. Annex F, Defend the AF Cyberspace Domain (AFCyMA Task 4.0) 88

XIX. Annex G, Exploit the Cyberspace Domain (AFCyMA Task 5.0) 100

XX. Annex H, Attack the Cyberspace Domain (AFCyMA Task 6.0) 107

XXI. Appendix 1, Concept of Operations for Twenty-Fourth Air Force Cyberspace Operations 112

XXII. Appendix 2, Command & Control and Operations of Cyberspace Forces, 10 Mar 2009, Change 3
113

XXIII. Appendix 3, System Interface Description/System Node Connectivity Description (SV-1/2) 114

XXIV. Appendix 4, Expeditionary Communications and Information (EC&I) Enabling Concept 115

XXV. Appendix 5, Cyberspace Professional Roadmap..... 116

“Cyberspace is critical to today’s fight as well as to the future of US National security. Securing cyberspace is critical to all Joint activities. To achieve this objective, AFSPC must organize, train, and equip cyberspace forces like those of the other domains, for use by Joint Force Commanders.”

General C. Robert Kehler, 2009-2010 Air Force Space Command Strategic Plan (*draft*)

I. Forward

The US faces a strategic environment that is unpredictable and increasingly dangerous. We are a globally networked society increasingly dependent on cyberspace and the cyber domain for essential services. Necessary process controls in manufacturing, public utilities distribution, banking, communications, and national security have shifted to integrated networked systems. Potential adversaries are developing technical capabilities to exploit these vulnerabilities and challenge US military superiority in air, space, and cyberspace. These competitors are fielding sophisticated systems and developing asymmetrical strategies to degrade our capabilities and deny our strategic advantage. These strategies circumvent our core strengths, exploit our weaknesses, and seek to constrain our freedom of action. As the Air Force looks forward, it must understand the contextual realities of the environment in which it operates, including the pressures and obstacles it faces, the opportunities it must seize, and the decisive actions it must take. These realities will define and shape the role of the Air Force and the future of cyberspace operations.

The creation of 24th Air Force (24 AF) under Air Force Space Command (AFSPC) is the first step in consolidating existing Air Force cyber capabilities under a single commander responsible for providing combat-ready forces equipped to conduct sustained operations in and through the cyberspace domain. These forces will be fully integrated with global air and space operations to achieve Combatant Commanders’ (CCDR) mission objectives. By establishing this Component Numbered Air Force (C-NAF), the Air Force improves its warfighting capability and operational effectiveness. Controlling cyberspace is a prerequisite to securing our national infrastructure and effective actions across the range of military operations —securing freedom from attack and enabling freedom to attack. The ability to act decisively throughout cyberspace at the time and “place” of our choosing is mandatory in the 21st Century.

Global Vigilance, Global Reach, and Global Power are the cornerstones of our Air Force. Our Global Vigilance is reflected in the ability to sense and act across cyberspace. Our Global Reach includes the ability to create effects around the earth instantaneously. Our Global Power is generated by the ability to deliver capabilities against any target to create kinetic and non-kinetic effects. Cyberspace is the primary domain for electronic warfare, command and control (C2), communications, surveillance, and reconnaissance and it allows the Air Force to create and execute capabilities across all other warfighting domains – providing reach, speed, stealth, massed effects, and precision regardless of natural or manmade boundaries. In cyberspace, these capabilities enable us to secure our infrastructure, conduct cyberspace operations whenever necessary, and deny, degrade, disrupt, disable, or destroy our adversaries’ military capabilities.

II. Executive Summary

This AFSPC Strategy to Task Plan defines the specific objectives, desired effects, required capabilities, operational tasks, and concepts necessary for the successful stand up of 24 AF and the integration and maturation of cyberspace as an Air Force core competency.

This strategy serves as a complement to Headquarters United States Air Force (HQ USAF) Program Action Directive (PAD) 07-08 Change 3: "Phase I of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces," 20 February 2009, and will shape the development of AFSPC's 24 AF Programming Plan (PPLAN); thereby, reinforcing areas of these plans that are critical to mission success. By quickly assigning and completing the tasks at Annexes A-H, a more effective and efficient stand up of a cyber C-NAF will occur.

The creation of 24 AF is recognition that effective and sustained cyber operations are possible only with trained personnel, hardware and software tools, battle-management rules of engagement, measures of effectiveness, and adequate C2 to perform specialized cyberspace operations. This links directly to the command's strategic vision **to provide the Commander, U.S. Strategic Commander (CDRUSSTRATCOM) and other combatant commanders (CCDR) with compelling, game-changing cyber capabilities to defend and attack in, through, and from cyberspace, integrated across all warfighting domains.** The mission of 24 AF is **to deliver cyberspace superiority through persistent and responsive world-class networks and cyber forces.**

This document contributes to the cyber community by:

- Providing foundational thought for capabilities-based assessment emphasizing cyber integration across the range of military operations.
- Guiding the development of subordinate cyber organizations planning efforts.
- Supporting and focusing Air Force cyber requirements generation.
- Influencing / providing justification for AF cyber resource allocation decisions.
- Providing support for capabilities prioritization.

This Strategy to Task Plan frames critical implementation tasks required for 24 AF stand up. It recommends creation, rewrite, and/or revision of Joint and Service operational, functional, and enabling concepts within the Joint and Service Family of Concepts. Additionally, it outlines the high-level activity tasks based on Air Force Communication Agency's architectural modeling that 24 AF must perform to achieve mission success. These high-level activity tasks, and associated critical actions, fall into eight broad categories, which are expanded upon in annexes A thru H in this document:

1. Annex A, Implementation Tasks, focuses on tasks considered critical to the stand up of 24 AF.
 - Codify relationships and authorities between 24 AF (AFSPC) and AF ISR Agency
 - Develop 24 AF operational concepts that include mission statement, mission sets, and critical operational and enabling capabilities IAW AFI 10-2081
 - Align and Assign 24 AF roles and responsibilities to units and capabilities IAW HQ USAF PAD 07-13

- Finalize Family of Concepts
 - Complete 24 AF Personnel Plan
 - Establish MOAs at designated 24 AF locations
 - Realign AFIOC to AFSPC
 - CONPLAN/Operational Plan Review
 - Exercise & Validate 24 AF Operational Capabilities
2. Annex B, Family of Concepts Tasks, provides the prioritized tasks associated with Joint and Service concept development. These tasks serve as a roadmap to facilitate successful Air Force cyberspace operations.
- Rewrite Global Strike CONOPS
 - Rewrite Space and C4ISR CONOPS
 - Rewrite Global Persistent Attack CONOPS
 - Rewrite Nuclear Response CONOP
 - Rewrite Agile Combat Support CONOPS
 - Rewrite Global Mobility CONOPS
 - Rewrite Homeland Defense and Civil Support CONOPS
 - Write AFSPC Cyber Functional Concept
 - Recommend Joint Staff Rewrite Major Combat Operations JOC
 - Recommend Joint Staff Rewrite Military Support to Stabilization, Security, Transition, and Reconstruction JOC
 - Recommend Joint Staff (AF Lead Service) Update Global Strike JIC
3. Annex C, Perform AF Cyberspace Force Management Tasks, provides a list of tasks which center on building a force requisite to meet the objectives outlined in Section VI. This list of personnel, doctrine, and training tasks are the most critical “Force Management” tasks for standing-up 24 AF and establishing a cyber warrior culture in the Air Force.
- Establish a cyber warrior force development and management program that integrates cyber warriors with the CAF
 - Integrate and elevate cyberspace to the same level as land, sea, air, and space in all AF professional military education curriculum
 - Establish minimum personnel criteria for access to the AF-GIG that is consistent with recruiting and retention processes
 - Define, acquire, and sustain training systems that replicate cyberspace capabilities to train and evaluate individual and shift/team performance in response to cyber incidents
 - Integrate cyberspace events in all headquarters-level exercise and inspection programs to confirm combat readiness
 - Identify DoD-wide cyberspace exercise list
 - Man Cyber Operations Center and Air Force Forces (AFFOR) staffs to initial operating capability (IOC) levels (mid-term)

4. Annex D, Establish AF Cyberspace Domain Tasks, and concentrates on establishing the cyberspace domain to meet the objectives outlined in Section VI. These tasks address issues affecting Joint partnering, information assurance, and electromagnetic frequency de-confliction, and represent the most critical “Establish” tasks for the stand up of 24 AF.
 - Partner with the Joint force and the private sector to identify Air Force cyberspace dependencies and vulnerabilities
 - Increase the current level of information assurance in the AF-GIG
 - Spearhead identification and de-conflict communications and other mission essential electro-magnetic frequency operations
 - Develop transition plan for Air Force Network Operations Center to Cyber Operations Center operations to include migration of Cyber Operations Center to final location (mid-term)

5. Annex E, Operate the AF Cyberspace Domain Tasks, lists tasks which frame 24 AF’s responsibility to operate in the cyberspace domain to meet the objectives outlined in Section VI. These tasks address issues affecting Joint partnering, exercises, commander’s critical information requirements (CCIR), all-source fusion required for cyber situational awareness, and acquisition timeline compression, and represent the most critical “Operate” tasks for the stand up of 24 AF.
 - Establish and develop mutually beneficial relationships with joint partners to facilitate cross-domain operations and freedom of action
 - Test the ability to rapidly respond to attacks and reconstitute cyberspace operations
 - Define Air Force essential elements of information for cyberspace
 - Define specific 24 AF priority intelligence requirements
 - Fuse all-source ISR, as well as AF-GIG and AF-GIG-dependent network status to increase cyberspace situational awareness
 - Work with the Office of the Secretary of Defense to define an acquisition process that can respond to the dynamic nature of the cyberspace domain
 - Define 24 AF operational IOC and full operating capability (FOC) criteria (mid-term)

6. Annex F, Defend the AF Cyberspace Domain Tasks, is associated with defending the cyberspace domain to meet the objectives outlined in Section VI. These tasks address issues affecting joint partnering, continuity of operations, best practice solutions, and exploitation prevention, and represent 24 AF’s most critical “Defend” tasks.
 - Establish response, recovery, and continuity of operations strategies to mitigate risk induced by identified dependencies and vulnerabilities
 - Incorporate global best practice-based solutions and architectures to preserve the effectiveness and survivability of mission-related military and non-military personnel, equipment, facilities, information, and infrastructure
 - Collaborate with joint and interagency partners to develop a Diplomatic, Information, Military and Economic (DIME)-integrated deterrent strategy for cyberspace

- Prevent exploitation of cyberspace systems and harden USAF assets against cyber attacks through the electro-magnetic spectrum
 - Define friendly force response thresholds in Air Force mission-relevant terms
 - Define and publish joint web-based rules of engagement to protect cyberspace capabilities that provide immediate updates to users
7. Annex G, Exploit the AF Cyberspace Domain Tasks, is intended to focus efforts on exploitation activities in the cyberspace domain to meet the objectives outlined in Section VI. These tasks address issues affecting integrated, global C2 operations; Joint and Interagency decision cycle compression; and CONPLAN/OPLAN review and role definition, and represent 24 AF's most critical "Exploit" tasks.
- Integrate the 624 Operations Center into a global, interconnected C2 enterprise
 - Develop AFTTP, memorandums of agreement, and legal processes to facilitate compression of the joint and interagency cyberspace decision-cycle
 - Review all CONPLANS/OPLANS for the integration of military effects through cyberspace
 - Define role(s) and participate in joint and combined exercises as integrated force providers IAW CONPLANS/OPLANS
8. Annex H, Attack the AF Cyberspace Domain Tasks, provides tasks which will strengthen the Air Force's ability to attack in, through, and from the cyberspace domain to meet the objectives outlined in Section VI. These tasks address issues affecting adversary capability neutralization; adversary decision-cycle expansion or misdirection; and asymmetric capabilities-based cyberspace attack and defense acquisition definition, and are considered 24 AF's most critical "Attack" tasks.
- Neutralize adversary operations in cyberspace and develop commensurate capabilities
 - Develop capabilities that expand or redirect/reorient the decision cycle of an adversary
 - Define an asymmetric, capabilities-based defense and attack cyberspace acquisition strategy

Additionally, other documents created to formalize cyberspace aspects affecting the operations of 24 AF are provided as appendices for reference. A description of each document follows:

- Appendix 1, *Concept of Operations for Twenty-Fourth Air Force Cyberspace Operations*, describes the initial capability and function of 24 AF to plan, direct, coordinate, C2, execute and assess cyberspace operations and capabilities in support of Air Force and Joint requirements. These functions are presented in terms of the current missions, functions, and capabilities of the Air Force units being assigned to 24 AF.
- Appendix 2, *Command & Control and Operations of Cyberspace Forces, 10 Mar 2009, Change 3*, further details how 24 AF, in its C-NAF role and from an operating center perspective, will conduct full spectrum offensive and defensive cyber operations. This appendix describes how the 624 Operations Center will fulfill its warfighter responsibilities and how it will C2 cyberspace forces.

- Appendix 3, *System Interface Description/System Node Connectivity Description (SV-1/2)*, presents the architectural depictions of the projected Air Force Cyberspace mission as described by the HQ USAF PAD 07-08 Change 3: “Phase I of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces,” 20 February 2009. It addresses the objective organizational changes that placed the cyberspace mission under the responsibility of AFSPC.
- Appendix 4, *Expeditionary Communications & Information (EC&I) Enabling Concept*, describes how the Air Force provides EC&I capability in support of the Joint Forces Air Component Commander and the AFFOR commander. It is based on the approved SAF/XC EC&I Enabling Concept Document. This enabling concept details the minimum expeditionary communications structure necessary to meet Air and Space Expeditionary Task Force (AETF) Force Module (FM), Theater Information Infrastructure, and direct mission support requirements. Additionally, this document standardizes the vocabulary used to describe EC&I forces.
- Appendix 5, *Cyberspace Professional Roadmap*, provides clear direction for the development of cyberspace forces. It is derived from the Air Force Roadmap for the Development of Air Force Cyberspace Professionals, which establishes a way ahead for the next 10 years. The roadmap provides specific guidance essential to successfully develop new Cyberspace Airmen. It also allows for flexibility, as we develop and better understand the operations and capabilities required to establish, control, and leverage the cyberspace domain. This roadmap considers the challenges presented by the cyberspace domain and charts the developmental path required to produce the Air Force’s Cyberspace Professionals. It formalizes the bridge between strategy and reality, establishing the appropriate sequencing of events and timelines to achieve success.

Controlling cyberspace is a prerequisite to effective operations through the strategic and operational levels of war to secure freedom from attack and to attack. The ability to act decisively throughout cyberspace across the range of military operations is mandatory in the 21st Century. By establishing a C-NAF for this purpose, the Air Force improves its warfighting capability and operational effectiveness. This Strategy to Task Plan supports the successful activation of 24 AF as the Air Force’s cyber warfighter. The guidance contained in this document is authoritative in nature. However, commanders can and must use their judgment in setting priorities based on new unforeseen realities.

III. Assumptions

This AFSPC Strategy to Task Plan is shaped by assumptions which are necessary to enable the commander and his staff to complete an estimate of the situation and to address gaps in knowledge that are critical for the planning process to continue. For planning purposes, subordinate commanders will treat these assumptions as true in the absence of proof to the contrary. These assumptions must be continually reviewed to ensure validity. For this document, the following planning assumptions are necessary to allow for successful completion of the critical actions outlined in this document:

- Commander, AFSPC will assume responsibilities as the Air Force's Designated Approval Authority as assigned by governing authorities as documented in Designated Approval Authority appointment letter.
- CCDRs will identify new mission requirements in response to adversaries' emerging capabilities and will need to leverage technologies available at any given time to respond. Command and control for those missions will require burgeoning technology to support the development of capabilities to stay ahead of the adversary in all situations.
- The AF Network Operations (AFNetOps) Commander will exercise existing authorities to defend the AF GIG. In addition, the AFNetOps Commander will implement Joint Task Force-Global Network Operations (JTF-GNO) guidance.
- 24 AF will have responsibility, as the Air Force component to the joint cyber command, for planning and apportionment of global offensive and defensive cyberspace operations.
- All funding and manpower will continue uninterrupted until all units are transitioned to AFSPC.
- All operations will continue with or without memorandums of agreement, host tenant agreements, or changes in authorities, unless required by law, until all staffs are fully transitioned and adequately manned to accept responsibilities for their assigned missions.
- Current Air Force cyberspace assets supporting Network Operations (NetOps), Network Warfare Operations, and Network Warfare Support will organize and transfer to wings under 24 AF. Additional future AF cyberspace assets may be assigned to 24 AF.
- Air Force cyberspace force presentation to CCDRs is in accordance with HQ USAF PAD 06-09, "Implementation of the Chief of Staff of the Air Force Direction to establish an Air Force Component Organization," 7 November 2006, to support the United States Strategic Command (USSTRATCOM) Cyber Strategy, Cyberspace Concept of Operations (CONOP), and concept plan / operations plans (CONPLANS/OPLANS).
- Unified Command Plan (UCP), dated December 2008, with respect to cyberspace authorities will remain in effect.

IV. Purpose

This AFSPC Strategy to Task Plan will attempt to answer the key strategic questions posed in the Independent Strategic Assessment Group (ISAG) Report, which are provided below along with ISAG's process methodology (Figure 1). This plan defines desired effects, required capabilities, and operational tasks associated with the activation of 24 AF and maturation of cyberspace as an AF core competency. It reflects critical actions required for 24 AF stand up, and outlines an operational concept for cyberspace operations in the new command. Finally, this plan charts the way forward with respect to the development of a professional cyber force.

ISAG – Key Questions a CONOPS Must Answer:

- (What are the) Missions to be accomplished?
- (What are the) Operational Concept or Combatant Commander's intent?
- (What are the) ISR capabilities that are to be used to accomplish the mission(s)?
- (What are the) Engagement capabilities that are to be used to accomplish the mission(s)?
- (What are the) Key forces/organizational units involved in mission execution and their command relationships?
- (What are the) Command and Control Centers to be involved in executing the mission(s)?
- (What are the) Operational tasks required to execute the mission(s) and the Command Centers assigned the tasks?
- (What are the) Information required for the successful execution of each assigned operational task?
- (What are the) Connectivity required between the participating system-of-systems elements to assure information availability for successful execution of each task?
- (What are the) Training tasks?
- (What are the) Mission readiness criteria?



**Source: AFSPC-ISAG Brief, Organizing and Preparing for Cyberspace Operations, 24 Mar 09, v10, DRAFT*

Figure 1 – Building & Sustaining Cyber Forces with Qualified People

This strategy is intended to complement the HQ USAF, PAD 07-08, Change 3: “Phase I of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces” and will shape the development of AFSPC’s 24 AF Programming Plan (PPLAN). By assigning and completing the critical actions identified in this strategy document, a more effective and efficient stand up of 24 AF will occur. This document will contribute to the activation of 24 AF and cyberspace operations by:

- Providing foundational thought for capabilities-based assessment emphasizing cyber integration across the range of military operations.
- Guiding the development of subordinate cyber organizations planning efforts.
- Supporting and focusing Air Force cyber requirements generation.
- Influencing / providing justification for AF cyber resource allocation decisions.
- Providing support for capabilities prioritization.

AFSPC and the new C-NAF will utilize this document to guide the stand up of 24 AF and subsequent efforts to declare initial / full operational capability. Although the guidance contained in this document is authoritative in nature, commanders should exercise their professional judgment in setting priorities.

V. Overview

A. C-NAF (24 AF) Mission and Vision

24 AF will bring together the myriad existing cyber capabilities and diverse cyber skill sets under a single commander. At the same time, 24 AF will allow the Air Force to focus scarce resources on the expansion of existing cyber capabilities and on the creation of new cyber capabilities to fulfill national security objectives across the range of military operations. This links directly to the command's strategic vision **to provide the CDRUSSTRATCOM and other CCDRs with compelling, game-changing cyber capabilities to defend and attack in, through, and from cyberspace, integrated across all warfighting domains.** The mission of 24 AF is **to deliver cyberspace superiority through persistent and responsive world-class networks and cyber forces.** The creation of 24 AF is recognition that effective and sustained cyber operations are possible only with trained personnel, hardware and software tools, battle-management rules of engagement, measures of effectiveness, and adequate C2 to perform specialized cyberspace operations.

B. Commander's Intent

On order 24 AF will generate integrated global cyberspace effects in support of CDR USSTRATCOM's military objectives and other combatant commands' (CCDR) objectives as directed. 24 AF will develop the operational capability to integrate, synchronize and execute cyberspace operations to deter, deny, disrupt, destroy, or defeat threats to US and US-aligned interests across all warfighting domains, throughout all phases of operations, and across the range of military operations. It will foster strong ties with sister service organizations, government agencies, industry and academic institutions to share intelligence, a common strategy, technology and intellectual capital.

C. USSTRATCOM's UCP Assigned Cyber Mission

CDRUSSTRATCOM is responsible for synchronizing planning for cyberspace operations, and will do so in coordination with other CCDRs, the Services, and as directed, appropriate US government agencies¹. CDRUSSTRATCOM's specific UCP responsibilities include:

- (a) Directing Global Information Grid (GIG) operations and defense.
- (b) Planning against designated cyberspace threats.
- (c) Coordinating with other CCDRs and appropriate US government agencies prior to the generation of cyberspace effects that cross areas of responsibility.
- (d) Providing military representation to US national agencies, US commercial entities, and international agencies for matters related to cyberspace, as directed.
- (e) Advocating for cyberspace capabilities.
- (f) Integrating theater security cooperation activities, deployments, and capabilities that support cyberspace operations, in coordination with the geographic combatant commanders, and making priority recommendations to the Secretary.
- (g) Planning operational preparation of the environment (OPE), and as directed, executing OPE or synchronizing execution of OPE in coordination with geographic combatant commanders.
- (h) Executing cyberspace operations, as directed.

D. USJFCOM's UCP Assigned Mission as Joint Force Provider

Effective operations within cyberspace require global expeditionary cyberspace operations and NetOps security to ensure cross-domain freedom of action for the U.S. and its allied forces and to deny that same freedom of action to our adversaries. IAW HQ USAF, PAD 07-08, Change 3, 24 AF will present expeditionary cyberspace capabilities, through Commander, United States Joint Forces Command (CDRUSJFCOM), to CCDRs to extend and establish the cyber domain in support of their military objectives and lines of operations. Appendix D, Expeditionary Communications and Information Enabling Concept, provides an overview of the operational concept for expeditionary cyberspace forces. CDRUSJFCOM's specific responsibilities as the Primary Joint Force Provider for conventional forces are:

- (a) Deploying trained and ready Joint forces and providing operational and intelligence support from assigned forces in response to the requirements of supported CCDRs.
- (b) Identifying and recommending global Joint sourcing solutions to the Chairman, in coordination with the Services and other combatant commanders, from all worldwide forces and capabilities (except designated forces sourced by US Special Forces Command, USSTRATCOM, and US Transportation Command), and supervising the implementation of sourcing decisions.

¹ CCDRs charged with synchronizing planning lead a global collaborative planning process that includes other CCDRs, Services, CSAs, and applicable Defense agencies and Field Activities in support of a designated global mission or campaign plan. The phrase "synchronizing planning" pertains specifically to planning efforts only and does not, by itself, convey authority to execute operations or direct execution of operations.

- (c) Serving as the Department of Defense (DoD) Joint Deployment Process Owner, responsible for maintaining the global capability for rapid and decisive military force power projection and redeployment.

VI. Component-NAF Operations

Achieving its mission alongside its joint partners and within the constraints of the standing national and military objectives, the Air Force has identified three cyberspace requirements: establish/ maintain/ operate/ defend Air Force cyber components; exploit enemy vulnerabilities; and attack enemy networks, systems, peripherals, and infrastructure.² This Strategy to Task Plan integrates ends, ways, and means as a construct to illustrate how 24 AF will meet these requirements. It identifies specific objectives (**ends**) that support the establishment of a C-NAF ready to conduct cyberspace operational tasking in support of CCDRs' mission requirements. It outlines how 24 AF will accomplish these objectives through desired effects (**ways**), and it describes the required capabilities and tasks (**means**) necessary for successful mission execution. A detailed explanation of 24 AF operations and command and control for cyberspace operations is provided in Appendixes A and B of this document.

A. Objectives

To meet the AF cyber requirements 24 AF will achieve the following military objectives:

Reduce vulnerability to cyberspace attacks. 24 AF will support the defense and protection of our critical national infrastructure. The secure function of cyberspace is essential to the US economy and national security. 24 AF will partner with the Joint force and the private sector to identify dependencies and vulnerabilities to develop and implement mitigation strategies.

Ensure freedom of action in cyberspace for US and Allied commanders. Freedom of action includes freedom from attack, as well as freedom to attack. Freedom of action in cyberspace is ensured through defensive operations. The attainment of freedom of action enables successful military operations in other warfighting domains.³

Deter and prevent cyberspace attacks against vital US interests and critical infrastructure. Cyberspace systems and practices will provide robust continuity of operations capability such that potential adversaries realize attacks on US or US-aligned interests are futile or exact a premium to achieve success.⁴

Ensure combat readiness meets Combatant Commander warfighting requirements. Realistic training is essential to proficiency and readiness of cyberspace professionals. Simulators and wargaming systems should replicate cyberspace capabilities and their effects on target systems within the domain. Training and evaluation programs along with range assets should create and integrate realistic peacetime and wartime scenarios to the fullest extent possible. To improve readiness, cyberspace forces should

² Program Action Directive 07-08, Change 3, page 5.

³ AFDD 2-11, 31 November 2008, pages 8-21.

⁴ Ibid, page 23.

participate as full partners with air and space assets in large-scale joint and combined exercises to provide realistic training for in-theater and deployable Air Force forces.⁵

Establish cyberspace defense plans that outline strategies and rules of engagement to protect cyberspace capabilities. Defensive measures should account for rapid decision cycle requirements to respond adequately to attacks. The reaction time required in the cyberspace domain is difficult to achieve in the domains of land, sea, air, and space. Hence, rules of engagement should be crafted with the concept of speed appropriate for the domain.⁶

Rapidly respond to attacks and reconstitute cyberspace operations. 24 AF will maintain capabilities in the physical and cyberspace environments. This requires system redundancy, self-healing, and automatic attack mitigation strategies. 24 AF will devise strategies to preserve the effectiveness and survivability of mission-related military and non-military personnel, equipment, facilities, information, and infrastructure.

Defeat adversaries operating through cyberspace. Forces must be able to deter and defeat threats to the cyber domain and cyberspace operations while remaining postured to support homeland security, critical infrastructure protection, and civil support operations. 24 AF will constantly evaluate and modernize network security operations to ensure protective measures adequately counter the evolving cyber threat, through integration of active and passive defenses.

Integrate cyberspace power into the full range of global and theater effects. 24 AF will provide scientific, technological, and operational leadership to integrate cyberspace capabilities into Joint and interagency operations. 24 AF will also integrate network-centric strategies in system acquisition, operational planning, and mission execution. To achieve this integration, 24 AF will integrate the 624 Operations Center into a global, interconnected C2 enterprise.

Establish persistent, comprehensive cyber situational awareness and enhance C2 to de-conflict operations and manage cyberspace resources. The vastness, complexity, volatility, and rapid evolution of cyberspace places a premium on continuous intelligence preparation of the operational environment. This is critical to effective defensive and offensive operations. Cyber situational awareness combines information concerning friendly activities and information derived from ongoing intelligence, surveillance, and reconnaissance (ISR) operations to find, fix, track, target, engage, and assess adversaries operating in cyberspace.⁷

Direct actions based on a commander's chosen course of action. 24 AF will provide effective C2 over cyberspace forces in support of Air Force and Joint operations to meet time critical needs and evolving conditions. To condense the decision cycle, 24 AF will collaborate with external partners through memorandums of agreement and other policy arrangements.

⁵ Ibid, page 53-54.

⁶ Ibid, page 8.

⁷ AFDD 2-11, pages 9 and 17.

Improve cyberspace safety, surety and sustainment. 24 AF will assess and balance the risks associated with communications infrastructure to ensure the ability to protect and dynamically reconstitute its capability.

Establish effective force development and management programs. A robust force development program is essential to ensure an effective and ready force to conduct the wide range of cyberspace operations and missions. 24 AF, in collaboration with AFSPC, will lead a robust force development program that includes a defined cyber career path, diverse opportunities for skill enhancement, training and exercises, education preparation, and strategies to ensure force stability and support. A career path for cyber warriors defines and sharpens the desired force structure to ensure 24 AF possesses the necessary personnel to perform its missions and conduct effective operations.

Determine personnel and training requirements to develop an intellectual foundation for cyberspace knowledge. 24 AF will collaborate with industry and academia to provide realistic training and enhanced education in an effort to ensure cyberspace warriors are familiar with the latest cyber technologies and applications. 24 AF will also provide enhanced skills training and education preparation to improve operational performance, make effective use of funding, and minimize the time required to train and deploy its forces. They will expand the training and education curriculum for cyberspace core competencies to improve technical skills and increase operational effectiveness.⁸

Develop, deliver, and conduct training, evaluation, exercise and inspection programs to ensure combat readiness. Realistic training is essential to proficiency and readiness of cyberspace professionals. Exercises train individuals, units, and staffs in the necessary skills and tools for cyberspace operations and ensure staffs can plan, control, and support such operations. To improve readiness, cyberspace forces will participate as full partners with air and space assets in large-scale Joint, Service, and combined exercises to provide realistic training for in-theater and deployable Air Force forces.⁹

Ensure program requirements are clearly documented, approved, and controlled to meet/exceed threshold performance, cost, and schedule parameters. Requirements generation, request for proposals, development, testing, fielding and sustainment processes must keep pace with the rate of information technology change and the unique requirements of the cyber mission. Rapid acquisition programs that provide quick reaction solutions are a key enabling capability across the cyber domain. These processes must also remain responsive to adversary asymmetries. 24 AF, with support of AFSPC, will develop processes designed to speed approval of urgent requirements. These processes will seek to move normal requirements through the approval process as quickly as possible.¹⁰

Implement a prioritized investment strategy with supporting resources. 24 AF, in partnership with AFSPC, will establish a capabilities-based resource allocation and decision-making process with effective corporate management and a rigorous analytical foundation. 24 AF will pursue a deliberate process development strategy to create a tailored resource allocation process. The process will be supported by

⁸ Ibid, pages 41-44.

⁹ AFDD 2-11, pages 53-54.

¹⁰ Concept of Operations for Twenty-Fourth Air Force Cyberspace Operations, page 14.

a robust strategic planning process that incorporates Air Force, Joint, and CCDR objectives to seamlessly interface with the Planning, Programming, Budgeting and Execution (PPBE) process.

Deliver new capability as promised. 24 AF, in cooperation with AFSPC, will partner with the acquisition community to develop and utilize abbreviated and accelerated processes coupled with rapid prototyping and spiral development to ensure the warfighter receives critical and timely systems and equipment. 24 AF will co-locate personnel with the Air Force Research Lab and other Air Force agencies to speak with a single voice in support of the cyber acquisition process.

Support & employ measures to preserve a healthy techno-industrial base and work force. 24 AF will support DoD efforts to develop and implement plans to mitigate risks to relevant portions of the defense industrial base. 24 AF will map interdependencies within the Air Force portion of the defense industrial base, analyze industry risk and exposure to potential adversary operations, and develop defensive operations to improve protection, increase survivability, and reduce risk.¹¹

B. Desired Effects

A set of desired effects contributes to the conditions necessary to achieve military objectives. Cyber effects are outcomes, events, or consequences resulting from specific cyberspace operations, which contribute directly to the attainment of the CCDR's military objectives. 24 AF will generate the following cyber effects in support of the military objectives articulated above:

Establish, maintain, and control the cyberspace domain. Effective 24 AF operations in cyberspace will require global expeditionary component cyberspace and network secure operations capabilities and forces to ensure cross-domain freedom of action for the U.S. and allied forces.¹²

Exploit adversary vulnerabilities. 24 AF will provide C2 to synchronize cross-domain operations and de-conflict friendly use of cyberspace to preserve appropriate command authorities for global and theater-level cyberspace operations. The integrated exploitation of adversary capabilities and vulnerabilities will further enable C2 of Air Force cyberspace forces.¹³

Provide forces to attack adversary structures. 24 AF forces will conduct offensive operations to achieve operational freedom of action through cyberspace. This includes further delivery of cross-domain effects through cyberspace force enhancement and the conduct of cyberspace support operations.¹⁴

Operate and defend AF cyberspace components. 24 AF will leverage Air Force NetOps to deny an adversary the ability to diminish Air Force operations in cyberspace.¹⁵

Establish cyber situational awareness. 24 AF will create persistent situational awareness through the integrated application of sensors, intelligence collection, exploitation, fusion, analysis, and production.

¹¹ Ibid, page 24.

¹² Concept of Operations for Twenty-Fourth Air Force Cyberspace Operations, page 10.

¹³ Ibid.

¹⁴ Ibid, pages 10-11.

¹⁵ Ibid, page 11.

Cyber situational awareness provides decision superiority to the US military across the network environment through visualization, planning, and decision tools that compress the warfighter's decision cycle.

Compress the warfighter decision cycle through an integrated, global C2 architecture. 24 AF will expand situational awareness to network activities, including potential criminal, military, and terrorist activity on the Internet. 24 AF will provide continuous, accurate, actionable intelligence on all forces, actors, and conditions capable of influencing the battlespace. These combinations of activities provide flexible situational awareness tailored to the warfighter. The resulting capability produces timely, relevant, persistent, accessible, and reliable intelligence in order to empower effective decision-making by commanders.

C. Required Capabilities

The essence of capabilities-based planning is to evaluate the interaction between capabilities a potential adversary could employ and the capabilities that could be available to Air Force forces.¹⁶ To operate effectively in cyberspace, networked components must first be established and then maintained. The System Interface Description/System Node Connectivity Description provided at Appendix C provides a high-level overview of the systems necessary to support Air Force cyberspace operations. Once established, critical portions of cyberspace must be controlled through offensive and/or defensive operations.¹⁷ Gaining and maintaining access is a critical first step to achieving effects in other domains and countering adversary use of cyberspace.¹⁸

Establish access. Effective operations within cyberspace will require global unfettered access to ensure cross-domain freedom of action. Access and infrastructure is provided at the base-level by local communication squadrons in conjunction with the Air Force Network Integration Center (formerly AF Communications Agency), and the host Major Command (MAJCOM). However, once local organizations are connected, C2 is provided by 24 AF.¹⁹ Network Attack (NetA) capabilities will be entirely dependent on access to the target network. This will require mechanisms specifically designed for the purpose of providing or enabling that access.²⁰

Conduct Network Defense. Network Defense (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.²¹ The Commander, 24 AF will require the capability to conduct NetD operations as Commander of Air Force Forces to JTF-GNO.²² Force presentation for NetD will be

¹⁶ Quadrennial Defense Review Report, 6 February, 2006, page 4.

¹⁷ AFDD 2-11, page 13.

¹⁸ Ibid, page 21.

¹⁹ 24AF CONOPS, page 12.

²⁰ 24AF CONOPS, page 13.

²¹ AFDD 1-2, 11 January 2007, pages 58-59.

²² Ibid, page 5.

through the 624 Operations Center to JTF-GNO. The C2 of Air Force NetD will be conducted by the 624 Operations Center.²³

Conduct Network Warfare Support. – 24 AF will require the capability to deliver Network Warfare Support activities. These activities will be tasked by or under direct control of an operational commander, and will include the capability to search for, intercept, identify, and locate or localize sources of access and vulnerability for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations.²⁴

Conduct Network Attack. Network Attack (NetA) is the employment of network-based capabilities to destroy, deceive, disrupt, corrupt, or usurp information resident in or transiting through networks. Networks include telephone and data service networks. Network Attack capabilities are entirely dependent on access to the target network. The purpose of NetA is to increase the decision cycle of the enemy thereby providing commanders with strategic and operational advantages.²⁵ Network Attack Forces will be requested through the 624 Operations Center but will be OPCON/TACON by Joint Force Component Command, Network Warfare (JFCC-NW). Force presentation for NetA will be through the 624 Operations Center to JFCC-NW. However, JFCC-NW will conduct C2 of AF NetA forces.²⁶

Conduct Network Operations. 24 AF will provide integrated Network Operations (NetOps) and network warfare operation capabilities to CCDRs in support of objectives across the full range of military operations. To do this, 24 AF will provide operationally ready forces able to deploy quickly and employ globally.²⁷ The 624 Operations Center will plan, direct, and provide C2 of NetOps across the AF-GIG under the authority given to the Air Force Network Operations Commander.²⁸

Perform network maintenance. To accomplish the 24 AF's mission through all phases of military operations, numerous cyber capabilities will be required. These include, but are not limited to, the ability to establish access and perform network maintenance.²⁹ Network maintenance consists of organizations, procedures, and functionalities to plan, administer, and monitor Air Force networks in support of operations and to respond to threats, power outages, and other operational impacts. It includes the continuous oversight and management of Air Force-wide networks. Maintenance of the cyber domain is inextricably linked to defense and often employs the same units, personnel, and equipment.³⁰

Establish and maintain cyber situational awareness Cyber situational awareness is the global visibility of computer networks across the electro-magnetic spectrum and the forces, actors, and conditions capable of influencing the cyberspace domain and cyberspace operations. This requires continuous,

²³ Ibid, page 19.

²⁴ Ibid, pages 12-13.

²⁵ Ibid, page 13.

²⁶ Ibid, page 19.

²⁷ Ibid, page 5.

²⁸ Ibid, page 11.

²⁹ Ibid, page 5.

³⁰ Ibid.

near real-time, non-personnel intensive, assessments, and status reporting of all blue, red, and gray cyberspace operational capabilities. This capability will be provided by 24 AF and performed by assigned 67 Network Warfare Wing cyber operators.³¹

Conduct frequency management. This includes requesting, recording, de-confliction and authorization to use frequencies coupled with monitoring and interference resolution processes. Air Force Space Command will provide this capability.³²

Educate and train forces. The ability to provide cyberspace warriors to the 24 AF mission is critical. The ability to maintain a training throughput to ensure 24 AF manpower positions are fully staffed is essential. The implementation and completion of tasks outlined in the Roadmap for Development of Cyberspace Professionals (Appendix D) will ensure fully educated and trained Air Force personnel are available to execute the 24 AF mission. Air Education and Training Command, AFSPC, and 24 AF will share responsibility for this capability.³³

Acquire and sustain cyber capabilities. Requirements generation, request for proposals, development, testing, fielding and sustainment processes must keep pace with the rate of information technology change and the unique requirements of the cyberspace mission. These processes must remain responsive to adversary asymmetries. Cyberspace acquisition strategy and delivery capabilities will enable 24 AF to leverage Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) products to ensure Air Force weapons systems dominate in cyberspace. Rapid acquisition programs that provide quick reaction solutions will be a key enabling capability across the cyberspace domain. The Air Force acquisition community will provide this enabling capability in coordination with AFSPC.³⁴

D. Cyber Tasks and Critical Actions

The Air Force Cyber Mission Area (AFCyMA) tasks and critical actions are derived from an analysis of the C-NAF objectives, desired effects, and required capabilities, and the high-level activity modeling completed by AFCA. A decomposition of each high-level AFCyMA task is provided in Annexes C-H. AFCA's IT Infrastructure Architecture Version 3.0 (Draft) provides a more detailed look at each of these high-level tasks associated with 24 AF. The critical actions identified below are associated with the activation and stand up of 24 AF. These actions are mapped to the appropriate AFCyMA task(s), parenthetically annotated following each bulleted critical action. The accomplishment of these actions is critical to successful 24 AF stand up and subsequent cyberspace operations.

Perform AF Cyberspace Force Management (Annex C, AFCyMA Task 1.0)

- Establish a cyber warrior force development and management program that integrates cyber warriors with the CAF. (1.0)

³¹ Ibid.

³² Ibid.

³³ Ibid.

³⁴ Ibid.

- Integrate and elevate cyberspace to the same level as land, sea, air, and space in all AF professional military education curriculum. (1.2.3)
- Establish minimum personnel criteria for access to the AF-GIG that is consistent with recruiting and retention processes. (1.2.1.1, 1.2.1.4, 1.4.1.1.4, 1.4.2.1.1)
- Define, acquire, and sustain training systems that replicate cyberspace capabilities to train and evaluate individual and shift/team performance in response to cyber incidents. (1.2.2.3, 1.3.1.3, 1.3.2)
- Integrate cyberspace events in all headquarters-level exercise and inspection programs to confirm combat readiness. (1.2.2.1, 1.2.4, 1.2.5)
- Man Cyber Operations Center and AFFOR staffs to IOC levels (mid-term). (1.1, 1.2)

Establish AF Cyberspace Domain (Annex D, AFCyMA Task 2.0)

- Partner with the joint force and the private sector to identify Air Force cyberspace dependencies and vulnerabilities. (4.1.1.1, 3.9)
- Increase the current level of information assurance in the AF-GIG. (4.2, 2.6)
- Spearhead identification and de-conflict communications and other mission essential electromagnetic frequency operations. (2.4)
- Develop transition plan for Air Force Network Operations Center to Cyber Operations Center operations to include migration of Cyber Operations Center to final location (mid-term). (2.2, 2.4, 2.5)

Operate the AF Cyberspace Domain (Annex E, AFCyMA Task 3.0)

- Establish and develop mutually beneficial relationships with joint partners to facilitate cross-domain operations and freedom of action. (3.5.5)
- Test the ability to rapidly respond to attacks and reconstitute cyberspace operations. (1.2.4)
- Define Air Force essential elements of information for cyberspace. (3.5.1)
- Define specific 24 AF priority intelligence requirements. (3.2.2.2)
- Fuse all-source ISR, as well as AF-GIG and AF-GIG-dependent network status to increase cyber situational awareness. (2.2.2.1.1, 4.1.1.1, 3.2)
- Work with the Office of the Secretary of Defense to define an acquisition process that can respond to the dynamic nature of the cyberspace domain. (1.3.1.2.3)
- Define 24 AF operational IOC and FOC criteria (mid-term) (3.1, 3.2, 3.3, 3.4, 3.5)

Defend the AF Cyberspace Domain (Annex F, AFCyMA Task 4.0)

- Establish response, recovery, and continuity of operations strategies to mitigate risk induced by identified dependencies and vulnerabilities. (4.4.3.4, 4.1.3.2, 4.3.2.1.2.2.4)
- Incorporate global best practice-based solutions and architectures to preserve the effectiveness and survivability of mission-related military and non-military personnel, equipment, facilities, information, and infrastructure. (1.3, 1.4)
- Collaborate with Joint and interagency partners to develop a DIME-integrated deterrent strategy for cyberspace. (4.1.1)
- Prevent exploitation of cyberspace systems and harden USAF assets against cyber attacks through the electro-magnetic spectrum. (4.4)
- Define friendly force response thresholds in Air Force mission-relevant terms. (4.1.3)
- Define and publish joint web-based rules of engagement to protect cyberspace capabilities that provide immediate updates to users. (4.2.1)

Exploit the Cyberspace Domain (Annex G, AFCyMA Task 5.0)

- Integrate the 624 Operations Center into a global, interconnected C2 enterprise. (3.3)
- Develop AFTTP, memorandums of agreement, and legal processes to facilitate compression of the Joint and interagency cyberspace decision cycle. (5.1.2, 5.1.3, 5.2.2)
- Review all CONPLANS/OPLANS for the integration of military effects through cyberspace. (5.2.3, 5.2.5, 3.3a)
- Define role(s) and participate in Joint and combined exercises as integrated force providers IAW CONPLANS/OPLANS. (5.2.3, 5.2.5, 3.3a, 4.4)

Attack the Cyberspace Domain (Annex H, AFCyMA Task 6.0)

- Neutralize adversary operations in cyberspace and develop commensurate capabilities. (6.1.6, 1.3.1.2)
- Develop capabilities that expand or redirect/reorient the decision cycle of an adversary. (5.1, 5.2)
- Define an asymmetric, capabilities-based defense and attack cyberspace acquisition strategy. (1.3.1)

VII. Capability Development Considerations

AFSPC and 24 AF must have a capabilities-based analytic process to develop and support capabilities that enable the command to successfully organize, train, equip and advocate for warfighting capabilities, meet CCDRs' mission requirements, and respond to the high-speed lifecycle requirements needed to operate effectively in the cyber domain. AFSPC must run its analysis process at a pace that, at a minimum, matches the constant changes in the operational environment, and better still, is able to exceed the pace at which potential enemies adjust.

Additionally, AFSPC must identify, allocate for, and field highly complex mission processes and systems that are necessary to the cyber mission. These processes and missions are best addressed in a coherent, end-to-end methodology. The capability development process must be founded in architectures, and be designed to outline and execute the complex tasks required for accomplishing the three major steps in the analytic process: What needs to be accomplished?; How well is it being done?; and How best to manage the operational risk? Various directorates within AFSPC and 24 AF are responsible for answering these questions. This approach must provide a traceable, repeatable, and defensible process that spans the entire spectrum of the AFSPC Capability Teams and its corporate process, including strategic vision and strategic goals; planning; requirements and prioritization; programming; budgeting; enactment and execution. Official USAF architectures will provide a solid, operator-approved foundation for analysis, thus making it critical to maintain existing architectures, as well as a prioritized schedule.

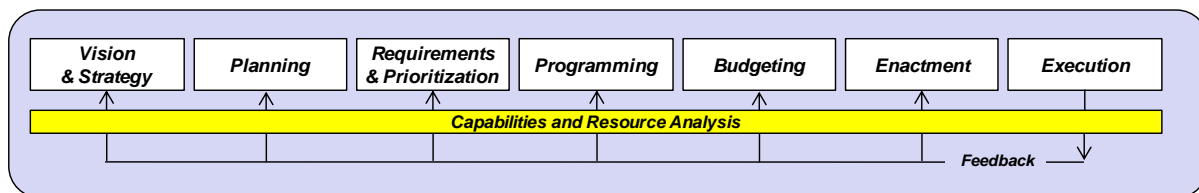


Figure 2 – Analysis Role in Portfolio Management

Given the current and emerging fiscal realities, i.e., the CSAF's focus on aircraft recapitalization; DoD's need to support the Global War on Terror; and the new Administration's budget priorities, AFSPC must secure scarce resourcing dollars during the Air Force Corporate Structure's PPBE cycle. A clearly articulated and responsive process for capability development that reflects operational changes and fiscal reality allows AFSPC to base programming requirements on a compelling foundation. Cyber warfighting capabilities and its specific programs must be used to effectively influence the HQ USAF Capabilities Review and Risk Assessment (CRRRA), the Annual Planning and Programming Guidance, and the biennial Program Objective Memorandum (POM).

The CRRRA process examines and assesses the proficiency and sufficiency of Air Force capability levels vis-à-vis specific warfighting effects. The AF CONOPS articulate the capabilities required to achieve those effects and inform Air Staff and MAJCOM senior leadership on the Air Force vision for capabilities development. They describe key Air Force mission areas and/or functional areas for enabling desired joint warfighting effects in accordance with national, joint, and service guidance.

The specific effects and capabilities outlined in the AF CONOPS provide the conceptual foundation for the CRRRA and the Air Force capabilities-based planning process.³⁵ Given their weight on the budgeting process, a single cyber advocate/champion within the CONOPS Champions (AF/A5XC) and AF/A8P (programmers) divisions would improve cyber's representation on the Air Staff.

A. Capabilities Review and Risk Assessment Incorporation

The first step to gaining advocacy on the Air Staff is to identify the Capability Champion(s) responsible for integrating cyber capabilities into the CRRRA and CONOPS documentation. There is a need to have both the support and operational warfighting roles of cyber capabilities represented. This will require significant operational background in order to accurately integrate cyber capabilities into all domains of the warfighting arena.

B. Inject AF Cyber Equities and Input into JCIDS Process

Once cyber capabilities are fully instantiated and integrated into the CRRRA process, the Air Force can utilize this single Air Staff voice generated from AF/A5XC to have their requirements carried forward from AF/A5XS to the Joint Staff to update or rewrite those Joint concepts lacking any appreciable cyber discussion. Section IX and Annex B outlines those concepts recommended for rewrite due to their insufficient incorporation cyberspace operations.

C. Determine Appropriate Panel for POM

Not only will cyber capabilities need to be represented by a Capability Champion, but a single programming voice should be identified to consolidate and advocate for the cyber portfolio across DOTMLPF in the Air Force POM.

VIII. Key Cyber Relationships

Cyberspace is not the exclusive domain of the US military alone, nor is the military the sole owner/operator of the cyber infrastructure; it is shared with many interagency entities, private industry, and private citizens around the globe. While the military is dependent upon cyberspace for conducting critical activities across the full range of military operations,³⁶ it is private industry that owns the preponderance of cyber infrastructure the US uses to conduct those activities. Thus, relationships between the military and government and the private sector should be examined and more fully explored to cohesively maintain freedom of maneuver in cyberspace. The following are the key relationships the Cyber NAF should foster to achieve cyber security and other cyberspace operations' goals outlined in national strategies.

³⁵ Ibid., page 2

³⁶ There are convincing arguments that the US military cannot operate without the use of cyberspace services, such as information-sharing, collaboration, and e-mail; *Report of the Defense Science Board, 2007 Summer Study: Challenges to Military Operations in Support of US Interests (CMO)*, December 2008, pages 43-44.

A. Service and Joint Partners and Relationships

At the service level, 24 AF is the lead entity for cyberspace operations within the US Air Force, sharing some functions with other agencies at Headquarters AFSPC.³⁷ Almost all cyber issues within the Air Force will be handled by 24 AF or AFSPC, which will guarantee a high level of coordination between these two organizations. For example, 24 AF will plan with and provide requirements to AFSPC; they will cooperate with the Air Force Office of Special Investigation for cyber incident investigation; information system configuration schemes will be coordinated with the Electronic Systems Command; and the Air Force Information Warfare Center (a wing under 24 AF) is responsible for coordinating information operations activities across the Air Force. By including IO in addition to cyberspace operations, this realignment provides 24 AF with an expanded mission focus.³⁸ Most of the relationships between 24 AF and the rest of the Air Force are detailed in HQ USAF PAD 07-08 and the associated PPLANs being developed to implement the stand up of the Air Force's Cyber NAF.³⁹

At the Joint level, 24 AF will conduct planning with USSTRATCOM's J51 shop in order to present cyber forces to CCDRs through two other USSTRATCOM organizations: JFCC NW and JTF-GNO. 24 AF will present cyber attack and exploit forces to JFCC-NW and cyber defense forces to JTF-GNO. There are also several NetOps activities 24 AF will coordinate with JTF-GNO: operation, maintenance, and protection of the Air Force's allocated portion of the GIG; Air Force Information Assurance; and Air Force Network Management.

B. Interagency Partners and Relationships

Twenty-Fourth Air Force cannot conduct its operations exclusively with only DoD partners; it must interface with interagency and private sector partners. Because of the close relationship between the National Security Agency, JFCC-NW, JTF-GNO, and the Defense Information Security Agency, 24 AF must forge core relationships with an interagency focus. Although, the interagency level can address all aspects of cyberspace, a majority of the activities will focus on cyber security – the area in which the private sector is primarily concerned. Because the interagency level can link the DoD with the rest of the world, it is recommended 24 AF's relationship with its interagency partners be as open and cooperative as possible. The following discussion provides examples of the types of interagency activities in which 24 AF should participate and/or continue.

24 AF efforts at the interagency level are critical to successful cyber security. Currently, no one agency oversees the protection of all DoD domains. Additionally, there is no single organization managing all cyber incidents. The response to cyber incidents may be impeded by this lack of centralized control.⁴⁰

³⁷ For example, the new Air Force Network Integration Center (formerly the Air Force Communications Agency) will be a MAJCOM-level office handling many communications issues for the Air Force (communication and information system architecture and hardware); *Air Force Program Action Directive (AFPAD) 07-08, Change 3*, 20 February 2009, page 8.

³⁸ *AFPAD 07-08*, pages 19-20; the 23d IOS manages TTPs for IO for the Air Force; the 39th IOS teaches IO and Network Warfare qualification courses.

³⁹ *Ibid.*, page 8; PPLANs were being written at the time this document was delivered.

⁴⁰ *CMO*, page 329; this chapter is devoted to cyber warfare and describes perceived weaknesses in how cyber security is executed.

Cyber incidents can be divided into five phases or activities: reporting, response, mitigation, investigation, and recovery. There are multiple agencies that 24 AF must partner with to perform these activities.

The primary agency for cyber coordination is the Department of Homeland Security (DHS). Through its affiliation with JTF-GNO, 24 AF will assist in managing national and civil cyber incidents with DHS departments. Coordination for attack indications and warnings and incident mitigation is the responsibility of the 33 Network Warfare Squadron and its long-standing relationship (as the Air Force Computer Emergency Response Team) with the United States Computer Emergency Readiness Team (operated by DHS' National Cyber security Division). Additionally, 24 AF will participate in the community of interest within the Information Technology Security Sector Area and its Information Sharing and Analysis Center. 24 AF should also participate in the Forum for Incident Response and Security Teams. Finally, the DHS sponsors Cyber Storm, a national-level cyber security exercise in which 24 AF has and should continue to participate. With so much activity centered within DHS, this relationship should be one of the strongest interagency partnerships 24 AF maintains.⁴¹

There is also considerable cooperation with the National Security Agency; this relationship is well-established.⁴² The NSA/Central Security Service's National Threat Operations Center provides attack indications and warning and threat analysis to customers. The Intelligence Community Incident Response Center protects Top Secret classified networks and NSA's Information Assurance Division oversees the national program.

For reporting cyber incidents considered to have a national impact, 24 AF should work with two interagency partners. First, the DoD Cyber Crime Center is a clearinghouse for reporting and handling malicious attacks against the military. Incident response can be coordinated through the Crime Center's Joint Inter Agency Cyber Task Force. For incidents affecting the highest levels of government, the US Secret Service becomes involved through its Electronic Crimes Task Force. Cooperative relationships between entities should enhance the attribution process, which is considered an impediment to launching timely response activities.⁴³

The FBI is often one of the first agencies private industry contacts to report and request investigation of cyber crime. The Cyber Incident Response Group within the FBI handles these requests and often turns to the private sector and/or the military for additional resources, such as subject matter expertise and forensic assistance during its investigations.

Finally another avenue for Joint and interagency coordination is in exercises, such as BULWARK DEFENDER, POSITIVE RESPONSE, CYBER STORM, and the National Level Exercise. Greater Joint and IA

⁴¹ There is doubt about whether DHS should be the Federal cyber mediator and if it can adequately execute this task; *Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission for the 44th Presidency (SC 44)*, December 2008, page 34.

⁴² CMO, page 329; 24 AF has a close working relationship with NSA since many of its members work for JFCC NW, co-located with the agency. A similar relationship exists with the Defense Information Security Agency and JTF-GNO.

⁴³ *Ibid.*, page 25; CMO, page 340.

participation in exercises has been encouraged, especially in the wake of 9/11 events.⁴⁴ The level of cyber-specific “play” in military exercises has steadily increased in the last five years. Some exercises have seen an increase in participation from non-government organizations; these partnerships should be expanded and strengthened.

C. Public-Private Partnerships and Relationships

In cyberspace, the paradox exists that DoD and the private sector are dependent upon each other for mutual protection. The private sector relies on DoD to defend the nation including its national cyberspace, especially since many attacks originate from outside the US.⁴⁵ DoD, however, does not own the infrastructure and must rely on the private sector for the services it uses to conduct day-to-day business. Often, DoD may not mitigate potential threats because of US citizens’ privacy oversight. These factors create a situation that is improved if government and industry had partnerships to benefit each other.⁴⁶

Research suggests one way to reduce the risk of cyber attacks is through the Partnership With Industry program. Partnership With Industry activities are used to protect Sensitive But Unclassified data on Cleared Defense Contractor networks and offer a venue for liaising with the Critical Infrastructure Partnership Advisory Council for incident management. These relationships and other public-private partnerships should be open and flexible with an air of mutual trust.

D. Partnership Summary

Table 1 provides a different visualization with respect to the question of required partnerships and relationships. The organizations with which 24 AF will interface are the same (i.e., Interagency, Private Sector, etc.); however, functional bins were added to describe the types of activities these partnerships should focus.

Cyberspace is a global domain connecting a wide variety of users – individual citizens, governments, terrorist organizations, criminal entities, etc. can make instantaneous connections. Because it does not nor cannot control the massive cyber infrastructure, the military must form effective partnerships. The nature of these relationships is primarily protective, but may also involve attack planning and collaboration. Perhaps more than any of other Air Force Numbered Air Forces, 24 AF will need to cultivate partnerships across a wide array of Air Force, sister service, Joint, interagency, and the private sector partners.

⁴⁴ *The National Response Framework*, January 2008; pages 9-31.

⁴⁵ *SC 44*, page 15.

⁴⁶ *SC 44*, pages 43-48.

Table 1 – 24 AF Partnerships by Function

	AFSPC	Air Force	Joint	Interagency	Private Sector
Warfighting – present forces, incident management (report/ respond/ mitigate/ investigate/ recover)			X	X	
Operations – NetOps, network management, C2/ integration, info assurance, info-sharing		X	X		
Staff Support – planning, training, exercises, manning, stan/eval, strategic communication, administration, finance, acquisition	X		X		
Mission Support – sustaining, maintaining, analysis, assessment, reach-back, intelligence, review	X	X	X	X	X

Notes:

AFSPC: Air Force Space Command distinct as the Lead MAJCOM for Cyber

Air Force: not only Big Blue, but the rest of the service

Joint: JFCC NW, JTF-GNO, and the CCDRs

IA: DHS, FBI, NSA, DISA, others

Private Sector: the business world or non-governmental agencies

IX. JOpsC Analysis/Concept Integration

A review of the Family of Concepts from Joint Concepts to Air Force level concepts identified a need to update several concept documents to reflect the current roles, missions, and definitions for cyber and cyberspace operations. This is largely due to the rate of change vis-à-vis the emerging role of cyberspace operations within DoD and the lack of cyber / cyberspace related language in these documents.

A. Concept Analysis and Shortfall Determination

In support of this Strategy to Task Plan, 44 concept documents, both classified and unclassified were examined for their handling of cyber and cyberspace operations. Most of the Joint documents and all the USAF concept documents require some degree of updating to reflect current Joint Publication 1-02 definitions. Additionally, several concepts require a full rewrite due to the limited or non-existent discussion of cyberspace operations.

B. Gap Determination

First and foremost the Air Force must develop a service level “Cyber Functional Concept” to guide Air Force cyber capability development and experimentation. An intellectually sound functional concept establishes a common framework for thinking about future cyberspace operations; provide a conceptual

foundation for subordinate Air Force concepts; and motivates and frames the study, experimentation, and evaluation of future cyber concepts and capabilities. The tasks identified in Section VI.d and Appendix B provides a starting point to frame the dialogue regarding the critical elements of an effective Air Force Cyber Functional Concept.

C. Concept Prioritization

As stated, most Joint and Service documents require some degree of rewrite in order to incorporate additional cyberspace operational concepts. The prioritized list at Table 2 is provided to guide efforts to update and integrate cyber into Joint and Service operational concepts. Documents are prioritized based on impact and perceived operational need. Annex B of this document contains the prioritized list of Concept Tasks.

Table 2 – Family of Concepts Update List

<u>Documents</u>	<u>Action</u>	<u>Owner</u>	<u>Estimated Revision Date</u>
AF CONOPS			
Global Strike	Rewrite	ACC	TBD
Space and C4ISR	Rewrite	AFSPC	TBD
Global Persistent Attack	Rewrite	ACC	TBD
Nuclear Response	Rewrite	ACC	TBD
Agile Combat Support	Rewrite	AFMC, HAF/A4/7	TBD
Global Mobility	Rewrite	AMC	TBD
Homeland Defense and Civil Support	Rewrite	ACC	TBD
AFSPC Cyber Functional Concept (New)	Write	AFSPC	ASAP
JOCs			
DoD Homeland Security and Civil Support	Update	J52/NORTHCOM	Currently under revision
Military Contributions to Cooperative Security	Update	JFCOM/EUCOM	Summer '09
Deterrence Operation	Rewrite	STRATCOM	Summer '09
Military Support to Stabilization, Security, Transition, and Reconstruction Operations	Rewrite	JFCOM	Summer '09
MCO	Rewrite	JFCOM	Summer '09
Irregular Warfare	Rewrite	SOCOM/USMC	Currently under revision
JFCs¹			
Training Joint Functional Concept	Rewrite	JS/J7	
C2	Rewrite	JS/J7	
Net-Centric Environment	Rewrite	JS/J7	
Force Management	Rewrite	JS/J7	
Protection	Rewrite	JS/J7	
Force Application	Rewrite	JS/J7	
Forced Logistics	Update	JS/J7	
Battlespace Awareness	Update	JS/J7	

<u>Documents</u>	<u>Action</u>	<u>Owner</u>	<u>Estimated Revision Date</u>
JICs			
C2	Rewrite	JFCOM/J9	CBA in progress ²
C2 Appendix E (SIPR)	Update	JFCOM/J9	UNK
CWMD	Rewrite	STRATCOM	CBA in progress ²
CWMD Appendix L (SIPR)	Update	DTRA	CBA in progress ²
Global Strike	Rewrite	AF/A5X	CBA in progress ²
Joint Logistics	Rewrite	TRANSCOM/Army (G4)	CBA in progress ²
Joint Urban Operations	Rewrite	JFCOM/J9	CBA in progress ²
Joint Undersea Superiority (JUSS)	Update	PACOM/J8	TBD
JUSS Annexes A & E	Update	PACOM/J8	TBD
Net-Centric Operating Environment	Rewrite	STRATCOM/J8	CBA in progress ²
Net-Centric Operating Environment Appendix G (SIPR)	Update	STRATCOM/J8	UNK
Persistent ISR	Rewrite	STRATCOM/J8	CBA in progress ²

¹Per JS/J7, JFCs are currently being archived and will subsequently be deleted (i.e., discontinued) from use. This process is currently ongoing and no projected end-date is available.

²Documents should be reviewed upon completion of CBAs.

X. Commander's Critical Information Requirements

Commander's Critical Information Requirements are elements of information required by the commander that directly affect decision-making. CCIRs are a key information management tool for the commander and help the commander assess the operational environment and identify decision points. **CCIRs belong exclusively to the commander.** The Commander can add, delete, adjust, and update them based on the information he needs for decision-making. In a doctrinal sense the staff would answer the CCIRs in order to facilitate decision-making during on-going operations. The following CCIRs support this Strategy to Task Plan and 24 AF's mission execution:

A. Priority Intelligence Requirements

1. What event occurred, due to a cyberspace attack on the US, its forces, vital interests, or allies that might justify a response?
2. What significant information indicates an imminent cyberspace attack is about to occur on the US, its forces, vital interests, or allies?
3. What actions are being taken by US adversaries that may deny, disrupt, degrade, or destroy the US Internet infrastructure or portions of the AF-GIG infrastructure vital to the US, its forces, vital interests, or allies?
4. What significant change(s) (i.e., increase or decrease) occurred in an adversary's cyberspace capability, or posture, to threaten or attack the US, its forces, vital interests, or allies?
5. What significant change(s) in a state or non-state adversary's cyberspace intent or position would potentially impact the US, its forces, vital interests, or allies?

6. What significant change(s) in a state or non-state adversary's cyberspace doctrine or strategy potentially impacts the US, its forces, vital interests, or allies?
7. What information reveals a significant weakness in an adversary state or non-state defense capability regarding their cyberspace networks?

B. Friendly Forces Information Requirements

1. Confirm any change in INFOCON worldwide.
2. Identify any event that negatively affects the execution of the network warfare mission.
3. Confirm attack(s) or intrusion(s) into the AF-GIG.
4. Identify any offensive cyber operation or intrusion that crosses, or has a high probability of crossing, into the AF-GIG.
5. Confirm any access into the AF-GIG by unauthorized person(s) that obtained privileged user, administrator, or root-level access.
6. Confirm any attack or intrusion to the AF-GIG that involved a second level domain web server (e.g., .gov, .mil, .edu).
7. Confirm any attack on the AF-GIG that impacts mission-essential, mission support, or mission critical computers, networks, and operations.
8. Confirm any attack or intrusion on the AF-GIG from a country against which the US is currently conducting military, diplomatic, or economic operations or will imminently conduct these operations.
9. Identify any attack or intrusion that is directed towards gaining or denying access to the AF-GIG.
10. Confirm any attack or intrusion on the AF-GIG that is directed towards gaining access to tactical or deployed operational networks.
11. Confirm any attack or intrusion on any cyber system involving a NIPRNET, SIPRNET, JWICS, PDAS, ISS, DSN, NSTS, and Red Switch gateway.
12. Identify any new computer virus for which no published countermeasure exists, any new virus whose propagation could likely outrun AF-containment capabilities, or any new virus which affects network services (e.g., e-mail, DNS services).
13. Confirm any attack or intrusion on the AF-GIG directed towards information systems shared with entities outside the AF (e.g., USA, USN, USMC, Joint-level organizations, agencies).
14. Identify any root-level access using methods that exploit a system's vulnerabilities.
15. Confirm an imminent or direct attack or intrusion on allied networks directed towards information systems shared with entities outside the AF (e.g., USA, USN, USMC, Joint-level organizations, and agencies).
16. Identify any event that negatively affects execution of the information operations mission.
17. Validate all assumptions from Section III.

C. Essential Elements of Information (classified)

XI. Commander's Estimate (SWOT Analysis)

The Commander's Estimate is presented below as a bullet item list, organized in a SWOT (Strength, Weakness, Opportunity, Threat) Analysis format. It allows the rapid presentation and recognition, without detailed analysis, of the many disparate factors that are germane to the stand up of 24 AF as a C-NAF. This presentation fosters an appreciation of the overall complexity and interdependency of the issues involved. Implementation tasks based on the consideration of this overview are included in Annex A.

A. Internal Factors

1. Strengths
 - Network/GIG Maintenance is established and robust
 - Discipline instantiates a standardized response
 - Work force is extremely motivated, talented and capable
 - Ability to establish networks in austere environments
 - Ability to solve network/GIG challenges in austere environments
2. Weaknesses
 - Forces are distributed across many sites
 - Attack response (response is according to attack location-can come from anywhere)
 - Current response actions are reactive--adversary chooses time & place of attack
 - Availability of forces in relation to demand (i.e., insufficient numbers)
 - Combat Comm Wing weighted on the side of the reserve forces (affects unit readiness)
 - Underdeveloped CND, CNA, and force integration C2 TTPs (i.e., compare to USN)
 - Lack of clarity/definition of cyberspace military effects in relation to principles of war
 - Consolidated, streamlined efforts of detection across military units, other government agencies
 - Cyber career field training does not exist and must be created

B. External Factors

1. Opportunities
 - Lead the DOD in organizing Cyber forces.
 - Ability to fill void created by lack of delegated roles and responsibilities beyond CND RA.
 - Ability to define warfare in cyberspace in terms of the principles of war that identify a revolution and alternative to the budget stressing solutions currently within the acquisition process.
 - Become Lead Service, from Joint perspective, in moving cyber forward.
2. Threats
 - Lack of a unified and coherent Policy.
 - Slow justice process = no swift & certain attribution = no credible deterrent.
 - Competing interests within the Service impede efficient C2 and execution of NetOps.
 - Lack of understanding with respect to authorities and established processes.
 - Lack of delegated roles and responsibilities beyond NetD.

- Inability to articulate the impact of cyberspace military effects to transform the conduct of CONPLANS/OPLANS in an increasingly constrained TOA.
- Title 10 and Title 50 responsibilities are not clearly shared between agencies with respect to cyberspace operations, especially in Net E and NetA areas.

XII. Summary

Controlling cyberspace is a prerequisite to effective operations through the strategic and operational levels of war in order to secure freedom from attack and to attack. The ability to act decisively throughout cyberspace across the range of military operations is mandatory in the 21st Century. By establishing a C-NAF for this purpose, the Air Force improves its warfighting capability and operational effectiveness.

This AFSPC Strategy to Task Plan defines specific objectives, desired effects, required capabilities, operational tasks, and concepts associated with the activation of 24 AF and maturation of cyberspace as an Air Force core competency. This document reflects critical actions required for activation of 24 AF and recommends creation, rewrite, and revision of concepts within the Joint and Air Force Family of Concepts.

AFSPC's strategic vision is to provide USSTRATCOM and other combatant commanders with compelling, game-changing cyber capabilities to defend and attack in, through, and from cyberspace. These capabilities will be integrated across all warfighting domains. 24 AF will provide global, integrated kinetic and non-kinetic strike capabilities in support of all CCDRs across the full range of military operations in order to deter, deny, disrupt, destroy, or defeat threats to US and US-aligned interests.

XIII. Annex A, Implementation Tasks

This annex list critical implementation tasks identified for 24 AF stand up. Inputs required for task completion, expected outputs of the task completion and the effects generated by this task being completed are captured on the left side of the slide. The right side of the slide lists all task milestones, ongoing actions, and any significant actions (positive or negative) that may impact the completion of the task. The following are 24 AF's critical implementation tasks:

1. Codify relationships and authorities between 24 AF (AFSPC) and AF ISR Agency.
2. Develop 24 AF operational concepts that include mission statement, mission sets and critical operational and enabling capabilities IAW AFI 10-2081.
3. Align and Assign 24 AF roles and responsibilities to units and capabilities IAW HQ USAF PAD 07-13
4. Finalize Family of Concepts.
5. Complete 24 AF Personnel Plan.
6. Establish MOAs at designated 24 AF locations.
7. Realign AFIOC to AFSPC.
8. CONPLAN/Operational Plan Review.
9. Exercise & Validate 24 AF Operational Capabilities.



As of: 20 Mar 09

Implementation 1

GREEN

Lead: 24 AF/DS
POC:
AO:

Task Description: Codify relationships and authorities between 24 AF (AFSPC) and AF ISR Agency

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p> <ul style="list-style-type: none"> • MOU? 	<p>Current Actions</p>
<p>Effects</p>	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 1				★																



As of: 20 Mar 09

Implementation 2

GREEN

Lead: 24 AF/A5/8
POC:
AO:

Task Description: Develop 24 AF operational concept that includes mission statement, mission sets and critical operational and enabling capabilities IAW AFI 10-2081

<p>Inputs</p> <ul style="list-style-type: none"> AFCYBER Stratplan 624 OC Op Concept DepSecDef Cyber Domain 24 AF Assumptions 	<p>Milestones</p> <ul style="list-style-type: none"> 4 Mar 09, Complete first draft 30 Mar 09, Deliver to AFSPC for approval
<p>Outputs</p> <ul style="list-style-type: none"> Used for other concept writers 	<p>Current Actions</p> <ul style="list-style-type: none"> First draft complete, awaiting 24 AF 2-letter review
<p>Effects</p> <ul style="list-style-type: none"> Instantiate AF cyber operations 	<p>Significant Issues</p> <ul style="list-style-type: none"> None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 2	★																			



As of: 20 Mar 09

Implementation 3

GREEN

Lead: 24 AF/A5/8
POC:
AO:

Task Description: Align and Assign 24 AF roles and responsibilities to units and capabilities IAW HAF PAD 07-13

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • 24 AF CONOPS • 624 OC OC 	<p>Milestones</p>
<p>Outputs</p>	<p>Current Actions</p>
<p>Effects</p>	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 3				★																



As of: 20 Mar 09

Implementation 4

GREEN

Lead: 24 AF/A5/8
POC:
AO:

Task Description: Finalize Family of Concepts

<p>Inputs</p> <ul style="list-style-type: none"> • JOPsC • AF CONOPS • AFSPC Concepts • DepSecDef Memo 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p> <ul style="list-style-type: none"> • Congruent Family of Concepts with Consistent Cyberspace “Message” 	
<p>Effects</p> <ul style="list-style-type: none"> • AF Unity of Effort for Cyberspace • Catalyst for DOD 	
<p>Current Actions</p> <ul style="list-style-type: none"> • Latest documents reviewed to ensure cyber/cyberspace was in keeping with the DepSecDef England’s stated cyberspace definition • Documents prioritized for update/rewrite 	
<p>Significant Issues</p> <ul style="list-style-type: none"> • Policy 	

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 4				★																



As of: 20 Mar 09

Implementation 5

GREEN

Lead: 24 AF/A1
POC:
AO:

Task Description: Complete 24 AF Personnel Plan

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • CyberProf. Roadmap • 24 AF CONOPS 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Personnel Plan for 24 AF standup 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Single message stating AF Personnel way-ahead 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 5				★																



As of: 20 Mar 09

Implementation 6

GREEN

Lead: 24 AF/DS
POC:
AO:

Task Description: Realign AFCA to AFSPC

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p>	<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Increased Synergy 	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 6				★																



As of: 20 Mar 09

Implementation 7

GREEN

Lead: 24 AF/DS
POC:
AO:

Task Description: Establish MOAs at designated 24 AF location

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • 24 AF CONOPS • 624 OC OC 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p>	<p>Current Actions</p>
<p>Effects</p>	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 7				★																



As of: 20 Mar 09

Implementation 8

GREEN

Lead: 24 AF/DS
POC:
AO:

Task Description: Realign AFIOC to AFSPC

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • Pplan 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p>	<p>Current Actions</p>
<p>Effects</p>	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 8				★																



As of: 20 Mar 09

Implementation 9

GREEN

Lead: 24 AF/A5/8
POC:
AO:

Task Description: CONPLAN/Operational Plan Review

<p>Inputs</p> <ul style="list-style-type: none"> CONPLAN 8039 	<p>Milestones</p> <ul style="list-style-type: none"> TBD
<p>Outputs</p>	<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> Understanding of AF's cybermission under STRATCOM 	<p>Significant Issues</p> <ul style="list-style-type: none"> None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 9				★																



As of: 20 Mar 09

Implementation 10

GREEN

Lead: 24 AF/A3
POC:
AO:

Task Description: Exercise & Validate 24 AF Operational Capabilities

<p>Inputs</p> <ul style="list-style-type: none"> • 24 AF CONOPS • 624 OC OC 	<p>Milestones</p>
<p>Outputs</p> <ul style="list-style-type: none"> • Exercise AARs • LLs 	<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Increased Mission Effectiveness 	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
IMP 10											★									

XIV. Annex B, Family of Concepts Tasks

This annex lists recommended tasks associated with the revision of existing Family of Concept documents. Inputs required for task completion, expected outputs of the task completion and the effects generated by this task being completed are captured on the left side of the slide. The right side of the slide lists all task milestones, ongoing actions, and any significant actions (positive or negative) that may impact the completion of the task. The following are the 11 Family of Concepts critical tasks:

1. Rewrite Global Strike CONOPS
2. Rewrite Space and C4ISR CONOPS
3. Rewrite Global Persistent Attack CONOPS
4. Rewrite Nuclear Response CONOP
5. Rewrite Agile Combat Support CONOPS
6. Rewrite Global Mobility CONOPS
7. Rewrite Homeland Defense and Civil Support CONOPS
8. Write AFSPC Cyber Functional Concept
9. Recommend Joint Staff Rewrite Major Combat Operations JOC
10. Recommend Joint Staff Rewrite Military Support to Stabilization, Security, Transition, and Reconstruction JOC
11. Recommend Joint Staff (AF Lead Service) Update Global Strike JIC



As of: 20 Mar 09

Family of Concepts 1

YELLOW

Lead: 24 AF/DS
POC:
AO:

Task Description: Rewrite Global Strike CONOPS

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • MCO JOC • GS JIC 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p> <ul style="list-style-type: none"> • AF CONOPS with integrated cyber operations 	<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> • More effective operations due to synergy of cyberspace domain 	<p>Significant Issues</p> <ul style="list-style-type: none"> • CRRA cycle

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 1								★												



As of: 20 Mar 09

Family of Concepts 2

YELLOW

Lead: 24 AF/DS
POC:
AO:

Task Description: Rewrite Space and C4ISR CONOPS

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • JOCs • C2JIC 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • AF CONOPS with integrated cyber operations 		<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> • More effective operations due to synergy of cyberspace domain 		<p>Significant Issues</p> <ul style="list-style-type: none"> • CRRA cycle

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 2								★												



As of: 20 Mar 09

Family of Concepts 3

YELLOW

Lead: 24 AF/DS
POC:
AO:

Task Description: Rewrite Global Persistent Attack CONOPS

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • MCO JOC • GS JIC 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • AF CONOPS with integrated cyber operations 		<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> • More effective operations due to synergy of cyberspace domain 		<p>Significant Issues</p> <ul style="list-style-type: none"> • CRRA cycle

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 3								★												



As of: 20 Mar 09

Family of Concepts 4

YELLOW

Lead: 24 AF/DS
POC:
AO:

Task Description: Rewrite Nuclear Response CONOPS

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • MCO JOC • GS JIC 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • AF CONOPS with integrated cyber operations 		<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> • More effective operations due to synergy of cyberspace domain 		<p>Significant Issues</p> <ul style="list-style-type: none"> • CRRA cycle

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 4								★												



As of: 20 Mar 09

Family of Concepts 5

YELLOW

Lead: 24 AF/DS
POC:
AO:

Task Description: Rewrite Agile Combat Support CONOPS

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • MCO JOC • GS JIC 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • AF CONOPS with integrated cyber operations 		<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> • More effective operations due to synergy of cyberspace domain 		<p>Significant Issues</p> <ul style="list-style-type: none"> • CRRA cycle

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 5								★												



As of: 20 Mar 09

Family of Concepts 6

YELLOW

Lead: 24 AF/DS
POC:
AO:

Task Description: Rewrite Global Mobility CONOPS

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • MCO JOC • GS JIC 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • AF CONOPS with integrated cyber operations 		<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> • More effective operations due to synergy of cyberspace domain 		<p>Significant Issues</p> <ul style="list-style-type: none"> • CRRA cycle

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 6								★												



As of: 20 Mar 09

Family of Concepts 7

YELLOW

Lead: 24 AF/DS
POC:
AO:

Task Description: Rewrite Homeland Defense and Civil Support CONOPS

<p>Inputs</p> <ul style="list-style-type: none"> PAD PPlan MCO JOC GS JIC 	<p>Milestones</p> <ul style="list-style-type: none"> TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> AF CONOPS with integrated cyber operations 		<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> More effective operations due to synergy of cyberspace domain 		<p>Significant Issues</p> <ul style="list-style-type: none"> CRRA cycle

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 7								★												



As of: 20 Mar 09

Family of Concepts 8

YELLOW

Lead: AFSPC/A8X
POC:
AO:

Task Description: Write AFSPC Cyber Functional Concept

<p>Inputs</p> <ul style="list-style-type: none"> PAD PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> Functional concept outlining functional cyber capabilities 		<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> More effective operations due to synergy of cyberspace domain 		<p>Significant Issues</p> <ul style="list-style-type: none"> CRRA cycle

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 8								★												



As of: 20 Mar 09

Family of Concepts 9

YELLOW

Lead: AF/A5XS
POC:
AO:

Task Description: Recommend Joint Staff Rewrite Major Combat Operations JOC

<p>Inputs</p> <ul style="list-style-type: none"> CCJO 	<p>Milestones</p> <ul style="list-style-type: none"> TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> MCO JOC describing how cyber is integrated with the other operations in all domains 		<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> More effective operations due to synergy of cyberspace domain 		<p>Significant Issues</p> <ul style="list-style-type: none"> JCIDS and Concept Update Cycles

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 9													★							



As of: 20 Mar 09

Family of Concepts 10

YELLOW

Lead: AF/A5XS
POC:
AO:

Task Description: Recommend Joint Staff Rewrite Military Support to Stabilization, Security, Transition, and Reconstruction JOC

<p>Inputs</p> <ul style="list-style-type: none"> CCJO 	<p>Milestones</p> <ul style="list-style-type: none"> TBD
<p>Outputs</p> <ul style="list-style-type: none"> SSTR JOC stressing cyber capabilities 	<p>Current Actions</p> <p>N/A</p>
<p>Effects</p>	<p>Significant Issues</p> <ul style="list-style-type: none"> JCIDS and Concept Update Cycles

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 10													★							



As of: 20 Mar 09

Family of Concepts 11

YELLOW

Lead: AF/A5XS
POC:
AO:

Task Description: Recommend Joint Staff (AF Lead Service) Update Global Strike JIC

<p>Inputs</p> <ul style="list-style-type: none"> • CCJO • MCO JOC 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • GS JIC stressing cyber capabilities 		<p>Current Actions</p> <p>N/A</p>
<p>Effects</p> <ul style="list-style-type: none"> • Cyber operations placed on par with traditional kinetic operations 		<p>Significant Issues</p> <ul style="list-style-type: none"> • JCIDS and Concept Update Cycles

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
FOC 11													★							

XV. Annex C, Perform AF Cyberspace Force Management (AFCyMA Task 1.0)

This annex outlines the Air Force Cyberspace Mission Area (AFCyMA) task associated with cyberspace force management. It is presented in high-level architecture format. This task and its supporting subtask must be performed based on analysis and modeling of current activities. For more detail see the IT Infrastructure Architecture Version 3.0 (Draft) available from AFCA/EAC.

Additionally, the most critical actions associated with the stand up of 24 AF are provided for consideration. These tasks have been mapped to the high-level architecture task(s) and are annotated in parentheses following the task description. Tasks and activities listed in the accompanying slides concentrate on building a force requisite to meet the objectives outlined in Section VI. Completion of these tasks will provide AFSPC and 24 AF educated, trained and competent personnel able to create the effects necessary in cyberspace complementary to air, space, land, and sea operations.

1. Establish a cyber warrior force development and management program that integrates cyber warriors with the CAF.
2. Integrate and elevate cyberspace to the same level as land, sea, air, and space in all AF professional military education curriculum.
3. Establish minimum personnel criteria for access to the AF-GIG that is consistent with recruiting and retention processes.
4. Define, acquire, and sustain training systems that replicate cyberspace capabilities to train and evaluate individual and shift/team performance in response to cyber incidents.
5. Integrate cyberspace events in all headquarters-level exercise and inspection programs to confirm combat readiness.
6. Identify DoD-wide cyberspace exercise list.
7. Man Cyber Operations Center and AFFOR staffs to IOC levels (mid-term).

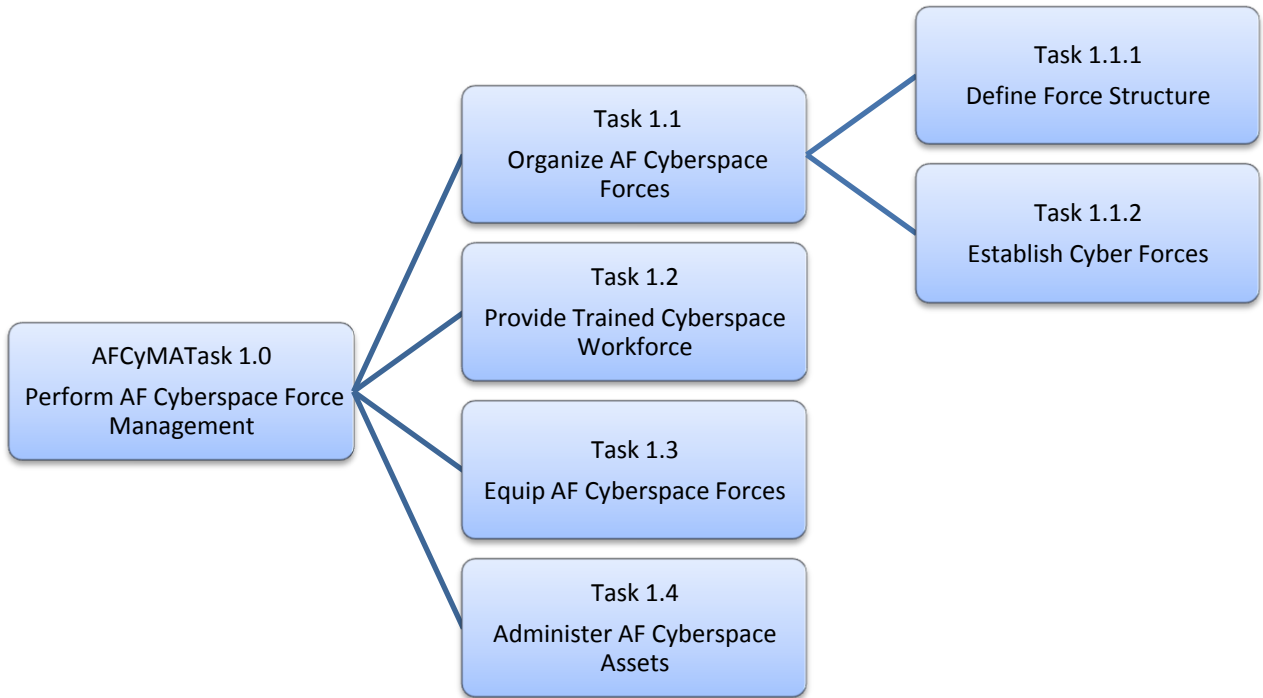


Figure C-1
Task 1.0, Perform AF Cyberspace Force Management (1 of 3)

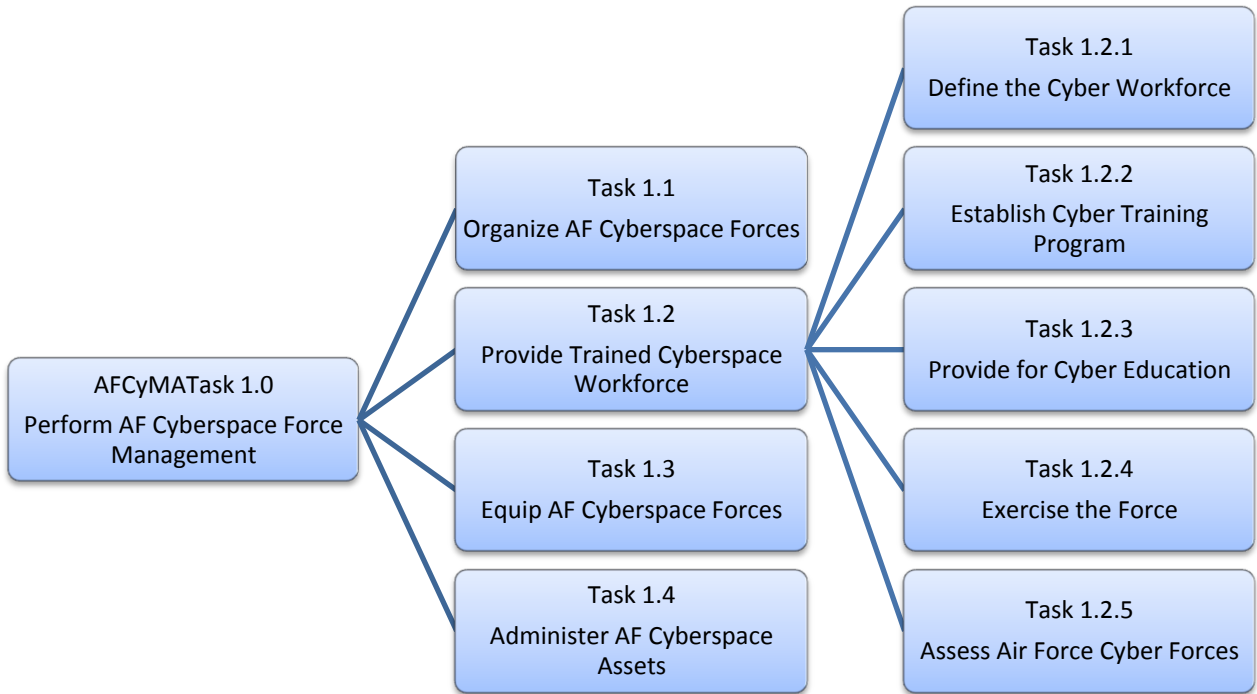


Figure C-2
Task 1.0, Perform AF Cyberspace Force Management (2 of 3)

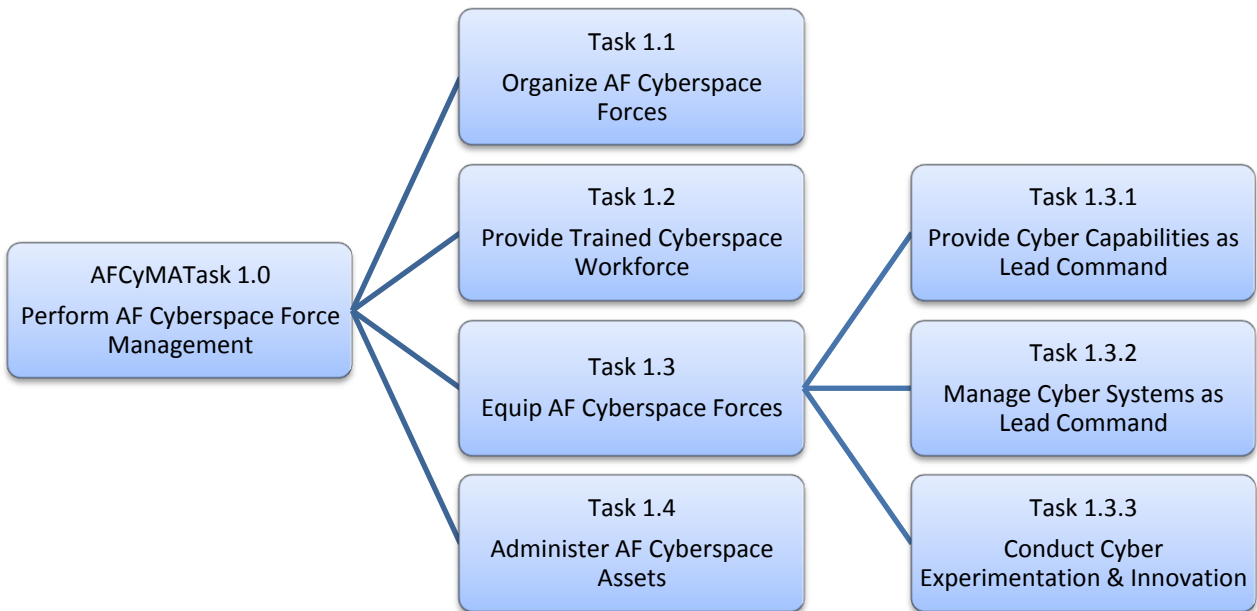


Figure C-3
Task 1.0, Perform AF Cyberspace Force Management (3 of 3)



As of: 20 Mar 09

Perform Force Management 1

GREEN

Lead: AFSPC/A1
POC:
AO:

Task Description: Establish a cyber warrior force development and management program that integrates cyber warriors with the CAF (1.0)

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p> <ul style="list-style-type: none"> • Coordinated and integrated force devel and management program 	<p>Current Actions</p> <ul style="list-style-type: none"> • Comm-Info Enlisted Transformation <ul style="list-style-type: none"> • 3D Career Field
<p>Effects</p> <ul style="list-style-type: none"> • Operationally focused and oriented cyber force 	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
PFM 1											★									



As of: 20 Mar 09

Perform Force Management 2

GREEN

Lead: AFSPC/A1
POC:
AO:

Task Description: Integrate and elevate cyberspace to the same level as land, sea, air, and space in all AF professional military education curriculum (1.2.3)

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p> <ul style="list-style-type: none"> • Educated cyberspace leaders 	<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Operationally focused and oriented air, space, cyberspace force across all domains 	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
PFM2																				★



As of: 20 Mar 09

Perform Force Management 3

GREEN

Lead: AFSPC/A1
POC:
AO:

Task Description: Establish minimum personnel criteria for access to the AF-GIG that is consistent with recruiting and retention processes (1.2.1.1, 1.2.1.4, 1.4.1.1.4, 1.4.2.1.1)

<p>Inputs</p> <ul style="list-style-type: none"> PAD PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> Trusted, competent user base 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> Secure cyberspace operations 		<p>Significant Issues</p> <ul style="list-style-type: none"> None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
PFM3							★													



As of: 20 Mar 09

Perform Force Management 4

GREEN

Lead: AFSPC/A1/A3/A8
POC:
AO:

Task Description: Define, acquire, and sustain training systems that replicate cyberspace capabilities to train and evaluate individual and shift/team performance in response to cyber incidents (1.2.2.3, 1.3.1.3, 1.3.2)

<p>Inputs</p> <ul style="list-style-type: none"> PAD PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> TBD
<p>Outputs</p> <ul style="list-style-type: none"> Exercise and training systems 	<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> Operationally focused and oriented cyber force 	<p>Significant Issues</p> <ul style="list-style-type: none"> None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
PFM4							★													



As of: 20 Mar 09

Perform Force Management 5

GREEN

Lead: AFSPC/A3
POC:
AO:

Task Description: Integrate cyberspace events in all headquarters-level exercise and inspection programs to confirm combat readiness (1.2.2.1, 1.2.4, 1.2.5)

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • AFPD 90-2 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Exercise and training systems 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Operationally focused and oriented cyber force 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
PFM5											★									



As of: 20 Mar 09

Perform Force Management 6

GREEN

Lead: AFSPC/A3
POC:
AO:

Task Description: Identify DoD-wide cyberspace exercise list (1.2.4.1)

<p>Inputs</p> <ul style="list-style-type: none"> Individual Exercise lists 	<p>Milestones</p> <ul style="list-style-type: none"> TBD
<p>Outputs</p> <ul style="list-style-type: none"> Comprehensive Exercise list 	<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> Commander better able to prioritize correct exercises 	<p>Significant Issues</p> <ul style="list-style-type: none"> None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
PFM6											★									



As of: 20 Mar 09

Perform Force Management 7

GREEN

Lead: AFSPC/A1
POC:
AO:

Task Description: Man CyOC and AFFOR staffs to IOC levels (mid-term) (1.1, 1.2)

<p>Inputs</p> <ul style="list-style-type: none"> PAD PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> Timely PCSs with right people 		<p>Current Actions</p> <ul style="list-style-type: none"> Comm-Info Enlisted Transformation <ul style="list-style-type: none"> 3D Career Field
<p>Effects</p> <ul style="list-style-type: none"> Initial Operationally capable C-NAF 		<p>Significant Issues</p> <ul style="list-style-type: none"> None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
PFM7				★																

XVI. Annex D, Establish AF Cyberspace Domain (AFCyMA Task 2.0)

This annex outlines the Air Force Cyberspace Mission Area (AFCyMA) task associated with establishing the AF cyberspace domain. It is presented in high-level architecture format. This task and its supporting subtask must be performed based on analysis and modeling of current activities. For more detail see the IT Infrastructure Architecture Version 3.0 (Draft) available from AFCA/EAC.

Additionally, the most critical actions associated with the stand up of 24 AF are provided for consideration. These tasks have been mapped to the high-level architecture task(s) and are annotated in parentheses following the task description. Tasks and activities listed in the accompanying slides concentrate on establishing the cyberspace domain to meet the objectives outlined in Section VI. Completion of these tasks will provide AFSPC and 24 AF the surety necessary to enable effects in cyberspace complementary to air, space, land, and sea operations. The most critical “Establish” tasks associated with the activation of 24 AF are as follows:

1. Partner with the joint force and the private sector to identify Air Force cyberspace dependencies and vulnerabilities.
2. Increase the current level of information assurance in the AF-GIG.
3. Spearhead identification and de-conflict communications and other mission essential electro-magnetic frequency operations.
4. Develop transition plan for Air Force Network Operations Center to Cyber Operations Center operations to include migration of Cyber Operations Center to final location (mid-term).

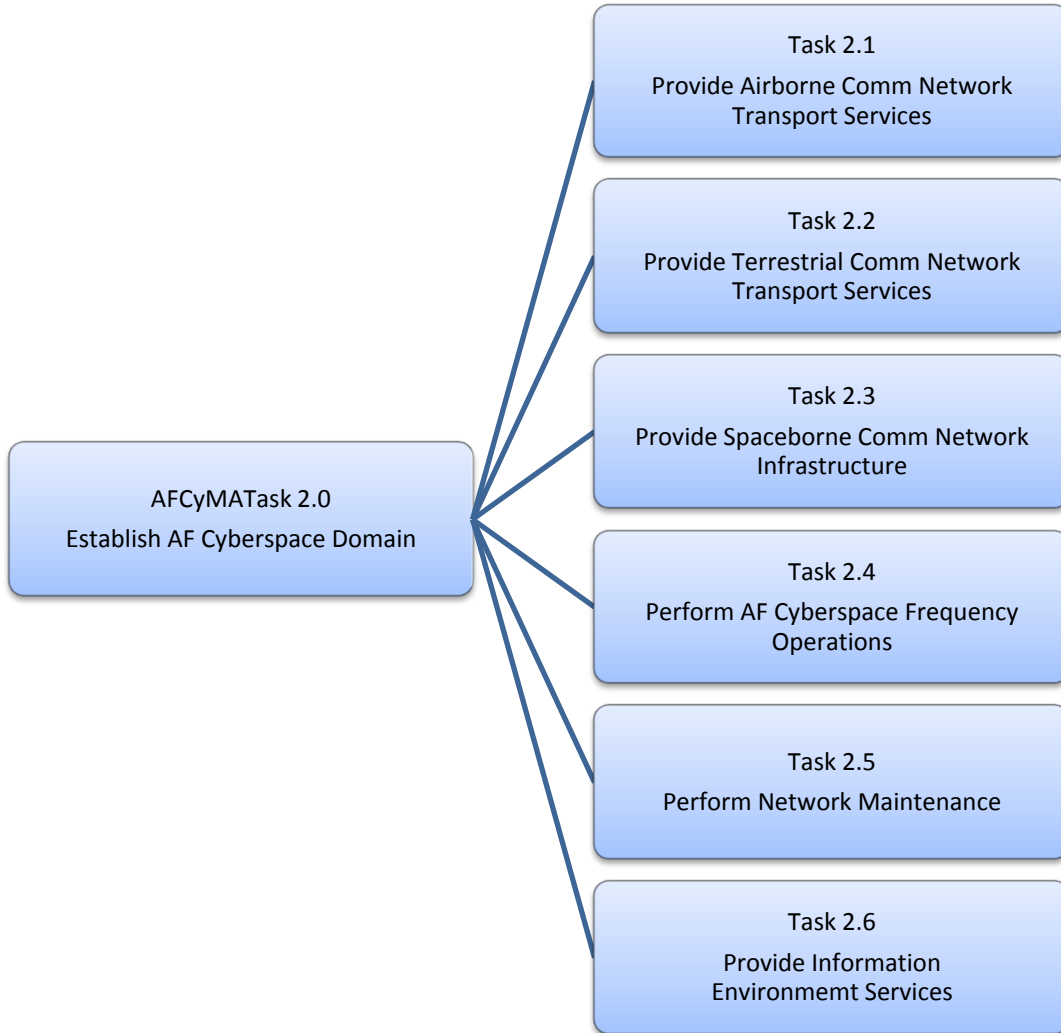


Figure D-1
Task 2.0, Establish AF Cyberspace Domain (1 of 5)

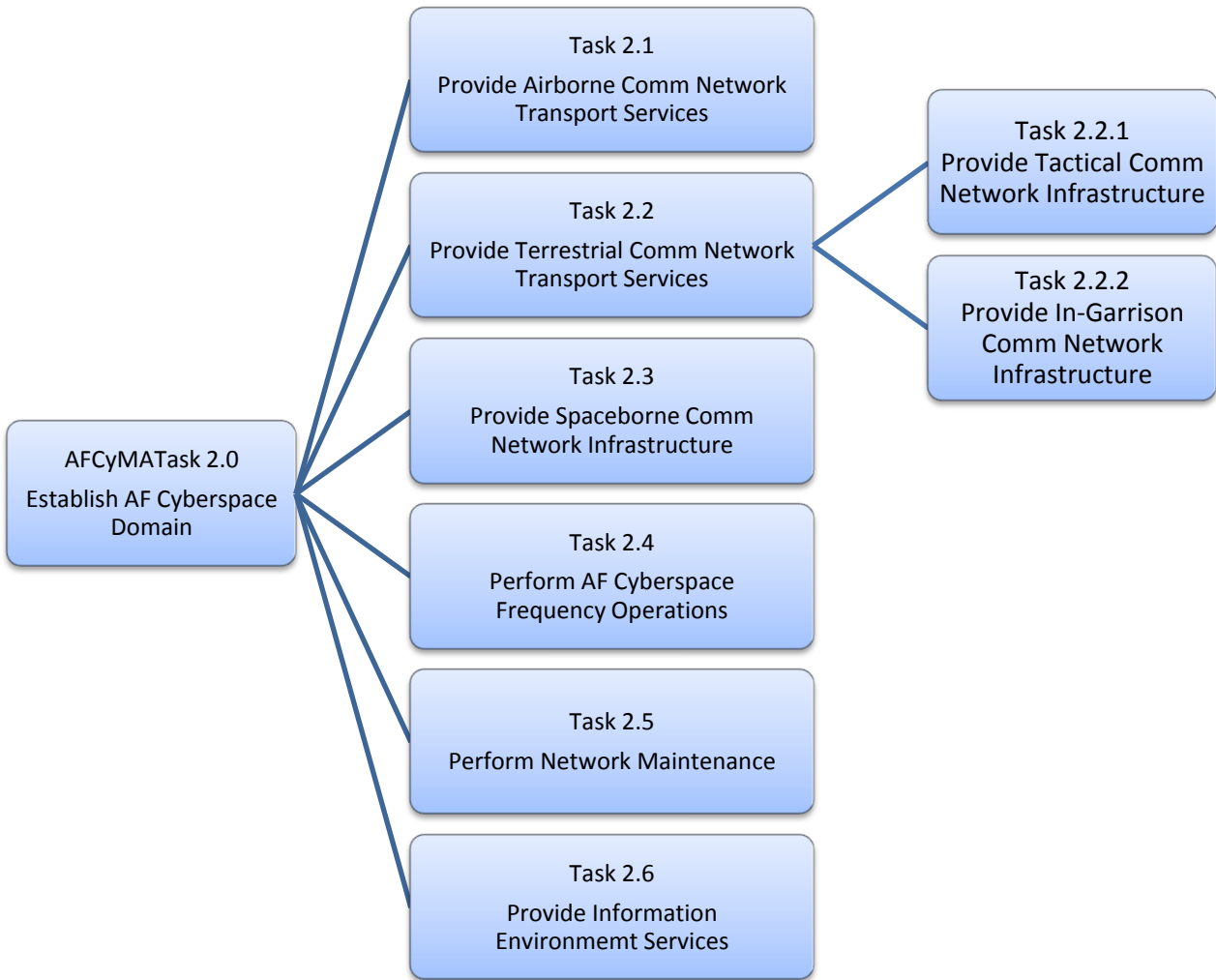


Figure D-2
Task 2.0, Establish AF Cyberspace Domain (2 of 5)

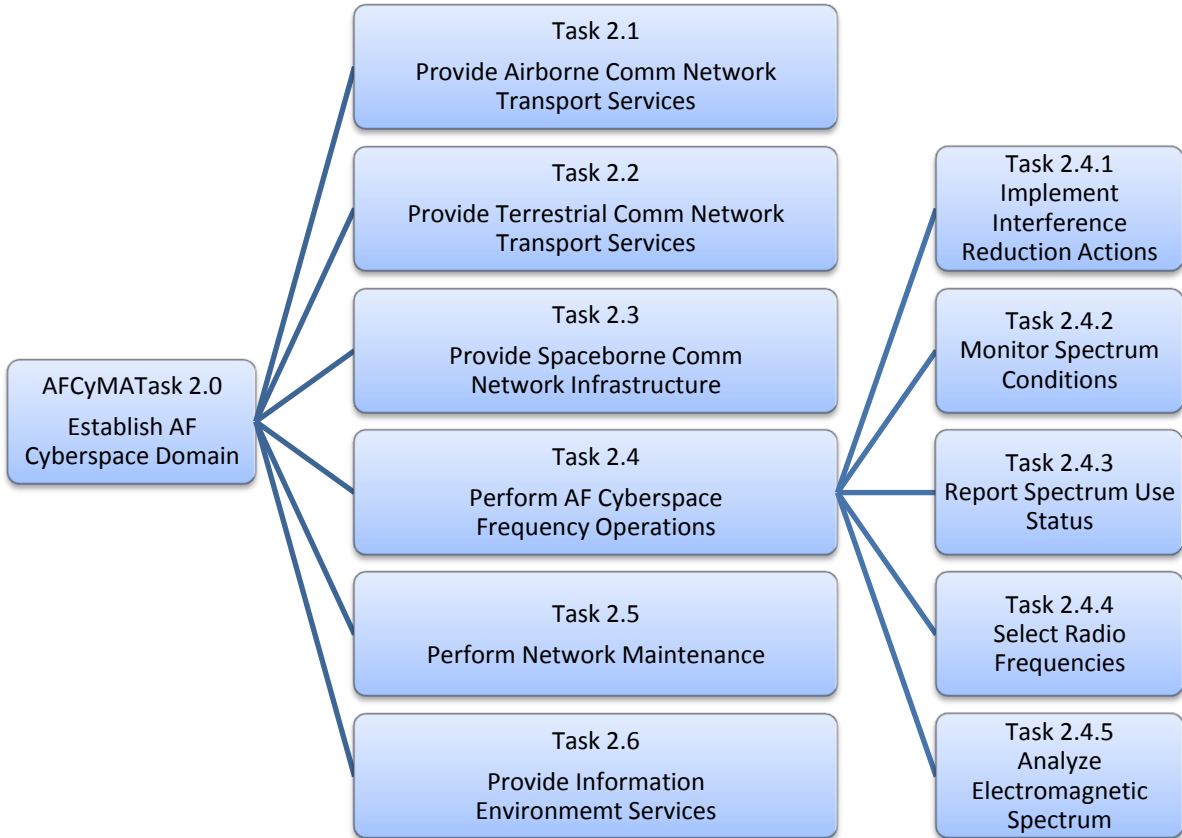


Figure D-3
Task 2.0, Establish AF Cyberspace Domain (3 of 5)

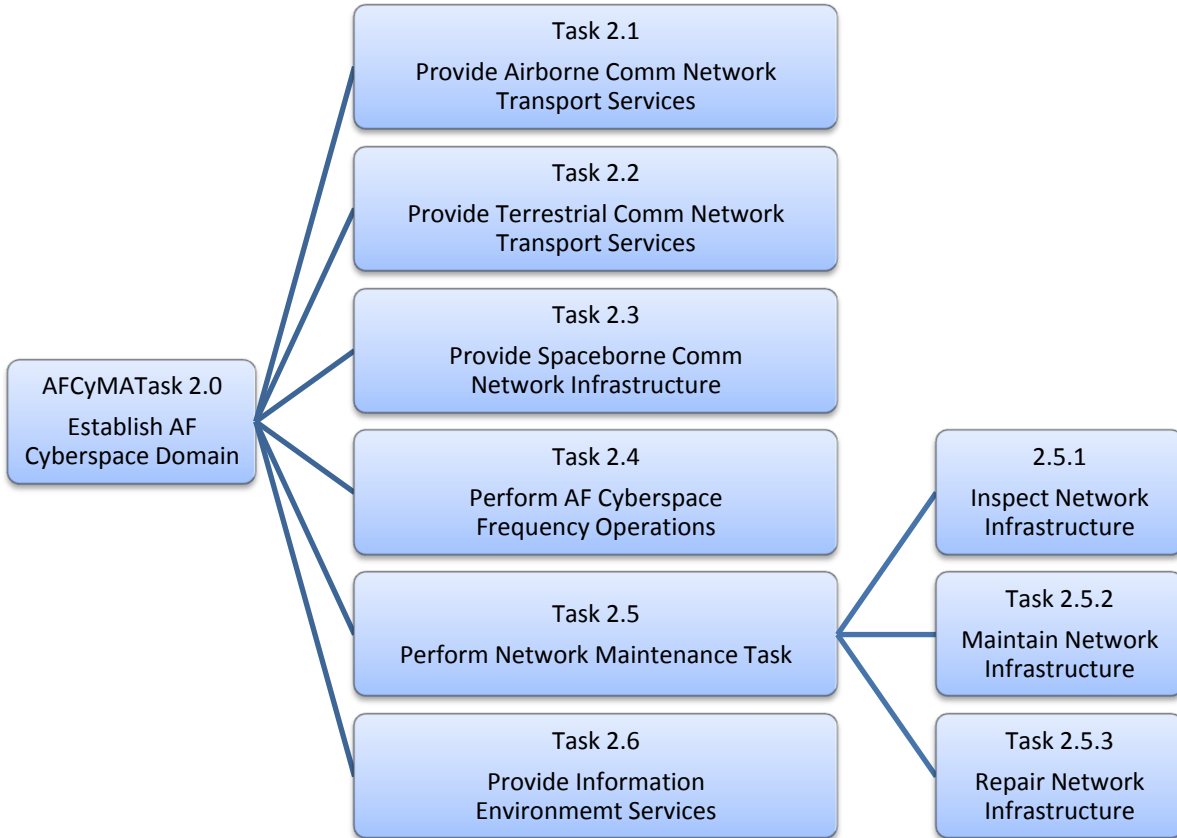


Figure D-4
Task 2.0, Establish AF Cyberspace Domain (4 of 5)

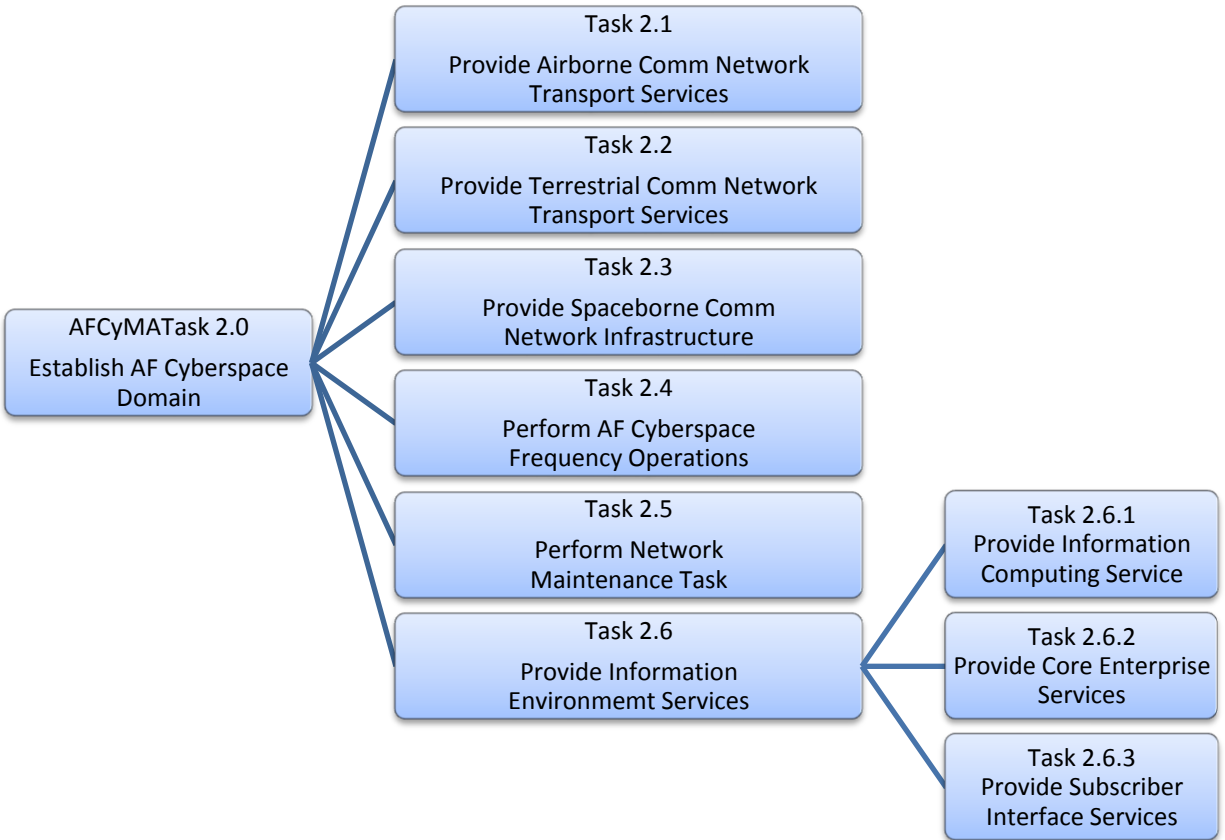


Figure D-5
Task 2.0, Establish AF Cyberspace Domain (5 of 5)



As of: 20 Mar 09

Establish 1

GREEN

Lead: AFSPC/A5
POC:
AO:

Task Description: Partner with the joint force and the private sector to identify Air Force cyberspace dependencies and vulnerabilities (4.1.1.1, 3.9)

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Dedicated Incident Response and COOP Plans • List of external AF-GIG Dependencies and internal AF-GIG Vulnerabilities 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Increased Cyberspace SA • Reduced susceptibility to attack 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
EST 1											★									



As of: 20 Mar 09

Establish 2

GREEN

Lead: AFSPC/A6
POC:
AO:

Task Description: Increase the current level of information assurance in the AF-GIG (4.2, 2.6)

<p>Inputs</p> <ul style="list-style-type: none"> PAD PPlan 	<p>Milestones</p> <ul style="list-style-type: none"> TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> IA OI Integrated short- and long-range Cyber Surety Plan 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> Assured Information 		<p>Significant Issues</p> <ul style="list-style-type: none"> None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
EST 2											★									



As of: 20 Mar 09

Establish 3

GREEN

Lead: AFSPC/A6/A3
POC:
AO:

Task Description: Spearhead identification and deconflict communications and other mission-essential electro-magnetic frequency operations (2.4)

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • C2 CBA (JFCOM) • Joint Lessons Learned 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Comm and C2 AoAs 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • No data lag, comm loss and increased C2 effectiveness • Comm interoperability 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
EST 3											★									



As of: 20 Mar 09

Establish 4

GREEN

Lead: AFSPC/A5
POC:
AO:

Task Description: Develop transition plan for Air Force Network Operations Center to Cyber Operations Center operations to include migration of Cyber Ops Center to final location (mid-term) (2.2, 2.4, 2.5)

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • 624 OC Operating Concept • 24 AF CONOPS 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Transition Plan complete • Sequenced Action List 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Seamless transition of operations 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
EST 4									★											

XVII. Annex E, Operate the AF Cyberspace Domain (AFCyMA Task 3.0)

This annex outlines the Air Force Cyberspace Mission Area (AFCyMA) task associated with operating the AF cyberspace domain. It is presented in high-level architecture format. This task and its supporting subtask must be performed based on analysis and modeling of current activities. For more detail see the IT Infrastructure Architecture Version 3.0 (Draft) available from AFCA/EAC.

Additionally, the most critical actions associated with the stand up of 24 AF are provided for consideration. These tasks have been mapped to the high-level architecture task(s) and are annotated in parentheses following the task description. Tasks and activities listed in the accompanying slides concentrate on operating the cyberspace domain to meet the objectives outlined in Section VI. Completion of these tasks will provide AFSPC and 24 AF with the foundation of operational capability necessary to generate effects in cyberspace complementary to air, space, land, and sea operations. The most critical “Operate” tasks associated with the activation of 24 AF are:

1. Establish and develop mutually beneficial relationships with joint partners to facilitate cross-domain operations and freedom of action.
2. Test the ability to rapidly respond to attacks and reconstitute cyberspace operations.
3. Define Air Force essential elements of information for cyberspace.
4. Define specific 24 AF priority intelligence requirements.
5. Fuse all-source ISR, as well as AF-GIG and AF-GIG-dependent network status to increase cyberspace situational awareness.
6. Work with the Office of the Secretary of Defense to define an acquisition process that can respond to the dynamic nature of the cyberspace domain.
7. Define 24 AF operational IOC and FOC criteria (mid-term).

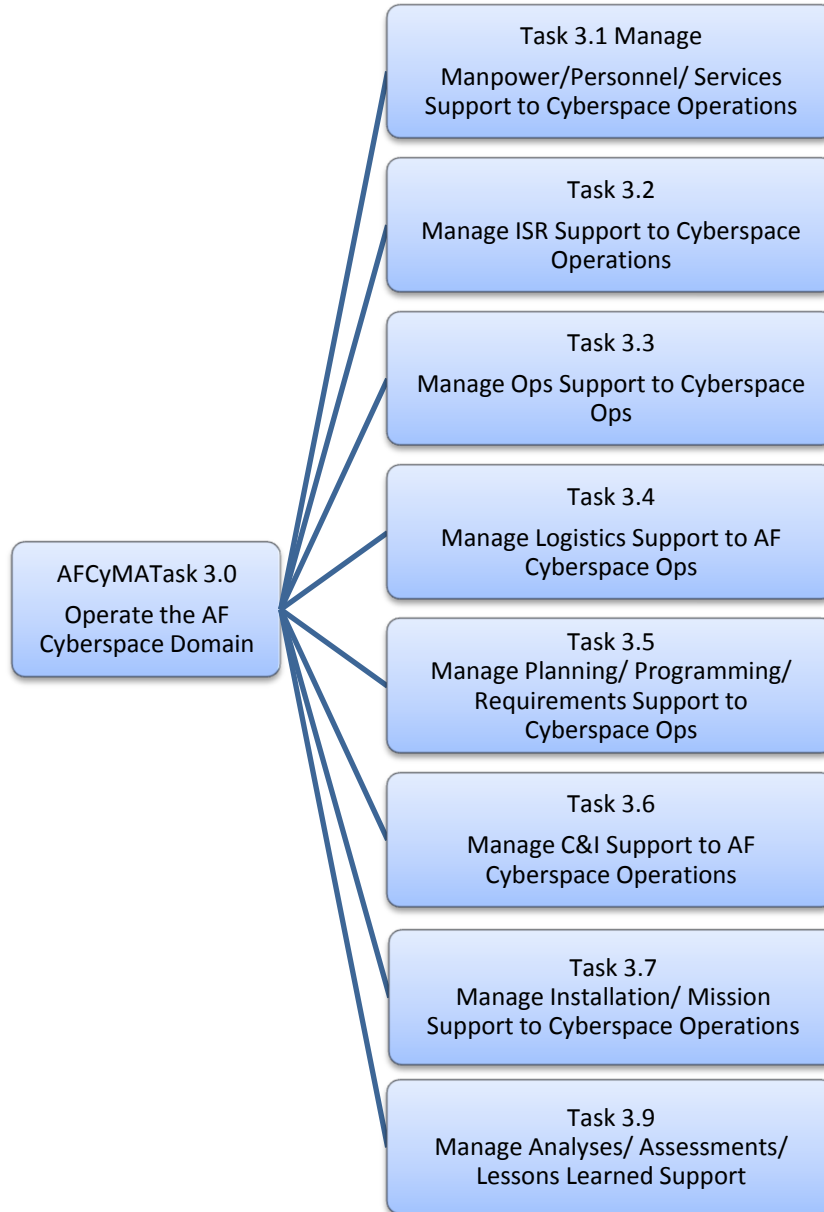


Figure E-1
Task 3.0, Operate the AF Cyberspace Domain (1 of 6)

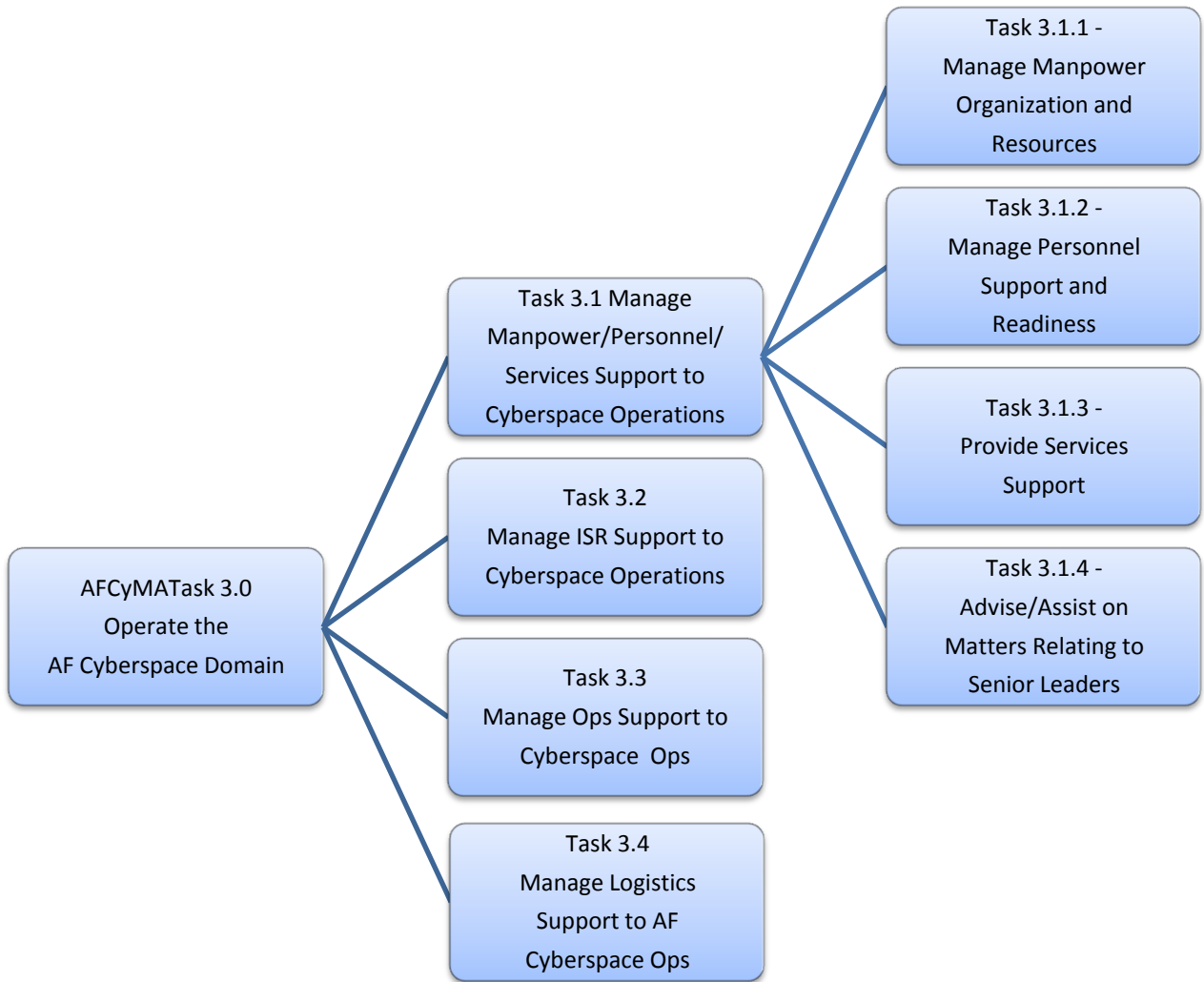


Figure E-2
Task 3.0, Operate the AF Cyberspace Domain (2 of 6)

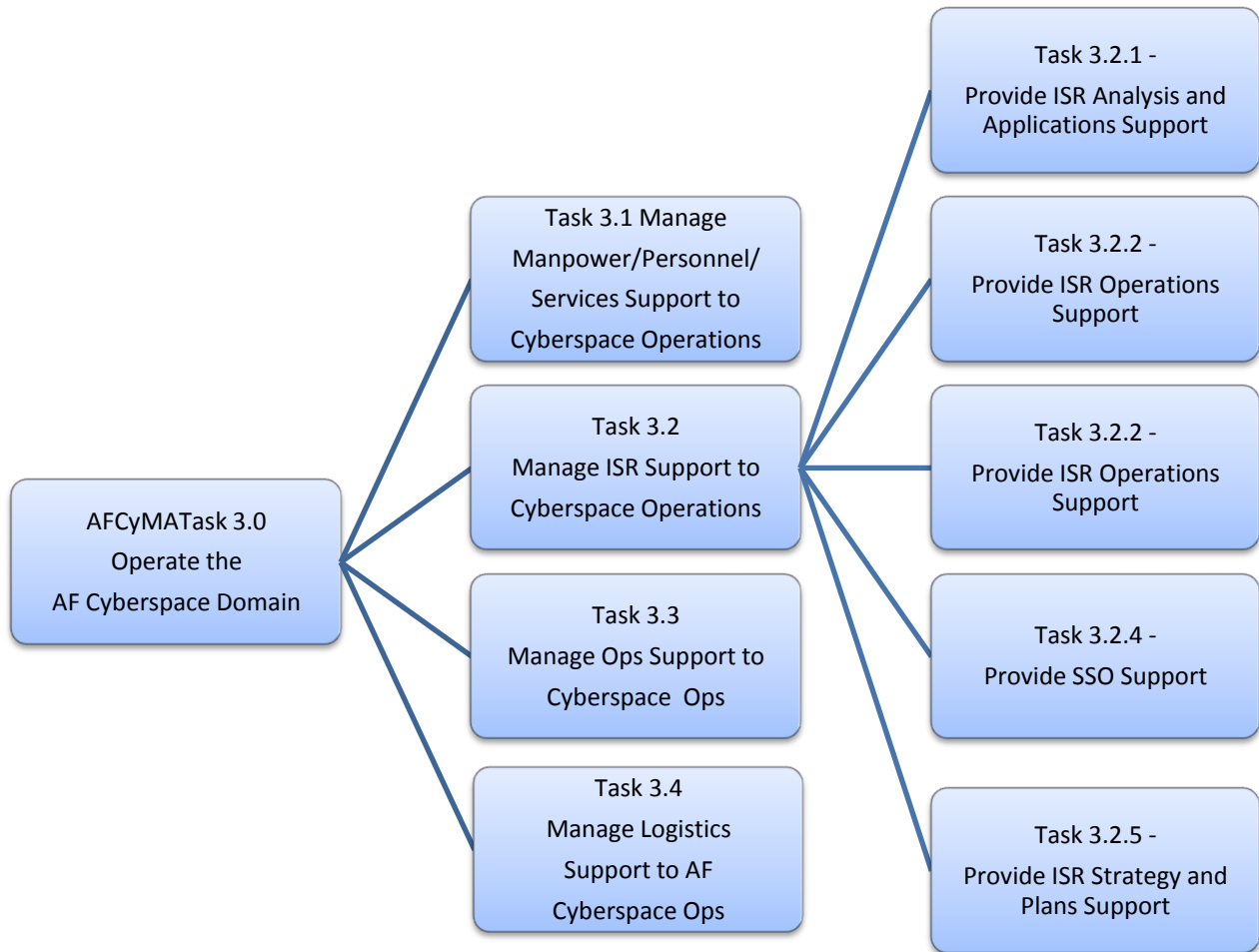


Figure E-3
Task 3.0, Operate the AF Cyberspace Domain (3 of 6)

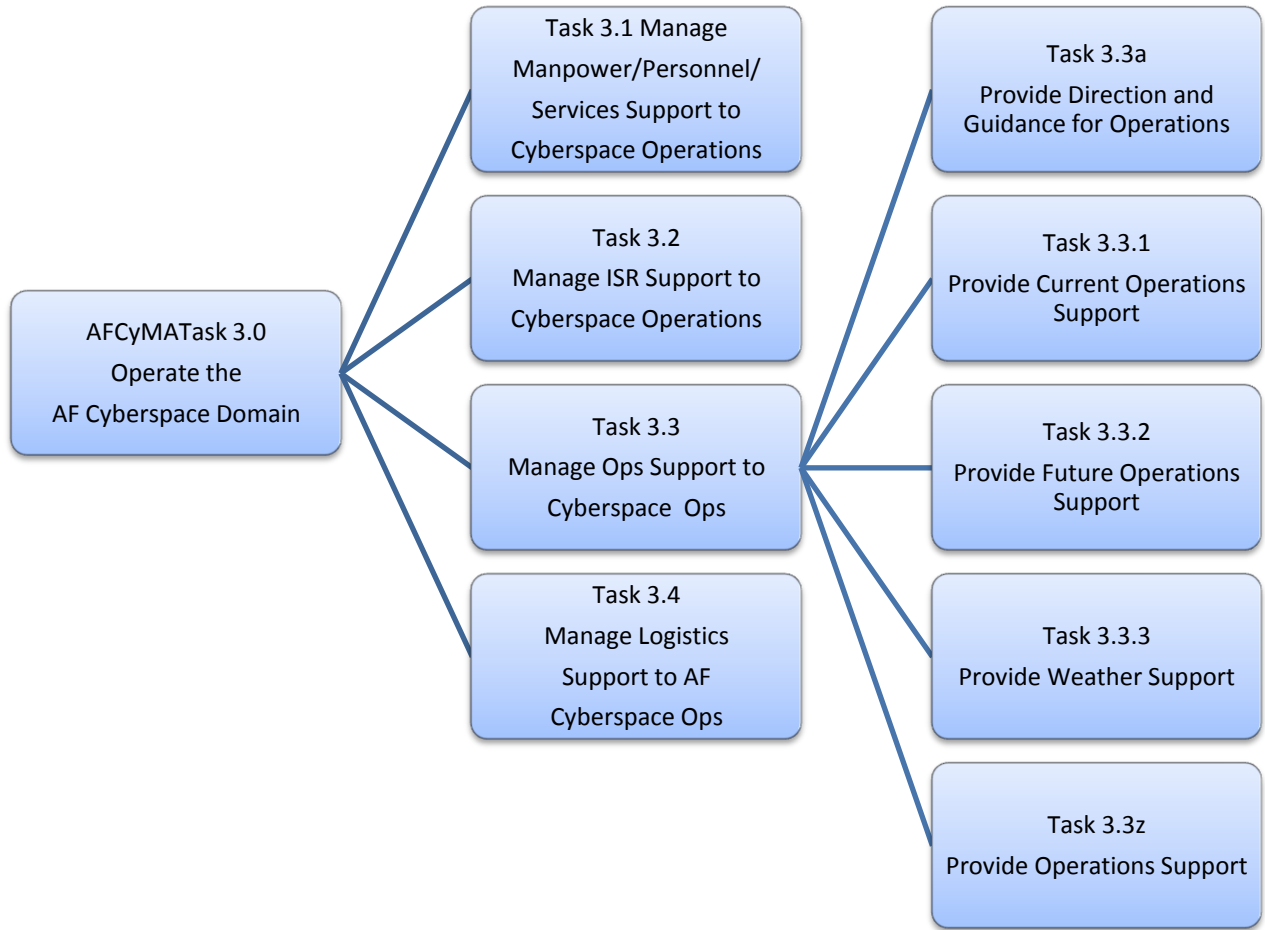


Figure E-4
Task 3.0, Operate the AF Cyberspace Domain (4 of 6)

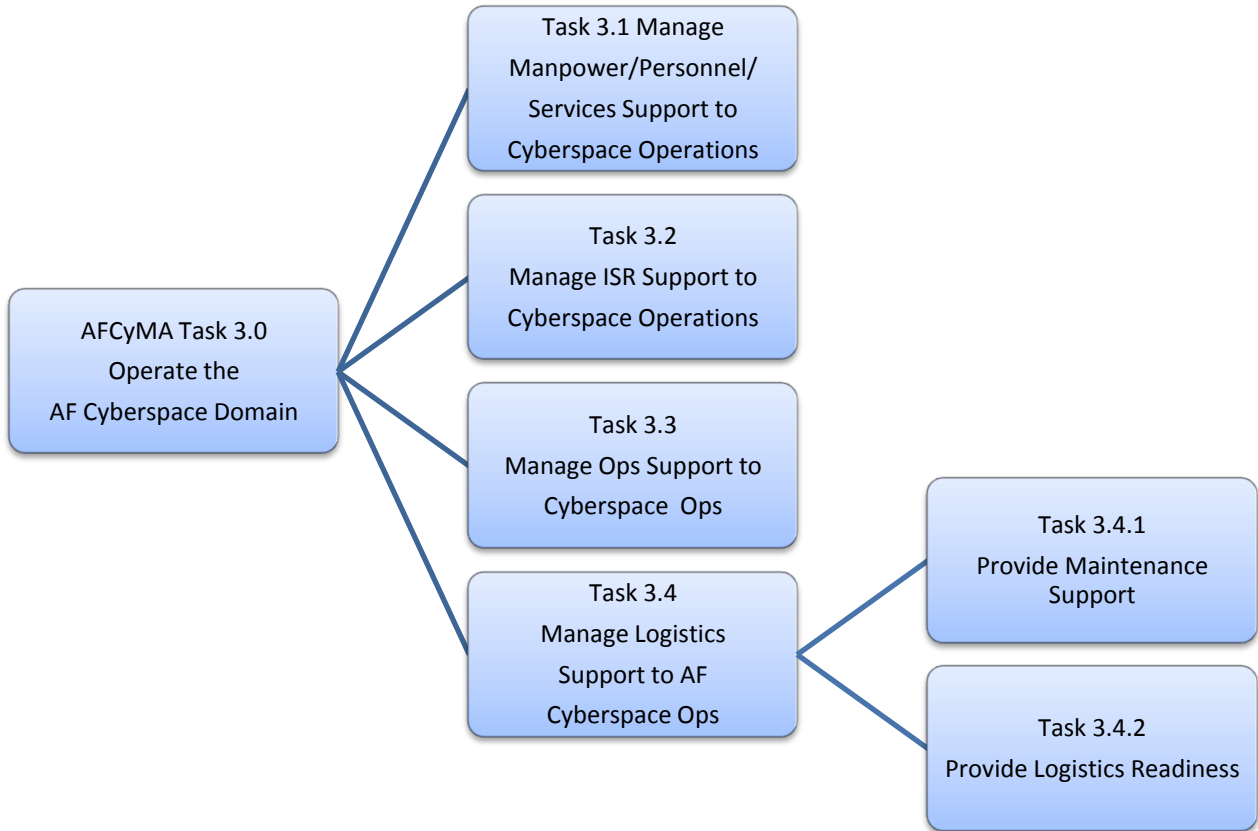


Figure E-5
Task 3.0, Operate the AF Cyberspace Domain (5 of 6)

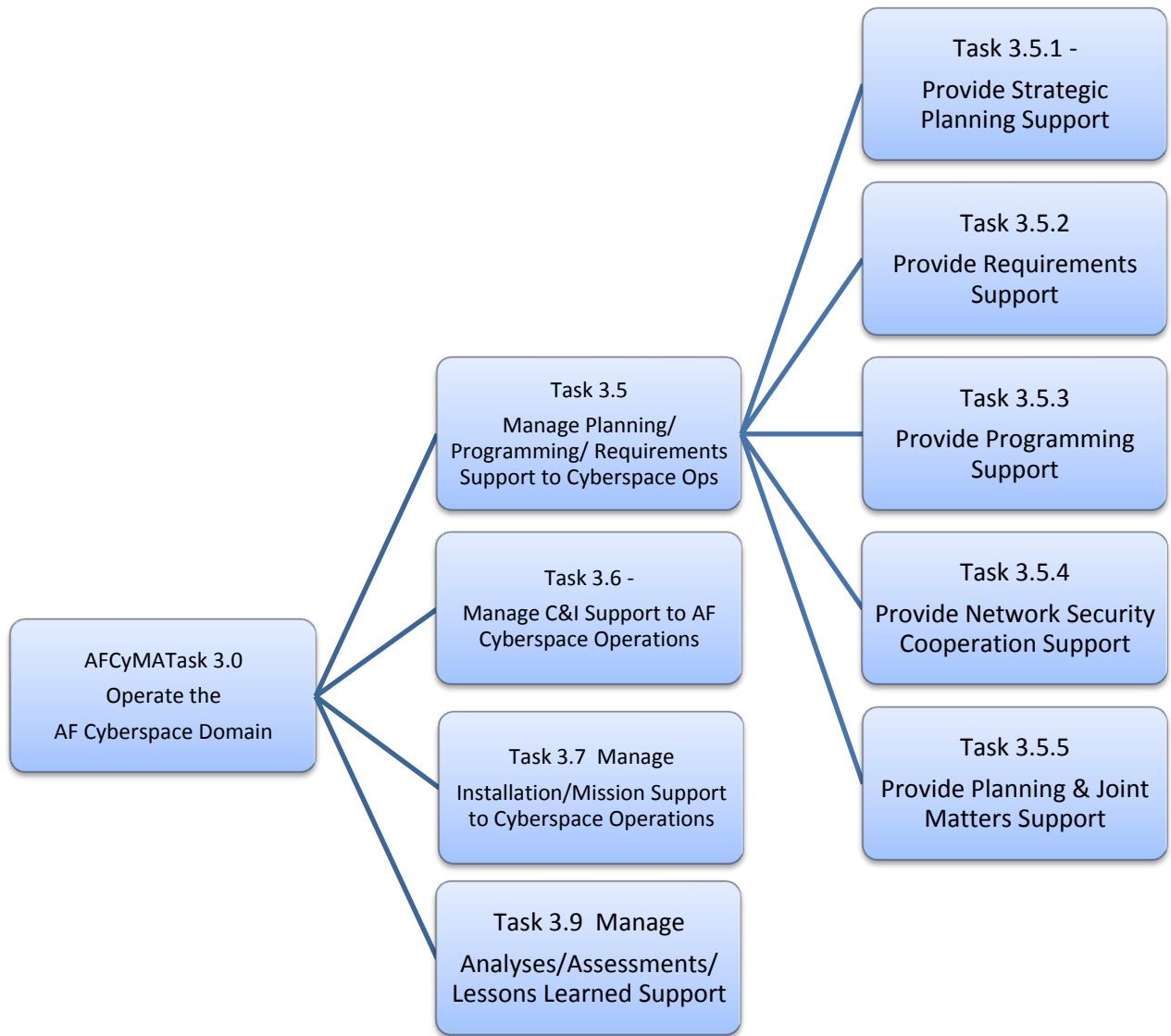


Figure E-6
Task 3.0, Operate the AF Cyberspace Domain (6 of 6)



As of: 20 Mar 09

Operate 1

GREEN

Lead: AFSPC/A3/A5
POC:
AO:

Task Description: Establish and develop mutually beneficial relationships with joint partners to facilitate cross-domain operations and freedom of action (3.5.5)

<p>Inputs</p> <ul style="list-style-type: none"> • CCJO • JOE 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • MOAs • Updated Joint Concepts 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Fully integrated and coordinated joint operations across all domains 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
OPR 1				★																



As of: 20 Mar 09

Operate 2

GREEN

Lead: AFSPC/A3/A5
POC:
AO:

Task Description: Test the ability to rapidly respond to attacks and reconstitute cyberspace operations (1.2.4)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Realistic Exercises stressing flexibility, responsiveness, and speed 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Operationally focused and oriented cyber force • Undiminished continuity of operations 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
OPR 2				★																



As of: 20 Mar 09

Operate 3

GREEN

Lead: AFSPC/A3/A2
 POC:
 AO:

Task Description: Define Air Force essential elements of information for cyberspace (3.5.1)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p> <ul style="list-style-type: none"> • Decision Quality Info 	
<p>Effects</p> <ul style="list-style-type: none"> • FOM/FFA • Enhanced OPSEC 	
<p>Current Actions</p>	
<p>Significant Issues</p> <ul style="list-style-type: none"> • None 	

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
OPR 3							★													



As of: 20 Mar 09

Operate 4

GREEN

Lead: 24 AF/A2
POC:
AO:

Task Description: Define specific 24 AF priority intelligence requirements (3.2.2.2)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Decision Quality Intel 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • FOM/ FFA • Enhanced OPSEC 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
OPR 4				★																



As of: 20 Mar 09

Operate 5

GREEN

Lead: AFSPC/A6/A3/A2
 POC:
 AO:

Task Description: Fuse all-source ISR, as well as AF-GIG and AF-GIG-dependent network status to increase cyberspace situational awareness (2.2.2.1.1, 4.1.1.1, 3.2)

<p>Inputs</p> <ul style="list-style-type: none"> All-source Intel 	<p>Milestones</p> <ul style="list-style-type: none"> TBD
<p>Outputs</p> <ul style="list-style-type: none"> COP Collaborative Environment 	<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> Global Cyber SA 	<p>Significant Issues</p> <ul style="list-style-type: none"> None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
OPR 5																			★	



As of: 20 Mar 09

Operate 6

GREEN

Lead: AFSPC/A8//AFNIC
 POC:
 AO:

Task Description: Work with the Office of the Secretary of Defense to define an acquisition process that can respond to the dynamic nature of the cyberspace domain (1.3.1.2.3)

<p>Inputs</p> <ul style="list-style-type: none"> • AF POM • Private Sector benchmarked processes 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • AFMC MOU/MOA • Dynamic Acquisition Process • USD/AT&L Guidance 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Effective and suitable operations' systems fielded as soon as required 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
OPR 6										★										



As of: 20 Mar 09

Operate 7

GREEN

Lead: AFSPC/A3/A5
POC:
AO:

Task Description: Define 24 AF operational IOC and FOC criteria (mid-term) (3.1, 3.2, 3.3, 3.4, 3.5)

<p>Inputs</p> <ul style="list-style-type: none"> • PAD • PPlan • 24 AF CONOPS 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Published IOC/FOC Criteria list 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Operationally Effective C-NAF 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
OPR 7					★															

XVIII. Annex F, Defend the AF Cyberspace Domain (AFCyMA Task 4.0)

This annex outlines the Air Force Cyberspace Mission Area (AFCyMA) task associated with defending the AF cyberspace domain. It is presented in high-level architecture format. These are the required tasks 24 AF must perform based on analysis and modeling of current activities. For more detail see the IT Infrastructure Architecture Version 3.0 (Draft) available from AFCA/EAC.

Additionally, the most critical actions associated with the stand up of 24 AF are provided for consideration. These tasks have been mapped to the high-level architecture task(s) and are annotated in parentheses following the task description. Tasks and activities listed in the accompanying slides concentrate on defending the cyber domain to meet the objectives outlined in Section VI. Completion of these tasks will provide AFSPC and 24 AF with the foundation of operational capability necessary to generate effects in cyberspace complementary to air, space, land, and sea operations.

1. Establish response, recovery, and continuity of operations strategies to mitigate risk induced by identified dependencies and vulnerabilities.
2. Description: Incorporate global best practice-based solutions and architectures to preserve the effectiveness and survivability of mission-related military and non-military personnel, equipment, facilities, information, and infrastructure.
3. Collaborate with joint and interagency partners to develop a DIME-integrated deterrent strategy for cyberspace.
4. Prevent exploitation of cyberspace systems and harden USAF assets against cyber attacks through the electro-magnetic spectrum.
5. Define friendly force response thresholds in Air Force mission-relevant terms.
6. Define and publish joint web-based rules of engagement to protect cyberspace capabilities that provide immediate updates to users

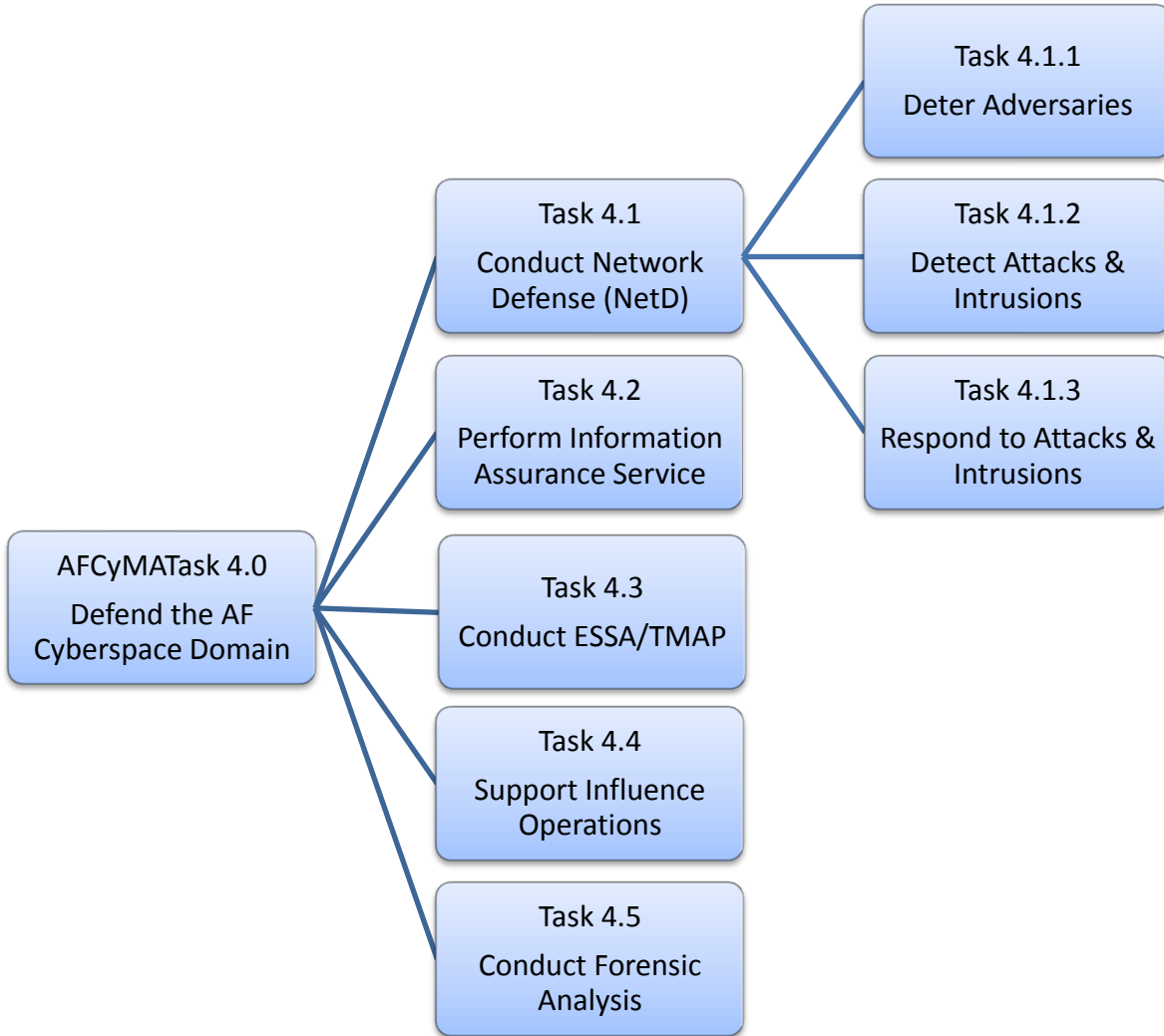


Figure F-1
Task 4.0, Defend the AF Cyberspace Domain (1 of 5)

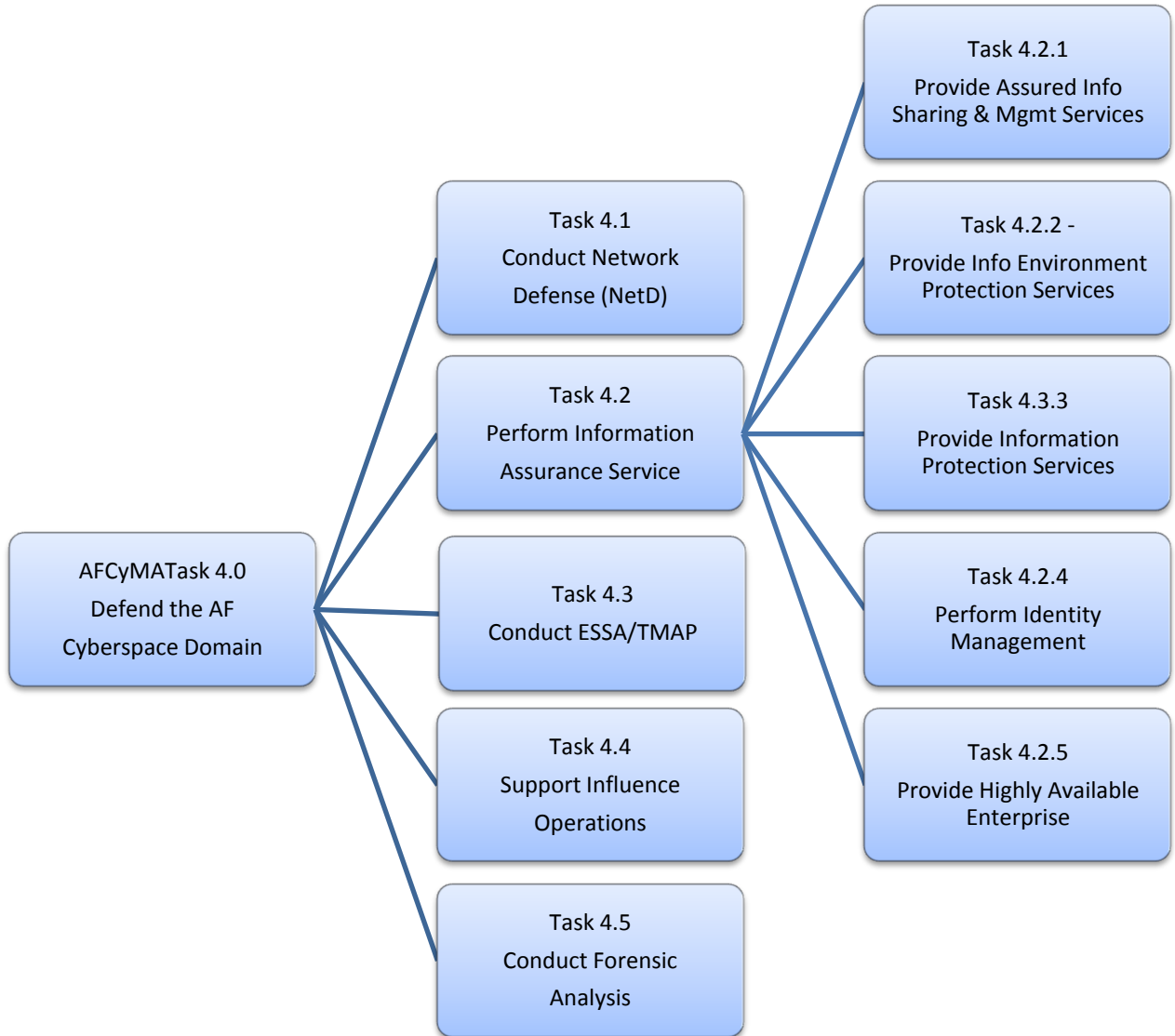


Figure F-2
Task 4.0, Defend the AF Cyberspace Domain (2 of 5)

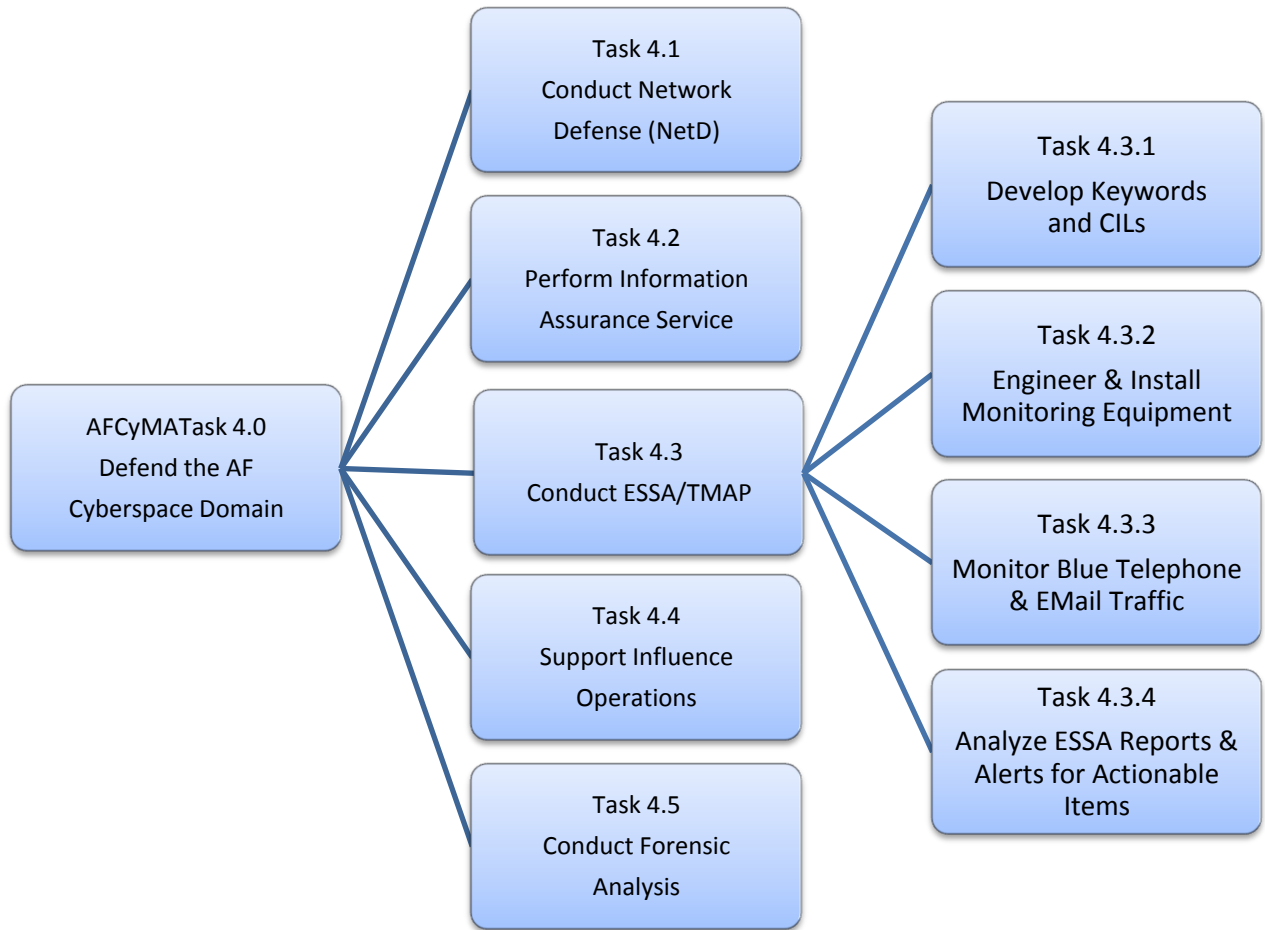


Figure F-3
Task 4.0, Defend the AF Cyberspace Domain (3 of 5)

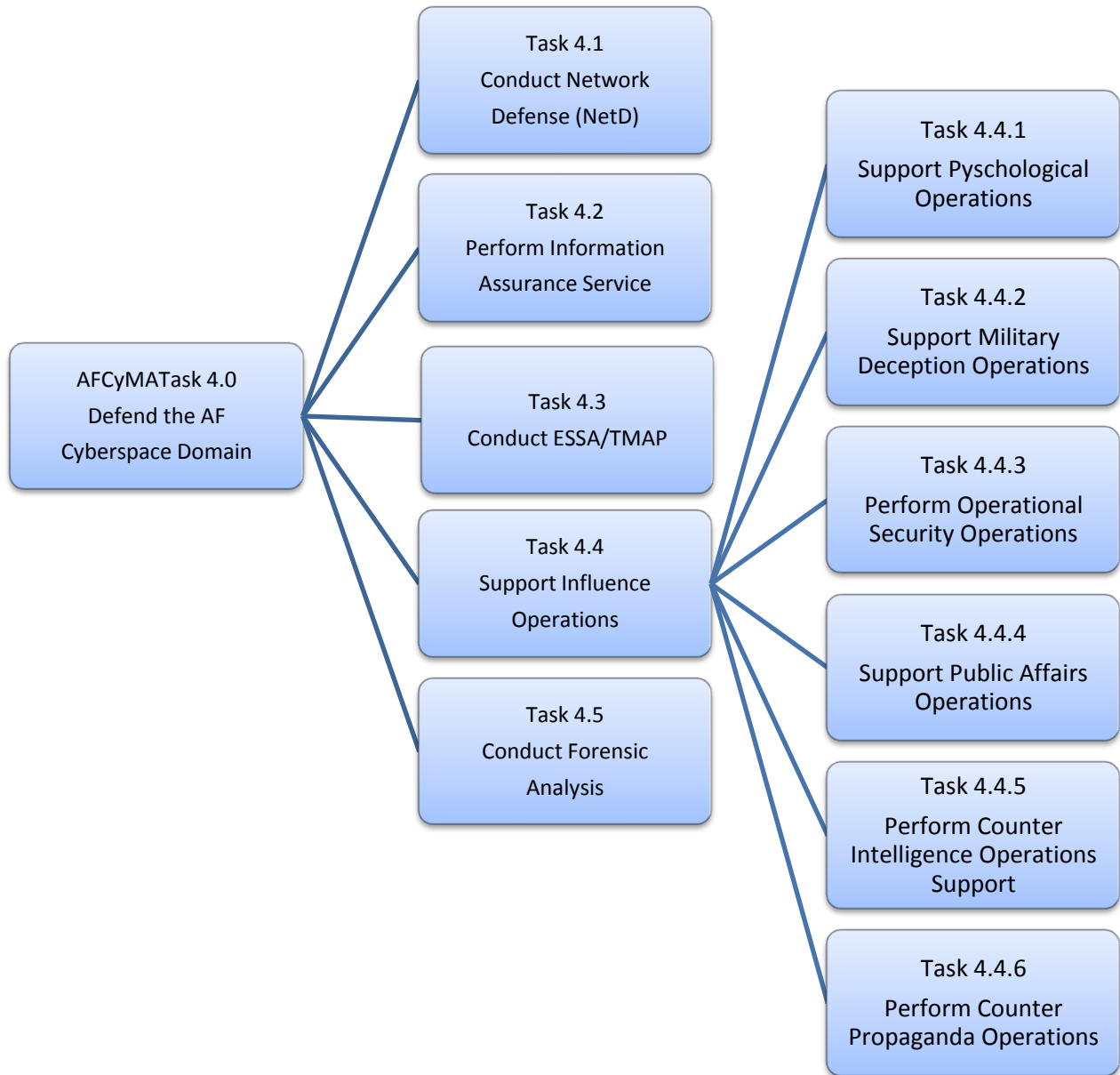


Figure F-4
Task 4.0, Defend the AF Cyberspace Domain (4 of 5)

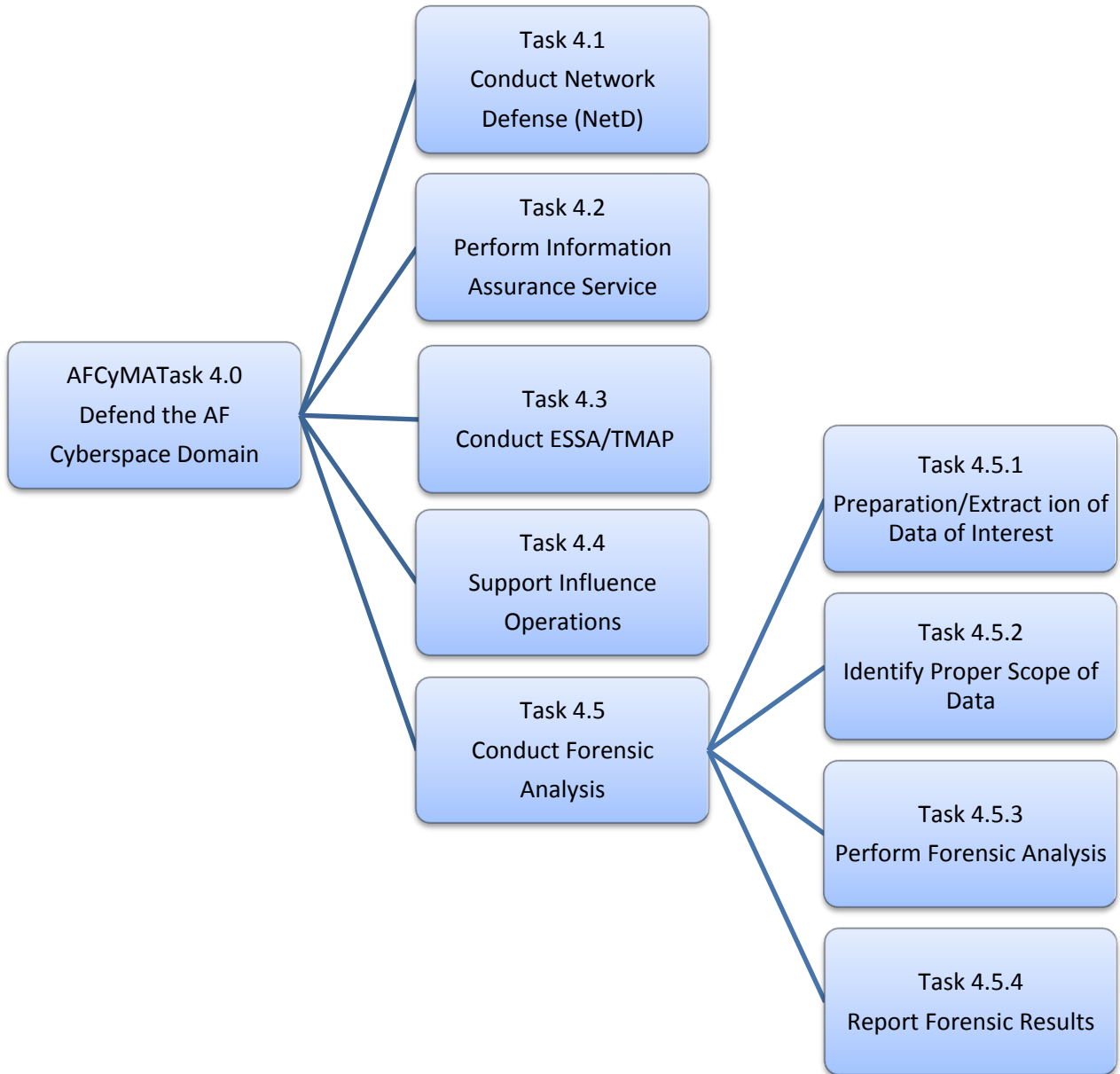


Figure F-5
Task 4.0, Defend the AF Cyberspace Domain (5 of 5)



As of: 20 Mar 09

Defend 1

GREEN

Lead: 24 AF/A3/A5
 POC:
 AO:

Task Description: Establish response, recovery, and continuity of operations strategies to mitigate risk induced by identified dependencies and vulnerabilities. (4.4.3.4, 4.1.3.2, 4.3.2.1.2.2.4)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs • Service Providers • PWI 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p> <ul style="list-style-type: none"> • Dedicated Incident Response and COOP Plans 	<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Reduced susceptibility to attack—operate through attacks 	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
DEF 1													★							



As of: 20 Mar 09

Defend 2

GREEN

Lead: AFSPC/A6/A3
POC:
AO:

Task Description: Incorporate global best practice-based solutions and architectures to preserve the effectiveness and survivability of mission-related military and non-military personnel, equipment, facilities, information, and infrastructure (1.3, 1.4)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs • ISO-27000 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Policy, processes, procedures that embrace global best practices 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Reduced susceptibility/vulnerability to attack, enhanced internal IA mechanisms 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
DEF 2										★										



As of: 20 Mar 09

Defend 3

GREEN

Lead: AFSPC/A5
POC:
AO:

Task Description: Collaborate with joint and interagency partners to develop a DIME-integrated deterrent strategy for cyberspace (4.1.1)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Government-approved public policy (i.e., National Cyberspace Deterrence Policy) 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Reduced attacks on the AF-GIG and AF-GIG dependencies 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
DEF 3													★							



As of: 20 Mar 09

Defend 4

GREEN

Lead: AFSPC/A6
POC:
AO:

Task Description: Prevent exploitation of cyberspace systems and harden USAF assets against cyber attacks through the electro-magnetic spectrum (4.4)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs • AARs 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Robust Acquisition Policy • Develop TTPs 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Little or no information compromised 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
DEF 4											★									



As of: 20 Mar 09

Defend 5

GREEN

Lead: AFSPC/A3/A2
 POC:
 AO:

Task Description: Define friendly force response thresholds in Air Force mission-relevant terms (4.1.3)

<p>Inputs</p> <ul style="list-style-type: none"> • Cyberspace Threat Assessments 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p> <ul style="list-style-type: none"> • Response Threshold Decision Matrices 	
<p>Effects</p> <ul style="list-style-type: none"> • Increased Responsiveness • Compressed Decision Cycle • Enhanced Decision Superiority 	
<p>Current Actions</p>	
<p>Significant Issues</p> <ul style="list-style-type: none"> • None 	

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
DEF 5											★									



As of: 20 Mar 09

Defend 6

GREEN

Lead: AFSPC/A8
POC:
AO:

Task Description: Define and publish joint web-based rules of engagement to protect cyberspace capabilities that provide immediate updates to users (4.2.1)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs • ROEs • CJCSI 3121.01A 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Definitive, single-source ROE 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Simplified operations and compressed decision cycles 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
DEF 6										★										

XIX. Annex G, Exploit the Cyberspace Domain (AFCyMA Task 5.0)

This annex outlines the Air Force Cyberspace Mission Area (AFCyMA) task associated with exploiting the cyberspace domain. It is presented in high-level architecture format. This task and its supporting subtask must be performed based on analysis and modeling of current activities. For more detail see the IT Infrastructure Architecture Version 3.0 (Draft) available from AFCA/EAC.

Additionally, the most critical actions associated with the stand up of 24 AF are provided for consideration. These tasks have been mapped to the high-level architecture task(s) and are annotated in parentheses following the task description. Tasks and activities listed in the accompanying slides concentrate on exploiting the domain to meet the objectives outlined in Section VI. Completion of these tasks will provide AFSPC and 24 AF with the foundation of operational capability necessary to generate effects in cyberspace complementary to air, space, land, and sea operations.

1. Integrate the 624 Operations Center into a global, interconnected C2 enterprise.
2. Develop AFTTP, memorandums of agreement, and legal processes to facilitate compression of the joint and interagency cyberspace decision-cycle.
3. Review all CONPLANS/OPLANS for the integration of military effects through cyberspace.
4. Define role(s) and participate in joint and combined exercises as integrated force providers IAW CONPLANS/OPLANS.

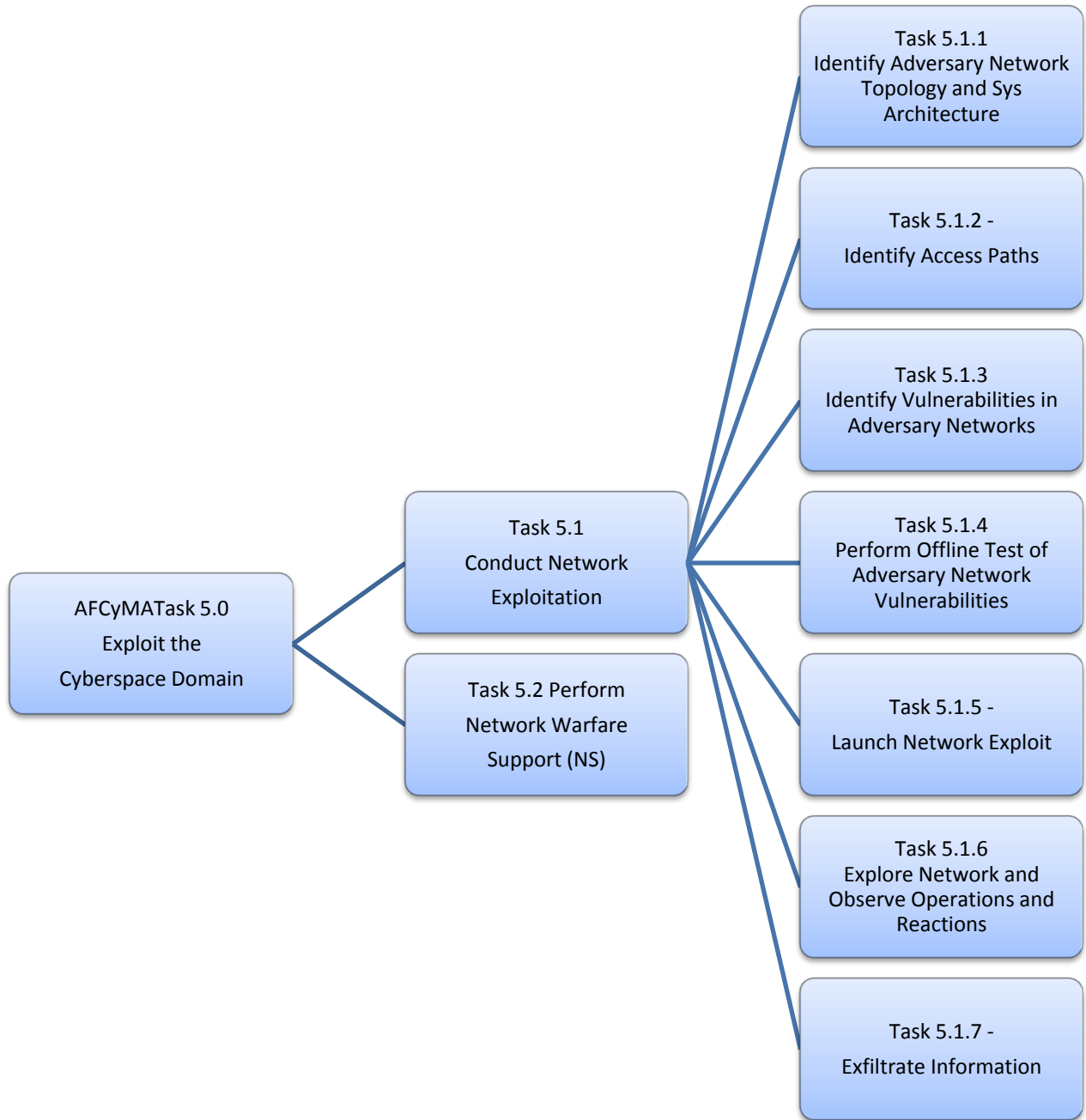


Figure G-1
Task 5.0, Exploit the Cyberspace Domain (1 of 2)

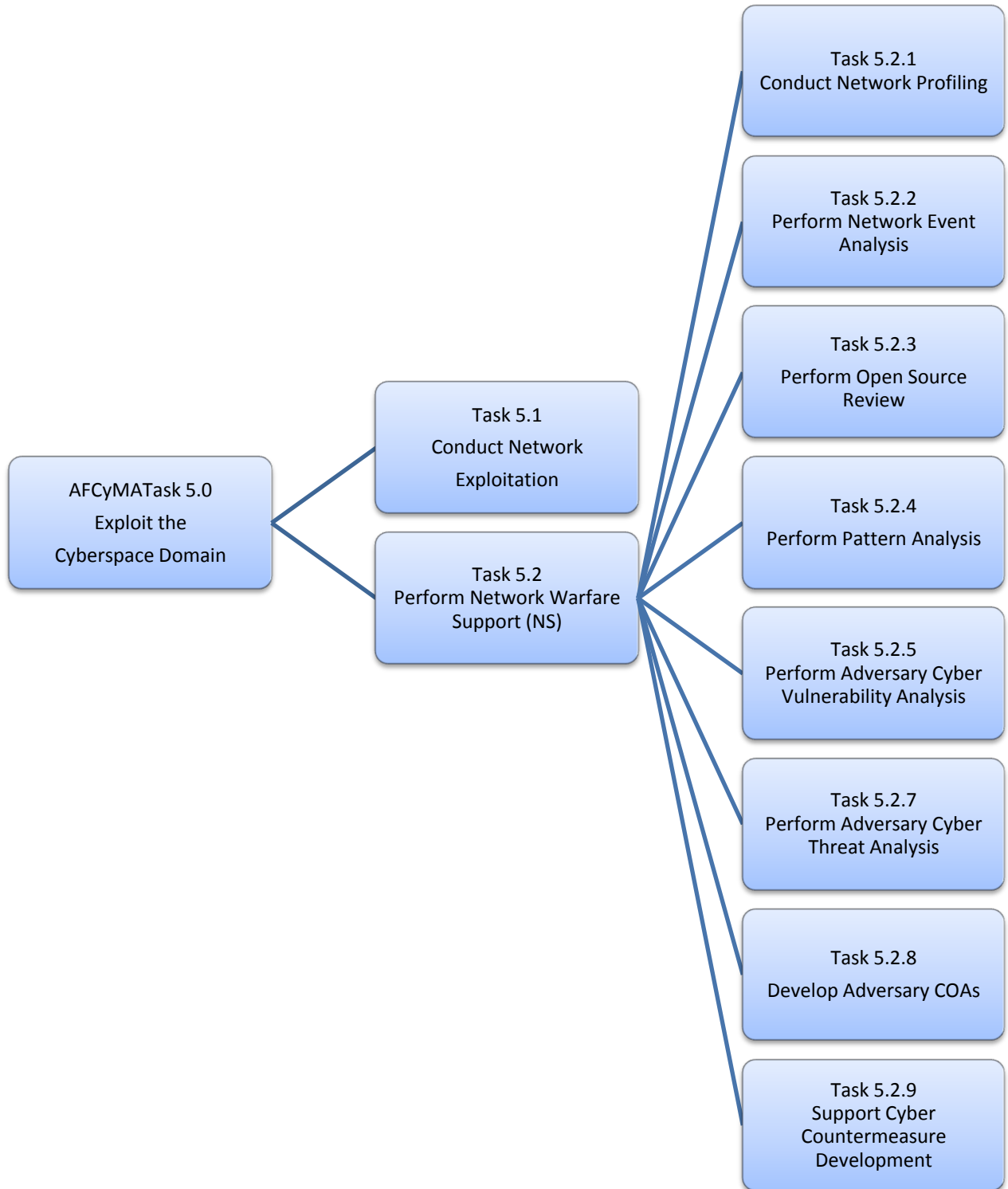


Figure G-2
Task 5.0, Exploit the Cyberspace Domain (2 of 2)



As of: 20 Mar 09

Exploit 1

GREEN

Lead: 24 AF/A3
POC:
AO:

Task Description: Integrate the 624 Operations Center into a global, interconnected C2 enterprise (3.3)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs • 24 AF OC OC • 24 AF Operational Concept 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Inter-op center MOUs/MOAs 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Integrated, global C2 Operations 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
EXP 1							★													



As of: 20 Mar 09

Exploit 2

GREEN

Lead: AFSPC/A5
POC:
AO:

Task Description: Develop AFTTP, memorandums of agreement, and legal processes to facilitate compression of the joint and interagency cyberspace decision-cycle. (5.1.2, 5.1.3, 5.2.2)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • AFTTP • MOAs • Legal Documentation 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Compressed Joint and interagency cyberspace decision cycles 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
EXP 2							★													



As of: 20 Mar 09

Exploit 3

GREEN

Lead: AFSPC/A5/A3
POC:
AO:

Task Description: Review all CONPLANS/OPLANS for the integration of military effects through cyberspace (5.2.3, 5.2.5, 3.3a)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANS • OPLANS 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD
<p>Outputs</p> <ul style="list-style-type: none"> • CONPLAN / OPLAN Annexes 	<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Well integrated cyber and cross-domain operations 	<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
EXP 3												★								



As of: 20 Mar 09

Exploit 4

GREEN

Lead: 24 AF/A3
POC:
AO:

Task Description: Define role(s) and participate in joint and combined exercises as integrated force providers IAW CONPLANS/OPLANS (5.2.3, 5.2.5, 3.3a, 4.4)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANS • OPLANS 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Exercise scripts fully defined for cyberspace forces 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Fully integrated, operationally focused and oriented cyber force 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
EXP 4							★													

XX. Annex H, Attack the Cyberspace Domain (AFCyMA Task 6.0)

This annex outlines the Air Force Cyberspace Mission Area (AFCyMA) task associated with attacking the cyberspace domain. It is presented in high-level architecture format. This task and its supporting subtask must be performed based on analysis and modeling of current activities. For more detail see the IT Infrastructure Architecture Version 3.0 (Draft) available from AFCA/EAC.

Additionally, the most critical actions associated with the stand up of 24 AF are provided for consideration. These tasks have been mapped to the high-level architecture task(s) and are annotated in parentheses following the task description. Tasks and activities listed in the accompanying slides concentrate on attacking the domain to meet the objectives outlined in Section VI. Completion of these tasks will provide AFSPC and 24 AF with the foundation of operational capability necessary to generate effects in cyberspace complementary to air, space, land, and sea operations.

1. Neutralize adversary operations in cyberspace and develop commensurate capabilities.
2. Develop capabilities that expand or redirect/reorient the decision cycle of an adversary.
3. Define an asymmetric, capabilities-based defense and attack cyberspace acquisition strategy.

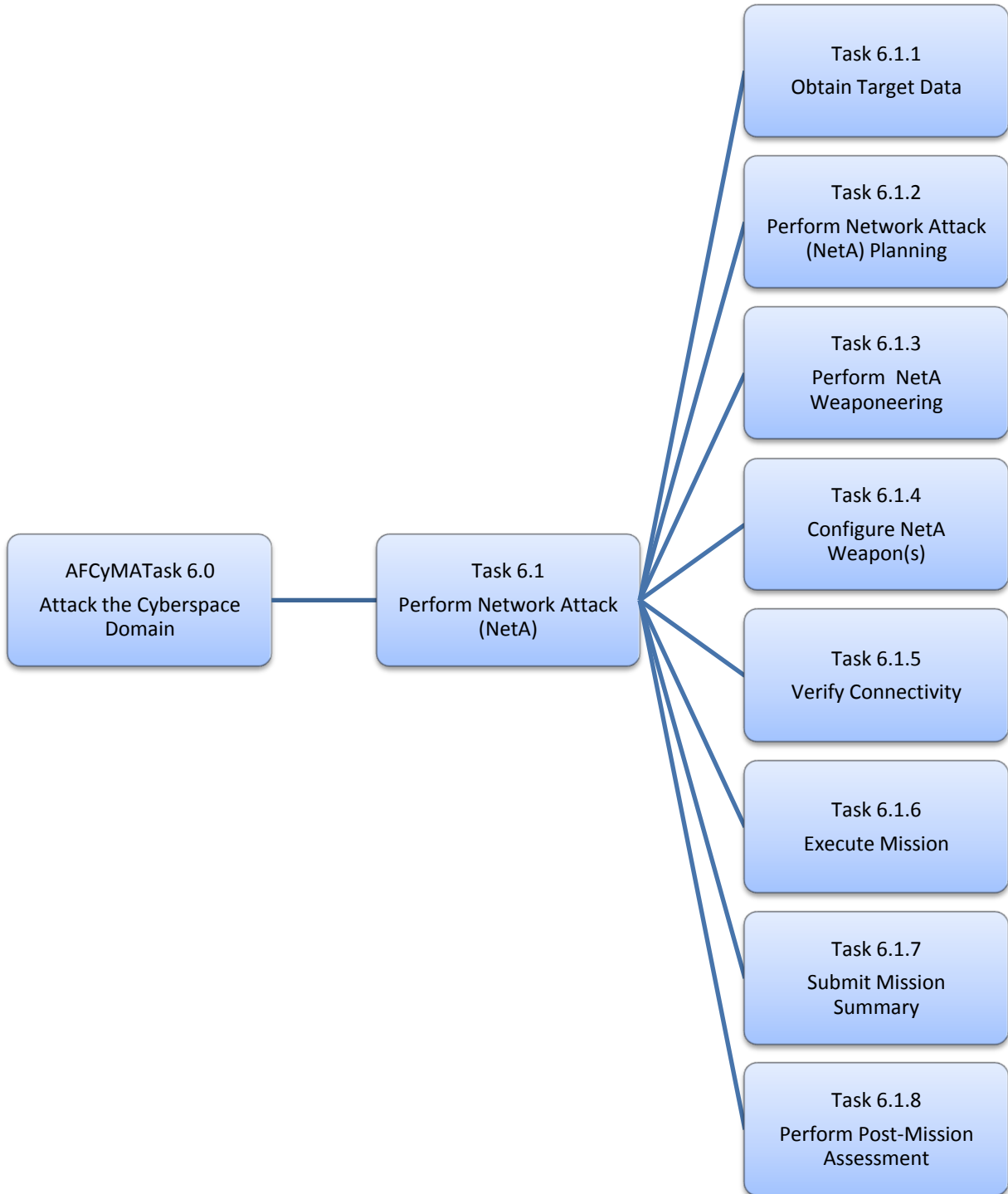


Figure H-1
Task 6.0, Attack the Cyberspace Domain



As of: 20 Mar 09

Attack 1

GREEN

Lead: AFSPC/A3/A8
POC:
AO:

Task Description: Neutralize adversary operations in cyberspace and develop commensurate capabilities (6.1.6, 1.3.1.2)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Up-to-date capabilities (dynamic capability development) 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Freedom of Maneuver • Cyberspace Dominance 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
ATT 1				★																



As of: 20 Mar 09

Attack 2

GREEN

Lead: AFSPC A3
POC:
AO:

Task Description: Develop capabilities that expand or redirect/reorient the decision cycle of an adversary (5.1, 5.2)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • Develop Asymmetric Capabilities 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Adversary's rate of decisions protracted relative to our own • Frame of Reference altered 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
ATT 2				★																



As of: 20 Mar 09

Attack 3

GREEN

Lead: AFSPC/A5/A8
POC:
AO:

Task Description: Define an asymmetric, capabilities-based defense and attack cyberspace acquisition strategy (1.3.1)

<p>Inputs</p> <ul style="list-style-type: none"> • CONPLANs • OPLANs • CRRA • DPSS 	<p>Milestones</p> <ul style="list-style-type: none"> • TBD 	
<p>Outputs</p> <ul style="list-style-type: none"> • See task Description 		<p>Current Actions</p>
<p>Effects</p> <ul style="list-style-type: none"> • Cyberspace capability advantage maintained 		<p>Significant Issues</p> <ul style="list-style-type: none"> • None

Task	M	A	M	J	J	A	S	O	N	D	J	F	M	A	M	J	J	A	S	O
	A	P	A	U	U	U	E	C	O	E	A	E	A	P	A	U	U	U	E	C
	R	R	Y	N	L	G	P	T	V	C	N	B	R	R	Y	N	L	G	P	T
ATT 3																				★

XXI. Appendix 1, Concept of Operations for Twenty-Fourth Air Force Cyberspace Operations

Appendix 1, *Concept of Operations for Twenty-Fourth Air Force Cyberspace Operations*, describes the initial capability and function of 24 AF to plan, direct, coordinate, C2, execute and assess cyberspace operations and capabilities in support of Air Force and Joint requirements. These functions are presented in terms of the current missions, functions, and capabilities of the Air Force units being assigned to 24 AF.

FOR OFFICIAL USE ONLY

**Concept of Operations
for
Twenty-Fourth Air Force
Cyberspace Operations**



30 March 2009

FOR OFFICIAL USE ONLY

**Concept of Operations
for
Twenty-Fourth Air Force
Cyberspace Operations**

Prepared by:

FLOYD A. MCKINNEY, Colonel, USAF
Director, Plans and Requirements
Air Force Cyber Command (Provisional)

Submitted by:

WILLIAM T. LORD, Major General, USAF
Commander, Air Force Cyber Command
(Provisional)

Approved by:

C. ROBERT KEHLER, General, USAF
Commander
Air Force Space Command

FOR OFFICIAL USE ONLY

Review/Change Log

Date	Description	OPR

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

1.0. PURPOSE4
2.0. OVERVIEW4
 2.1. Background4
 2.2. Summary5
3.0. SITUATION5
 3.1. Time Horizon5
 3.2. Description of the Military Challenge5
 3.3. Assumptions8
 3.4. Risks9
4.0. SYNOPSIS10
 4.1. Desired Effects10
 4.2. Missions of 24 AF Subordinate Units11
5.0. NECESSARY AND ENABLING CAPABILITIES12
 5.1. Necessary Capabilities12
 5.2. Enabling Capabilities14
6.0. REPRESENTATIVE ACTIONS15
7.0. COMMAND RELATIONSHIPS18
 7.1. Organization18
 7.2. USSTRATCOM Interactions18
 7.3. Authorities19
8.0. SUMMARY19
APPENDIX A. ACRONYMS20
APPENDIX B. TERMS AND DEFINITIONS22

1.0. PURPOSE

This concept of operations (CONOP) describes the initial capability and function of the Twenty-fourth Air Force (24 AF) to plan, direct, coordinate, command and control (C2), execute and assess cyberspace operations and capabilities in support of Air Force (AF) and Joint requirements. These functions are presented in terms of the current missions, functions, and capabilities of the Air Force units being assigned to the 24 AF.

2.0. OVERVIEW

2.1. Background

2.1.1. The mission of the AF is to “fly, fight, and win...in air, space, and cyberspace.” The AF considers cyberspace to be a physical domain, like those of air, land, sea and space. The Department of Defense defines cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers, as depicted in Figure 1.

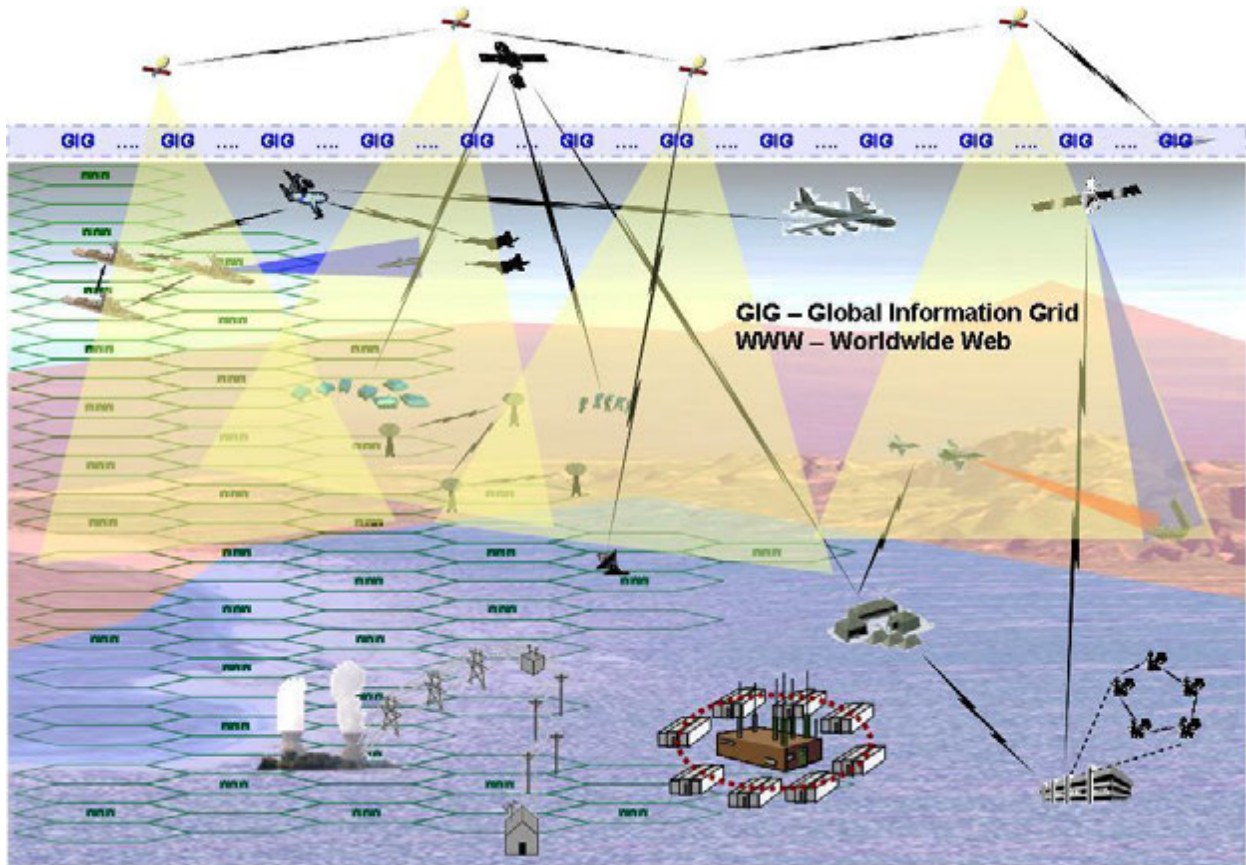


Figure 1. Cyberspace Representation

FOR OFFICIAL USE ONLY

2.1.2. To fully leverage the cyberspace portion of the AF mission, the Secretary of the Air Force approved a concept at Corona Fall 2008 to create a cyberspace Component Numbered Air Force (C-NAF). To implement this direction and Headquarters Air Force (HAF) Program Action Directive (PAD) 07-08 (Change 3), the AF established 24 AF Air Forces Strategic (AFSTRAT). The 24 AF mission is to deliver cyberspace superiority through persistent and responsive world-class networks and cyber forces.

2.2. Summary

2.2.1. To accomplish 24 AF's mission through all phases of military operations, numerous cyber capabilities are required. These include, but are not limited to, the ability to establish access, perform network maintenance, and conduct: Network Defense (NetD), Network Warfare Support [NS, includes Network Exploitation (NetE)], Network Attack (NetA), Air Force Network Operations (AFNetOps). These are described in detail in section 5.

2.2.2. The commander of 24 AF is Commander of Air Force Forces (COMAFFOR) to Joint Task Force-Global Network Operations (JTF-GNO) for NetD operations. As COMAFFOR, under US Strategic Command (USSTRATCOM), 24 AF/CC provides command and control of assigned and attached cyberspace forces to facilitate integration of air, space, and cyberspace capabilities to achieve cyberspace superiority. 24 AF/CC will provide forces through Joint Functional Component Commander for Network Warfare (JFCC-NW) to USSTRATCOM for NetA operations. The 24 AF Commander also provides expeditionary communications and information (EC&I) forces to Geographic Combatant Commands (GCC) with communication capabilities to support operations across the range of military operations.

2.2.3. Many AF cyberspace forces fight in place. Security of the homeland provides these forces increased freedom from physical attack. This freedom facilitates the ability to plan and project power in the manner and time best suited to achieve objectives in support of the joint and interagency efforts to secure and control the cyberspace domain. These forces, together with the rest of 24 AF and Air Force Space Command (AFSPC), ensure the integrity and freedom of movement throughout cyberspace.

3.0. SITUATION

3.1. Time Horizon

This concept is ready for immediate implementation, upon standup of 24 AF in accordance with HAF PAD 07-08 (Change 3) and AFSPC Programming Plan for Twenty-fourth AF Activation.

3.2. Description of the Military Challenge

3.2.1. The 24 AF provides integrated AFNetOps and network warfare operation (NW Ops) capabilities to Combatant Commanders (CCDRs) in support of their strategic objectives across the full range of military operations. To do this, 24 AF will provide operational ready forces able to deploy quickly and employ globally. It will effectively command and control these

FOR OFFICIAL USE ONLY

forces in support of operations. Its primary mission is to protect the AF portion of the Department of Defense (DoD) Global Information Grid (GIG), also known as the AF-GIG.

3.2.2. This mission is conducted by the Total Force. The Total Force offers the exceptional experience and esprit de corps inherent in units populated with personnel that have performed the same role with the same team for many years. The Total Force must be finely tailored, accessible to the joint commander, and configured to operate with other agencies and international partners in complex operations. It must have great endurance. It must be trained, ready to operate, able to make decisions in traditionally non-military areas, and adaptable. As identified in the 2006 Quadrennial Defense Review, the balance of skills should ensure accessibility to the right forces at the right time. The Total Force also should be prepared to compete for the highly-skilled work force intrinsic to the complex mission sets of 24 AF.

3.2.3. A significant challenge for 24 AF, for both offensive and defensive operations, is the size and complexity of the cyberspace domain (Figure 2) and the extensive collection of nodes that AF networks touch. As AF dependence upon this network expands, so does its need to ensure its freedom of movement. Almost everything the AF does requires access to networks and protecting these networks from external and internal threats is a continuous task. Specific examples include, but are not limited to, planning, operations, and acquisitions.

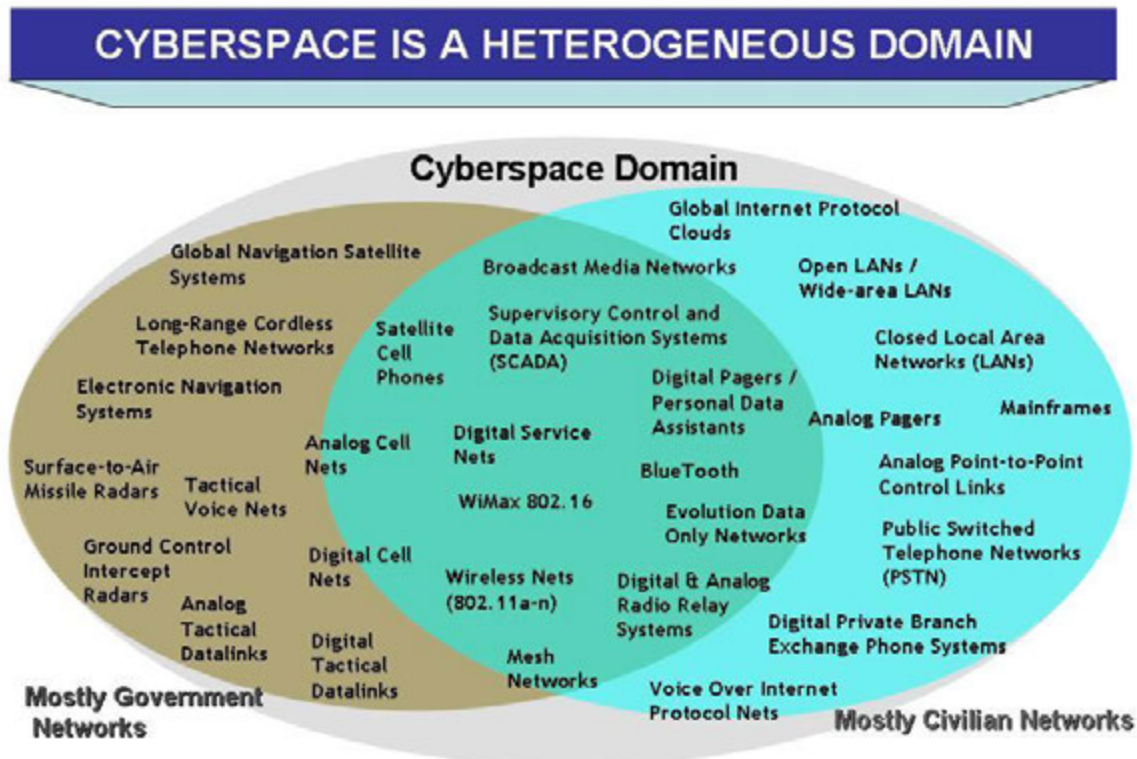


Figure 2. Cyberspace Domain

FOR OFFICIAL USE ONLY

3.2.4. Most of the interconnected networks are not owned by the AF or even the military, but are public, private, commercial, or other government entities throughout the world, as depicted in Figure 3, below. This diversity of ownership and control can make coordination extremely difficult and can cause interface issues between these networks and agencies. However, this diversity creates flexibility, assists in resisting enemy actions, and allows for rapid reconstitutions of information paths. Use of these networks can raise legal issues at the local, national, and international levels.

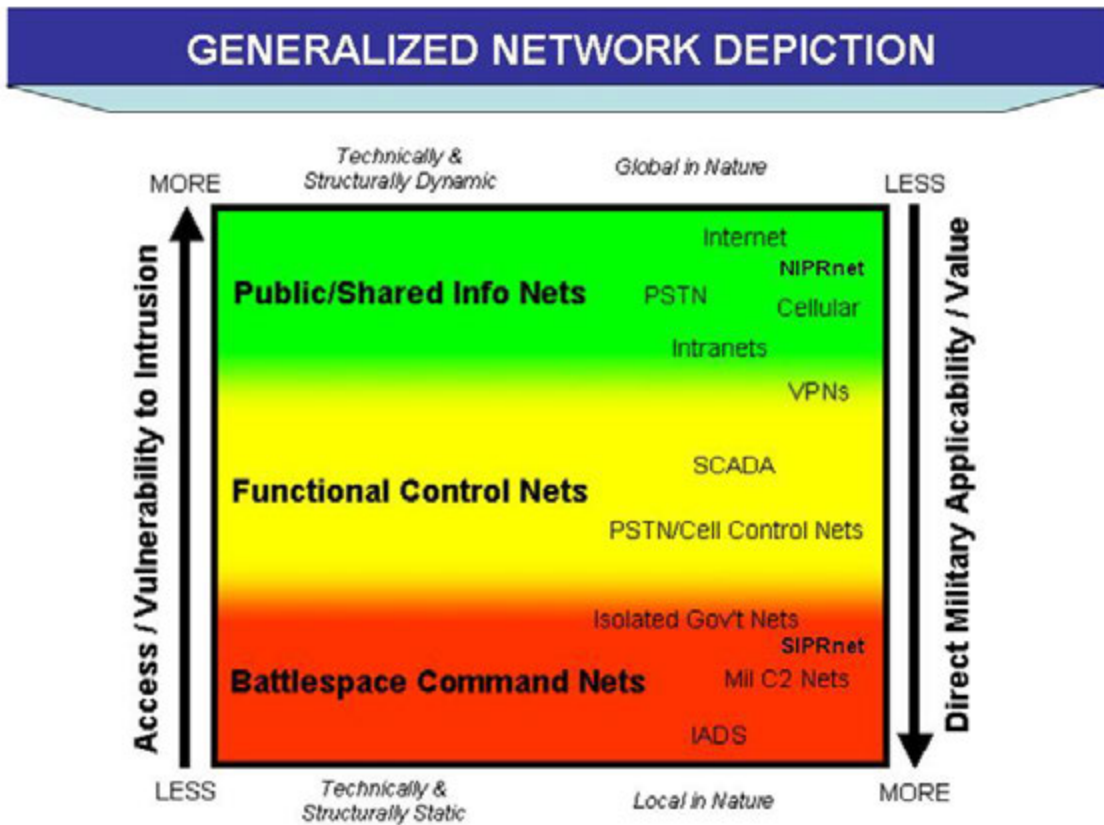


Figure 3. Generalized Network Depiction

3.2.5. In order to produce integrated effects across the spectrum of Agile Combat Support, Global Persistent Attack, Global Strike, Global Mobility, Homeland Defense and Civil Support, Space and C4ISR, and Nuclear Response, Airmen depend upon cyberspace to communicate, coordinate, and command and control operations. Airmen rely upon the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems to meet the commander's intent. The rate of information throughput is critical to enable mission accomplishment and force a desired adversary response. However, potential adversaries are increasingly adept at discovering asymmetric capabilities that challenge the security of AF networks.

3.2.6. The complexity of cyberspace is just as important when looking at an adversary's use. The many users range from individuals to nation states and include terrorists and criminals

FOR OFFICIAL USE ONLY

intermixed with legitimate businesses, international corporations, and defense employees. All these entities establish, maintain, or use segments of cyberspace. The segments they employ consist of networks with differing degrees and means of connectivity, and with nodes and links that usually extend across political boundaries.

3.2.7. This complexity is exacerbated by increasing vulnerabilities, due to:

- rapidly evolving software,
- sophistication and availability of malicious tools,
- increasing amount of information stored on each user-level computer,
- increased capacity and complexity of computers,
- interface issues between various software,
- fulfilling requirements of time compliance network/technical orders and computer security guidance and
- inability to distinguish between normal and abnormal computer activities.

3.2.8. These vulnerabilities offer a fertile environment for adversaries to develop asymmetric capabilities that undermine information assurance (IA) and network defenses. The absence or lack of throughput in continuing education responsive to the changing environment hinders the ability to keep pace with the amorphous and continually transforming threat.

3.2.9. Unlike other orders of battle (OB), the cyberspace OB changes second-by-second, and grows each year, sometimes exponentially, resulting in a changing and complex strategic environment. Keeping up with this constantly changing environment is taxing on cyberspace resources, let alone trying to anticipate the next cyberspace evolution. The AF will need new ways of looking at this rapidly changing environment to effectively use it to further the mission to “Fly, fight, and win in ... cyberspace.”

3.2.10. Inclusion of cyberspace activities in exercise master scenario event lists in order to confirm, reinforce, and socialize unit IA capabilities, processes, and procedures is an AF requirement and increases the probability of successful execution of these processes when real-world incidents occur. Compliance with this requirement presents significant challenges when considering the level of effort and tasking required for the limited resources which conduct cyberspace operations. For example, determining which exercises (e.g. Flag exercise, Operational Readiness Exercise), at what level (Joint or AF), using which heavily tasked unit, attending or scripting inputs, prioritizing funds for exercise participation or classroom training; all represent additional stress.

3.3. Assumptions

3.3.1. All funding and manpower will continue uninterrupted until all units are transitioned to AFSPC.

FOR OFFICIAL USE ONLY

3.3.2. All operations will continue with or without memorandums of agreement, host tenant agreements, or changes in authorities, unless required by law, until all staffs are fully transition and adequately manned to accept responsibilities for their assigned missions.

3.3.3. CCDRs will identify new mission needs in response to adversaries' emerging capabilities and will need to leverage technologies available at any given time to respond. Command and control for those missions requires burgeoning technology to support the development of capabilities to stay ahead of the adversary in all situations.

3.3.4. Current AF cyberspace assets supporting AFNetOps, Network Warfare Operations (NW Ops), and Network Warfare Support (NS) will organize and transfer to wings under 24 AF. Additional future AF cyberspace assets may be assigned to 24 AF.

3.3.5. AF cyberspace force presentation to CCDRs is in accordance with HAF PAD 06-09 to support the USSTRATCOM Cyber Strategy, Cyberspace CONOP, and concept plan / operations plans (CONPLANS/OPLANS).

3.3.6. Air Force Intelligence Surveillance and Reconnaissance Agency (AFISRA), as Service Cryptologic Component (SCC), has oversight of all Signals Intelligence/Computer Network Exploitation (SIGINT/CNE) in the AF (PAD 07-09, NSCID 6, DCID 7/3, USSID SP3000). Network exploitation capability (the 91NWS and 315NWS) will be embedded in 24 AF, with SIGINT oversight from National Security Agency (NSA) through AFISRA as SCC.

3.3.7. *Guidance for Computer Network Defense Response Actions* (Stenbit Memo, dated February 2003) remains in force.

3.3.8. *Trilateral Memorandum of Agreement Among the Department of Defense and Department of Justice and the Intelligence Community Regarding Computer Network Attack and Computer Network Exploitations Activities* (Secret) (dated May 2007) remains in force. This document identifies command relationship authorities with respect to NetA activities.

3.3.9. *Unified Command Plan* (dated December 2008) with respect to cyberspace authorities will remain in effect.

3.3.10. AFSPC/CC will assume responsibilities as the Air Force's Designated Approval Authority (DAA) as assigned by governing authorities as documented in DAA appointment letter.

3.3.11. The Air Force Partnership with Industry Program (PWI) will be directed by the 24 AF as part of their operational responsibility for the integration and execution of cyber-related missions across the Air Force.

3.4. Risks

3.4.1. Interruptions in funding or manning support to 24 AF during the transition period from standup to Full Operational Capability (FOC) could result in lack of protection to the AF-GIG

FOR OFFICIAL USE ONLY

and may lead to the loss of critical information from AF or contractor databases, disruption of information from sensors/sources of intelligence, or other forms of service denial. It is imperative all units continue to provide mission support to 24 AF gained units until 24 AF and its wing staffs are adequately manned to begin management functions.

3.4.2. If an authoritative, active, single-source of cyberspace databases (e.g. malware, non-state actors) is not created or provided, redundant activity and missed opportunities are inevitable, decreasing unity of effort and effectiveness of low density and high demand resources.

3.4.3. If an ability to map the GIG is not developed, the 24 AF will be unable to devise adequate protection strategies.

3.4.4. The continued lack of a single authoritative source for service and joint cyberspace doctrine could undermine 24 AF's ability to accomplish its mission as a result of increased confusion, complexity, and lack of clear roles of responsibility. AF and joint cyberspace doctrine and guidance often conflict in definition or function. Mission or unit specific CONOPS often conflict with AF and Joint doctrine.

3.4.5. If a single point of entry for joint force cyberspace taskings is not established, AF cyberspace unity of command and effort may continue to be adversely effected.

3.4.6. If cyberspace-unique United States Code (USC) Title 10 and USC Title 50 relationships are not more fully defined in rules of engagement, transient high value targets may be missed. Intelligence professionals performing SIGINT activities often cannot share information with operators in an actionable timeframe.

4.0. SYNOPSIS

4.1. Desired Effects

4.1.1. It is the 24 AF Commander's intent to:

4.1.1.1. *Establish and Maintain the Cyberspace Domain.* Effective operations within cyberspace require global expeditionary component cyberspace and network secure operations capabilities and forces to ensure cross-domain freedom of action for the United States and allied forces.

4.1.1.2. *Control the Domain while Exploiting Adversary Vulnerabilities.* Provide C2 to synchronize cross-domain operations and de-conflict friendly use of cyberspace to preserve appropriate command authorities for global and theater-level cyberspace operations. The integrated exploitation of adversary capabilities and vulnerabilities will further enable C2 of USAF cyberspace forces.

4.1.1.3. *Provide Forces to Attack the Adversary Structures.* Offensive operations will gain the military advantage to ensure operational freedom of action through cyberspace attacks on

FOR OFFICIAL USE ONLY

adversary networks, systems, peripherals, and infrastructure though exploiting enemy vulnerabilities. This includes further delivery of cross-domain effects through cyberspace force enhancement, and the conduct of cyberspace support operations.

4.1.1.4. *Use the Domain to Operate and Defend AF Cyberspace Components*. Leverage AF network operations to deny an adversary the ability to diminish AF operations in cyberspace.

4.1.2. In order to meet the commander's intent, the following effects must be achieved:

- Harden USAF assets against cyber attacks, expanding active and passive cyber defense operations and preparing defensive measures to neutralize or limit the effectiveness of adversaries and protect against the exploitation of friendly systems and information.
- Deploy cyberspace attack capabilities able to produce kinetic and non-kinetic effects across all operational domains to deny, degrade, disrupt, disable, or destroy an adversary's infrastructure and warfighting capabilities.
- Creating real-time, persistent, pervasive and cyberspace situational awareness across the network-centric environment; enhancing decision-making through new visualization, planning, and decision tools; and developing an integrated, global C2 architecture to compress the warfighter's decision cycle.

4.2. Missions of 24 AF Subordinate Units

4.2.1. *624th Operations Center (624 OC)*: Protecting the AF-GIG is the primary mission of the 624 OC. The 624 OC plans, directs, and provides command and control of network operations across the AF-GIG under the authority given to the Air Force Network Operations (AFNetOps) Commander

4.2.2. *67th Network Warfare Wing (67 NWW)*: The primary mission of the 67 NWW is to conduct network operations, defense, attack and exploitation, creating integrated air, space and cyberspace effects under the authority of USSTRATCOM. The 67 NWW will provide trained and equipped network forces to USSTRATCOM. Additionally, the 67 NWW will conduct the Electronic Security Systems Assessment (ESSA) mission, which is transitioning to the new Cyber Operations Risk Assessment (CORA) mission.

4.2.3. *688th Information Operations Wing (688 IOW)*: 688 IOW is responsible for creating the information operations advantage for combatant forces through exploring, developing, applying and transitioning counter-information technology, strategy, tactics and data to control the information environment.

4.2.4. *689th Combat Communications Wing (689 CCW)*: 689 CCW's primary mission is to organize, train, and equip cyber forces to extend and sustain the AF-GIG in support of theater commanders and AFSPC operations. The Wing's capabilities include combat communications, engineering and installation, radar evaluation, cyberspace architecture, lead command

FOR OFFICIAL USE ONLY

management, assessment/validation, and Communications and Information (C&I) maintenance / sustainment.

5.0. NECESSARY AND ENABLING CAPABILITIES

5.1. Necessary Capabilities

The following necessary capabilities produce the 24 AF desired effects within cyberspace:

5.1.1. *The ability to establish access:* Effective operations within cyberspace require global unfettered access to ensure cross-domain freedom of action. Access and infrastructure is provided at the base-level by local communication squadrons in conjunction with the AF Network Integration Center (formerly AF Communications Agency), and the host MAJCOM. However, once local organizations are connected, C2 is provided by 24 AF.

5.1.1.1. 689 CCW provides expeditionary operations to establish and sustain the cyberspace domain at garrison and bare bases during peacetime and contingency/wartime situations. It activates expeditionary communications and expands services to achieve full operating capability and provides operational commanders with communication capabilities to support operations across the range of military operations. These forces support air operations by enabling C2, intelligence, logistics, medical, and other mission support functions from initial deployment through redeployment. The objective is to communicate information rapidly, accurately, and securely to achieve interoperability between deployed AF, joint, and coalition elements throughout the theater and with reach-back C2 centers.

5.1.2. *The ability to conduct NetD:*

5.1.2.1. 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. Responses to attacks in cyberspace depend on the situation, attack method, and network involved. The most effective response may simply be to increase security measures or isolation of the target network which must be weighed against mission impact. Network defense capabilities, however, go beyond just network-based and include all capabilities required to support this mission and the practical layered defense strategy. This approach can be applied to all networks and cyberspace.

5.1.2.2. Defensive activities are divided into three major components: active, passive and inherent. Active defenses are measures taken to directly counter adversary activities to penetrate the network or actions taken to terminate an ongoing intrusion. Passive defenses are security-related activities such as malware detection, port security and system configuration. Passive defense maintains the network security posture and prepares defenders to assist with active defense activities. Inherent defense identifies the capabilities implemented in the design of the system itself to support passive and active defensive measures.

5.1.3. *The ability to conduct Network Warfare Support (NS):* NS activities are tasked by or under direct control of an operational commander to search for, intercept, identify, and locate or

FOR OFFICIAL USE ONLY

localize sources of access and vulnerability for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. NS includes both NetE and Intelligence Preparation of the Operational Environment (IPOE), which are also enabling capabilities. NetE is defined as enabling operations and intelligence collection capabilities to gather data from target or adversary automated information systems or networks. NetE is accomplished under the SCC (USC Title 50) authority of the AFISRA Commander. IPOE is similar to NetE, but is accomplished under USC Title 10 authorities. Without NS, 24 AF would be unable to adapt to the changing threat environment.

5.1.4. *The ability to conduct NetA:* NetA is the employment of network-based capabilities to destroy, deceive, disrupt, corrupt, or usurp information resident in or transiting through networks. Networks include telephone and data service networks. NetA capabilities are entirely dependent on access to the target network. This sometimes requires mechanisms specifically designed for the purpose of providing or enabling that access. Cyberspace attacks can be conducted on an adversary's terrestrial, airborne, and space-based communication infrastructure, as well as, his forces, equipment and logistics. The purpose of NetA is to increase the decision cycle of the enemy thereby providing our commander's with strategic and operational advantages.

5.1.5. *The ability to conduct AFNetOps:* NetOps are those activities conducted to operate and defend the Global Information Grid (GIG). It is comprised of network attack, network defense, and related network exploitation enabling operations. AFNetOps is the service-level activity to provide the global-level operational planning and command and control to operate and defend the Air Force provisioned portion of the GIG (AF GIG). It integrates planning and employment of military capabilities to provide the friendly net environment needed to plan, control and execute military operations and conduct service functions. AFNetOps provides the three operational elements of information assurance (IA), network/system management (N&SM), and information dissemination management (IDM). This capability is provided by the 24 AF and performed by assigned 67 NWW and AF Computer System Administrators

5.1.5.1. Information assurance protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. 24 AF/CC's lead role in the AF Partnership with Industry Program (AFPWI) falls into this element. It enables the AF to assist its Defense Industrial Base (DIB) partners in securing their unclassified networks, particularly against the Advanced Persistent Threat and thus extends protection of future and present capabilities. The AFPWI Program represents the Air Force's participation in the DoD DIB Cyber Security effort.

5.1.5.2. Network/system management is the execution of the set of activities required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a telecommunications network. This includes performing actions such as initial network planning, frequency allocation, predetermined traffic routing. This is performed to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management. Configuring and allocating AF-GIG system and network resources, ensures effective and efficient processing,

FOR OFFICIAL USE ONLY

connectivity, routing, and information flow; accounting for resource usage; and maintaining robust AF-GIG capabilities in the face of component or system failure and/or adversarial attack.

5.1.5.3. Information dissemination management provides the right information to the right person, in the right format, at the right place and time in accordance with commanders' information dissemination policies. IDM optimizes the use of information infrastructure resources and involves the compilation, cataloging, caching, distribution, and retrieval of data to manage information flow to users.

5.1.6. *The ability to perform network maintenance:* Network maintenance consists of organizations, procedures, and functionalities to plan, administer, and monitor AF networks in support of operations and to respond to threats, power outages, and other operational impacts. It includes the continuous oversight and management of Air Force-wide networks. Maintenance of the cyber domain is inextricably linked to defense and often employs the same units, personnel, and equipment.

5.1.7. *The ability to establish and maintain cyber situational awareness (CSA):* Cyber situational awareness is the global visibility of computer networks across the electromagnetic spectrum and the forces, actors, and conditions capable of influencing the cyber domain and cyberspace operations. This requires continuous, near real-time, non-personnel intensive, assessments and status reporting of all blue, red, and gray cyberspace operational capabilities. This capability is provided by the 24 AF and performed by assigned 67 NWW cyber operators.

5.2. Enabling Capabilities

The following capabilities facilitate achievement of the desired effects:

5.2.1. *The ability to conduct frequency management:* This includes requesting, recording, deconfliction of and issuance of authorization to use frequencies (operate electromagnetic spectrum dependent systems) coupled with monitoring and interference resolution processes. AFSPC will provide this capability.

5.2.2. *The ability to educate and train:* The ability to provide cyberspace warriors to the 24 AF mission is critical. The ability to maintain a training throughput to ensure 24 AF manpower positions are fully staffed is essential. The implementation and completion of tasks outlined in the Roadmap for Development of Cyberspace Professionals ensures fully educated and trained AF personnel are available to execute the 24 AF mission. Air Education and Training Command and 24 AF share responsibility for this capability.

5.2.3. *The ability to acquire and sustain:* Requirements generation, request for proposals, development, testing, fielding and sustainment processes must keep pace with the rate of information technology change and the unique requirements of the cyber mission. These processes must remain responsive to adversary asymmetries. Cyberspace acquisition strategy and delivery capabilities enable 24 AF to leverage Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) products to ensure AF weapons systems dominate in cyberspace. Rapid acquisition programs that provide quick reaction solutions are a key enabling

FOR OFFICIAL USE ONLY

capability across the cyber domain. The AF Acquisition Community provides this enabling capability in coordination with the AFSPC.

6.0. REPRESENTATIVE ACTIONS

The following 24-AF actions consist of ways in which commanders employ cyberspace capabilities to accomplish desired effects.

Capability	Inputs	24 AF Activities	Output
Provide global connectivity (Establish Access and frequency management)	GCC or installation's requirements	A4/6, 689 CCW, & 85 th Engineering and Installation Squadron (85 EIS) Scope need, engineer network, install network (computer and communications)	Interconnected networks
Provide global connectivity (Frequency Operations)	Joint Frequency Management Office, Electronic Warfare Coordination Cell, JTF Spectrum Management Element, and AFFMA	A2/3, 624 OC, 689 CCW, 85 EIS Scope interference issues and propose/engineer solutions	Capable networks
Shared SA and Understanding (NS)	Data on adversary and friendly force capabilities, activities, and intentions; USSTRATCOM directives; AFSPC inputs; supported MAJCOM requirements; inputs from other operations centers	A2/3 and/or 624 OC: Conduct daily staff battle rhythm, to include daily briefings and meetings Monitor current operations and unit operational situation reports Coordinate information and display tasks in ops center Confirm current operational picture	Shared knowledge of current adversary/friendly forces and forecasts

FOR OFFICIAL USE ONLY

Capability	Inputs	24 AF Activities	Output
Ability to plan collaboratively & leverage mission partners (NetA&D)	Commanders Intent; NS; GCC 2 nd and 3 rd order effects;	A-2/3/5 and/or 624 OC: Conduct JOPES Course of Action (COA) development Identify and coordinate reach back efforts to other Air Force analytic organizations Manage all-source collection	Approved plan
Ability to synchronize execution of cyberspace operations across all domains (NetA&D)	Approved plan, ROE, limiting factors, IPOE	A-3 and/or 624 OC: Provide real-time display of significant activities for all components to input and share Share operational timeline including actions, reactions, counteractions, and supporting actions (e.g., logistics, Intelligence, Surveillance, and Reconnaissance (ISR) Baseline normal network traffic; assess risks to networks, detect anomalous activities; identify attack and estimate impact; notification of attack; contain/mitigate the incident	Military effects
Ability to assess effects and adapt operations (NS, NetA&D)	Plan, mission execution, initial results, and Measures of Effectiveness (MOE)	A-2/3: Conduct change assessment, functional damage assessment and target system assessment against MOEs Determine if reallocation of forces is appropriate	Mission effectiveness report, Tactics, Techniques, and Procedures (TTPs), or replan
Ability to train forces (educate and train)	Initial Qualification Training (IQT) /	A3, OV, & below wing-level units:	Trained and ready force

FOR OFFICIAL USE ONLY

Capability	Inputs	24 AF Activities	Output
	Mission Qualification Training (MQT)/upgrade requirements, SORTs reports	Monitor unit strengths and process personnel assignment and performance reports Maintain evaluation reports (Forms 8) Operate and maintain contingency manpower and resource management systems Conduct mission training and evaluations Participation in Joint and AF exercises	
Maintain and operate networks (AFNetOps and network maintenance)	IA policies and guidance, requirements, technical orders, error reports, trouble tickets, TCTOs, MTOs, identified vulnerability, cryptographic key materials	A-3, 67 NWW & 624 OC: Prioritize and allocate resources Provide assured and timely network-centric services Provide global connectivity and services, in addition to C2 of those services Support the doctrinal concept of centralized control and decentralized execution of AFNetOps assets Provide unit interoperability and interchangeability Plan and conduct AFNetOps on a 24 hours-a-day/7days-a-week (24/7) basis	An operational network that meets customers' needs
Respond to evolving technology or changing threat	Requirements, concepts, acquisition	A2/3/4/5/6/8 & units: Issue requests for proposals	Delivered hardware, software, or

FOR OFFICIAL USE ONLY

Capability	Inputs	24 AF Activities	Output
environment (acquisition and sustainment)	guidance	Obtain COTs and GOTs Develop operational concept Testing	process solutions

7.0. COMMAND RELATIONSHIPS

7.1. Organization

7.1.1. Command relationships vary depending on nature of the operation and whether effects occur in an individual theater, multiple theaters, or globally. AF-GIG NetD forces are presented through the 624 OC to JTF-GNO. NetA Forces are requested through the 624 OC but are OPCON/TACON by JFCC-NW. In the case of NetA, JFCC-NW’s commander is responsible for planning, executing, and assessing operations conducted by service component cyberspace forces while serving as either a supported or supporting commander. Embedded 24 AF personnel within Air and Space Operations Centers (AOCs) and functional component commander planning staffs ensure ready availability of subject matter expertise. If 24 AF personnel are not embedded in an AOC, reach-back support for AFNetOps will be provided to the IO cell through the 624 OC.

7.1.2. USJFCOM will exercise C2 of expeditionary communications and information (combat communications) units during deployment in support of CCDR’s operational requirements. C2 transitions to GCC upon arrival and is maintained by the CCDR until redeployment. ACC will retain DIRLAUTH with the 3 CCG, 5 CCG, and ARC combat communications units as required.

7.2. USSTRATCOM Interactions

7.2.1. Strategic level interaction with USSTRATCOM is conducted by the HQ AFSPACE staff. This interaction includes:

- Component-level input to conduct cyberspace operations.
- Studies to examine deterrence of cyberspace attacks.

7.2.2. Operational- and tactical-level interaction with USSTRATCOM includes:

- Dissemination of AFNetOps tasking orders.
- Implementation of “patches” directed by tasking orders.
- Synchronization of cyberspace operations with kinetic operations.
- Planning to enable mission execution of cyberspace operations.

7.3. Authorities

Figure 4 represents the Combatant Command (COCOM), Operational Control (OPCON), Tactical Control (TACON), and Administrative Control (ADCON) authorities envisioned for 24 AF and AFSPC.

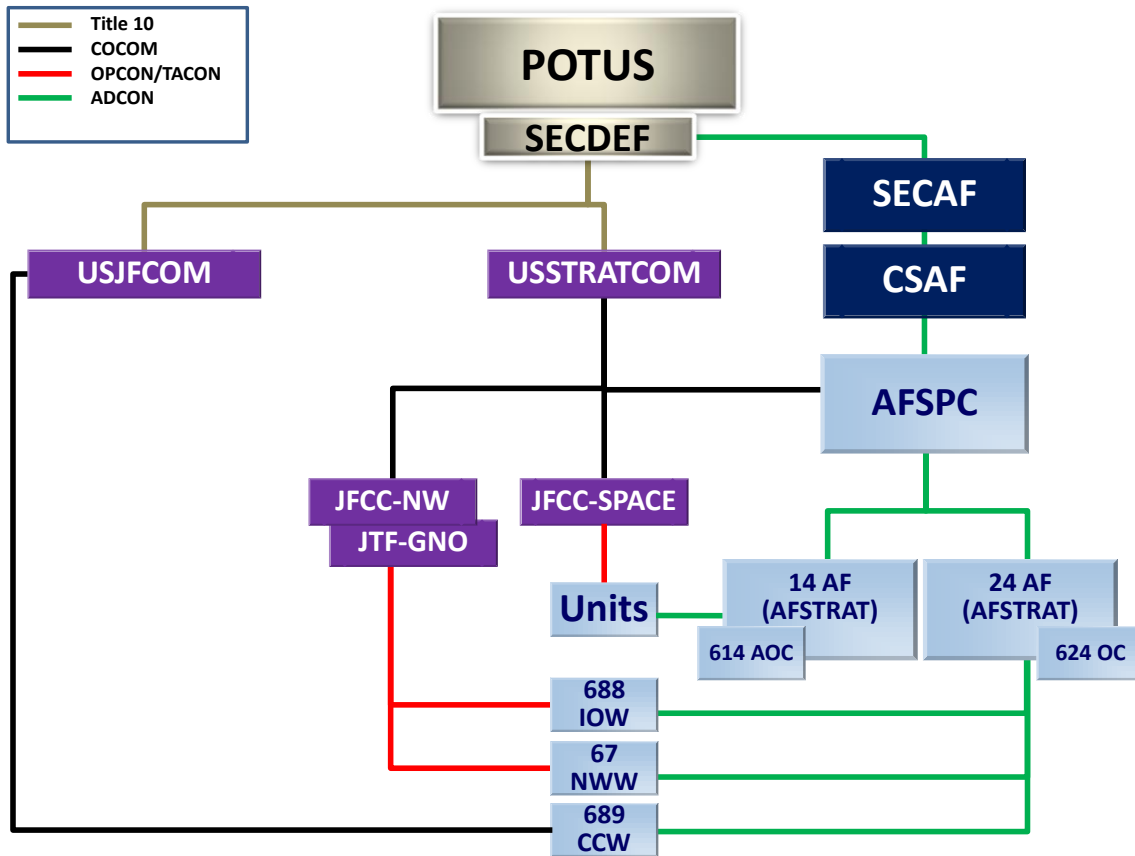


Figure 4. Command Relationships

8.0. SUMMARY

The 24 AF is a C-NAF subordinate to AFSPC and USSTRATCOM. The organizational structure of 24 AF is in accordance with PAD 06-09, PAD 07-13, and PAD 07-08 (Change 3). The primary missions of the 24 AF are defense of the AF-GIG, and force provider of NetE and NetA capabilities. The 67 NWW, 624 OC, 688 IOW, and 689 CCW are subordinate units to 24 AF. Force presentation for NetD is through the 624 OC to JTF-GNO. The C2 of AF NetD is conducted by the 624 OC. Force presentation for NetA is through the 624 OC to JFCC-NW. However, JFCC-NW conducts C2 of AF NetA forces. Combat communications forces are presented to U.S. Joint Forces Command for deployment to GCCs.

FOR OFFICIAL USE ONLY

APPENDIX A. ACRONYMS

ACRONYM	DEFINITION
ADCON	Administrative Control
AF	Air Force
AFFOR	Air Force Forces
AF-GIG	Air Force Global Information Grid
AFISRA	Air Force Intelligence, Surveillance, and Reconnaissance Agency
AFFMA	Air Force Frequency Management Agency
AFNetOps	Air Force Network Operations
AFSPC	Air Force Space Command
AFSTRAT	Air Forces Strategic
AOC	Air and Space Operations Center
C&I	Communications and Information
C2	Command and Control
CCDR	Combatant Commander
CCW	Combat Communications Wing
C-NAF	Component - Numbered Air Force
CNE	Computer Network Exploitation
COA	Course of Action
COCOM	Combatant Command
COMAFFOR	Commander of Air Force Forces
CONOPS	Concept of Operations
CONPLAN	Concept Plan
CORA	Cyber Operations Risk Assessment
COTS	Commercial-Off-The-Shelf
DCID	Director of Central Intelligence Directive
DoD	Department of Defense
EIS	Engineering and Installation Squadron
ESSA	Electronic Systems Security Assessment
FOC	Full Operational Capability
GCC	Geographic Combatant Command
GIG	Global Information Grid
GOTS	Government-Off-The-Shelf
HAF	Headquarters Air Force
IA	Information Assurance
IDM	Information Dissemination Management
IOW	Information Operations Wing
IPOE	Intelligence Preparation of the Environment
IQT	Initial Qualification Training
ISR	Intelligence, Surveillance, and Reconnaissance
JFCC	Joint Functional Component Command
JFCC-NW	Joint Functional Component Commander for Network Warfare
JOPES	Joint Operation Planning and Execution System

FOR OFFICIAL USE ONLY

ACRONYM	DEFINITION
JTF-GNO	Joint Task Force - Global Network Operations
MAJCOM	Major Command
MOE	Measures of Effectiveness
MQT	Mission Qualification Training
N&SM	Network and Systems Management
NAF	Numbered Air Force
NetA	Network Attack
NetD	Network Defense
NetE	Network Exploitation
NetOps	Network Operations
NS	Network Warfare Support
NSA	National Security Agency
NSCID	National Security Council Intelligence Directive
NW Ops	Network Warfare Operations
NW	Network Warfare
NWW	Network Warfare Wing
OB	Order of Battle
OC	Operations Center
OPCON	Operational Control
OPLAN	Operation Plan
ORE	Operational Readiness Exercise
PAD	Program Action Directive
SCC	Service Cryptologic Component
SIGINT	Signals Intelligence
TACON	Tactical Control
TTP	Tactics, Techniques, and Procedures
USC	United States Code
USSID	United States Signals Intelligence Directive
USSTRATCOM	United States Strategic Command

FOR OFFICIAL USE ONLY

APPENDIX B. TERMS AND DEFINITIONS

TERM	DEFINITION
Action	The performance of an activity. An act or actions are taken in order to create a desired effect. Actions may be kinetic (physical, material) or non-kinetic (logical, behavioral). Actions are invariably tactical, usually producing tactical level direct effects. (AFDD 2)
Administrative Control	Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. (JP 1)
Air Force Global Information Grid	The Air Force portion of the globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid (GIG) includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense (DOD), National Security, and related intelligence community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems. (JP 1-02)
Air Force Network Operations	The AF-level command and control for the Air Force provisioned portion of the DoD Global Information Grid (GIG). (AFI 10-711 [DRAFT])
Adversary	A party with whom one has a conflict, peaceful or otherwise. (AFDD 2)
Air and Space Operations Center	The senior agency of the Air Force component commander that provides command and control of Air Force air and space operations and coordinates with other components and Services. (AFDD 2)

FOR OFFICIAL USE ONLY

TERM	DEFINITION
Battlespace	The environment, factors, and conditions which must be understood to successfully apply combat power, protect the force, or complete the mission. This includes air, land, sea, space, enemy and friendly forces, facilities, weather, terrain, the electromagnetic spectrum, and information environment within the operational areas and areas of interest. (JP 1-02)
Combatant Command	Nontransferable command authority established by title 10 (“Armed Forces”), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command. (JP 1)
Combatant Commander	A commander of one of the unified or specified combatant commands established by the President. (JP 3-0)
Command and Control	The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP 1)
Commander, Air Force Forces	The senior U.S. Air Force officer designated as commander of the U.S. Air Force component assigned to a joint force commander (JFC) at the unified, sub-unified, and joint task force level. In this position, the COMAFFOR presents the single U.S. Air Force voice to the JFC. (AFDDs 1, 2)

FOR OFFICIAL USE ONLY

TERM	DEFINITION
Computer Network Exploitation	Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (JP 1-02)
Concept of Operations	A verbal or graphic statement that clearly and concisely expresses what the joint force commander intends to accomplish and how it will be done using available resources. The concept is designed to give an overall picture of the operation. (JP 5-0)
Concept Plan	In the context of joint operation planning level 3 planning detail, an operation plan in an abbreviated format that may require considerable expansion or alteration to convert it into a complete operation plan or operation order. (JP 5-0)
Cyberspace	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 1-02).
Cyberspace Operations	The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (CJCS CM-0527-08)
Cyber Situational Awareness	The systems and information to provide global visibility on computer networks across the electromagnetic spectrum and the forces, actors, and conditions capable of influencing that battlespace that involve cyberspace operations.
Cyberspace Superiority	The degree of dominance in cyberspace of one force over another that permits the conduct of operations by the former and its related land, air, sea, space, and special operation forces at a given time and place without prohibitive interference by the opposing force. (AFDD 2-11).
Denial	A form of coercion strategy that destroys or neutralizes a portion of the adversary's physical means to resist. (AFDD 2)
Education	Instruction and study focused on creative problem solving that does not provide predictable outcomes. Education encompasses a broader flow of information to the student and encourages exploration into unknown areas and creative problem solving. (AFDD 1-1)

FOR OFFICIAL USE ONLY

TERM	DEFINITION
Effect	1. The physical or behavioral state of a system that results from an action, a set of actions, or another effect. 2. The result, outcome, or consequence of an action. 3. A change to a condition, behavior, or degree of freedom. (AFDD 2)
Information Assurance	Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 1-02)
Information Dissemination Management	The subset of information management with a supporting infrastructure that addresses awareness, access, and delivery of information. The primary mission is to provide the right information to the right person, in the right format, at the right place and time in accordance with commanders' information dissemination policies while optimizing the use of information infrastructure resources. It involves the compilation, cataloging, caching, distribution, and retrieval of data; manages the information flow to users; and enables the execution of the commanders' information dissemination policy. (AFDD 2-5)
Information Operations	The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (JP 1-02)
Intelligence Preparation of the Environment	IPOE is a key tool for conducting intelligence analysis and production. This is a four-step systematic process of analyzing the environment and threat in order to help commanders understand the variables that can influence the mission and operations. In step one, commanders and analysts define the operational environment. Step two is to describe the impact of the operational environment on operations. Step three is to evaluate the adversary and step four entails determining and describing the adversary's course(s) of action. (AFDD 2-11)
Information Technology	An umbrella term describing the suite of tools used for managing and processing information. These tools can include any communications device or computer, its ancillary equipment, software applications, and related supporting resources. (AFDD 2-5)

FOR OFFICIAL USE ONLY

TERM	DEFINITION
Intelligence, Surveillance, and Reconnaissance	Integrated capabilities to collect, process, exploit and disseminate accurate and timely information that provides the battlespace awareness necessary to successfully plan and conduct operations. (AFDD 2-5.2)
Joint Operation Planning and Execution System	A system of joint policies, procedures, and reporting structures, supported by communications and computer systems, that is used by the joint planning and execution community to monitor, plan, and execute mobilization, deployment, employment, sustainment, redeployment, and demobilization activities associated with joint operations. (JP 5-0)
Kinetic	Relating to actions that involve the forces and energy of moving bodies, including physical damage to or destruction of targets through use of bombs, missiles, bullets, and similar projectiles. (AFDD 2-1.9)
Malware	Software such as viruses or Trojans designed to cause damage or disruption to a computer system. (AFDD 2-11)
Measure of Effect	Independent qualitative or quantitative empirical measure assigned to an intended effect against which the effect's achievement is assessed. (AFDD 2)
Network Attack	The employment of network-based capabilities to destroy, disrupt, corrupt, or usurp information resident in or transiting through networks. Networks include telephony and data services networks. (AFDD 2-5)
Network Defense	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)
Network Exploitation	Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (JP 1-02)
Network Operations	The capability to establish, operate, and maintain our vital "backbone" networks in cyberspace. (AFDD 2-11)

FOR OFFICIAL USE ONLY

TERM	DEFINITION
Network Warfare Operations	Network warfare operations are the integrated planning, employment, and assessment of military capabilities to achieve desired effects across the interconnected analog and digital network portion of the battlespace. Network warfare operations are conducted in the information domain through the combination of hardware, software, data, and human interaction. Networks in this context are defined as any collection of systems transmitting information. The operational activities of network warfare operations are network attack (NetA), network defense (NetD) and network warfare support (NS). (AFDD 2-5)
Network Warfare Support	Actions tasked by or under direct control of an operational commander to search for, intercept, identify, and locate or localize sources of access and vulnerability for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. (AFDD 2-5)
Non-kinetic	Relating to actions that produce effects without direct use of the force or energy of moving objects, including such means as electromagnetic radiation, directed energy, and information operations. (AFDD 2-1.9)
Operational Control	Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. (JP 1)

FOR OFFICIAL USE ONLY

TERM	DEFINITION
Operation Plan	1. Any plan for the conduct of military operations prepared in response to actual and potential contingencies. 2. In the context of joint operation planning level 4 planning detail, a complete and detailed joint plan containing a full description of the concept of operations, all annexes applicable to the plan, along with a time-phased force and deployment data. It identifies the specific forces, functional support, and resources required to execute the plan and provide closure estimates for their flow into the theater. (JP 5-0)
Operational Environment	A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)
Order of Battle	The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. (JP 2-01.3)
Reachback	The process of obtaining products, services, and applications or forces, equipment, or materiel from Air Force organizations that are not forward deployed. (AFDD 2-8)
Space Control	Combat, combat support, and combat service support operations to ensure freedom of action in space for the US and its allies and, when directed, deny an adversary freedom of action in space. The space control mission area includes: surveillance of space; protection of U.S. and friendly space systems; prevention of an adversary's ability to use space systems and services for purposes hostile to U.S. national security interests; negation of space systems and services used for purposes hostile to U.S. national security interests; and directly supporting battle management, command, control, communications, and intelligence. (JP 1-02)
Tactical Control	Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of combatant command. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. (JP 1)

FOR OFFICIAL USE ONLY

TERM	DEFINITION
Total Force	The U.S. Air Force organizations, units, and individuals that provide the capabilities to support the Department of Defense in implementing the national security strategy. Total Force includes regular Air Force, Air National Guard of the US, and Air Force Reserve military personnel, U.S. Air Force military retired members, U.S. Air Force civilian personnel (including foreign national direct- and indirect-hire, as well as non-appropriated fund employees), contractor staff, and host-nation support personnel. (AFDD 2)
War	Open and often prolonged conflict between nations (or organized groups within nations) to achieve national objectives. (AFDD 1)

XXII. Appendix 2, Command & Control and Operations of Cyberspace Forces, 10 Mar 2009, Change 3

Appendix 2, *Command & Control and Operations of Cyberspace Forces, 10 Mar 2009, Change 3*, further details how 24 AF, in its C-NAF role and from an operating center perspective, will conduct full spectrum offensive and defensive cyber operations. This appendix describes how the 624 Operations Center will fulfill its warfighter responsibilities and how it will C2 cyberspace forces.

24th Air Force



Command & Control and Operations of
Cyberspace Forces

10 Mar 2009

Change 3

TABLE OF CONTENTS

1. INTRODUCTION	1
2. EXECUTIVE SUMMARY	2
3. LEGAL AUTHORITIES OF THE AFNETOPS COMMANDER.....	5
3.1. NETWORK DEFENSE	6
3.1.1. <i>Service Provider</i>	6
3.1.2. <i>Warfighter</i>	6
3.1.3. <i>Law Enforcement</i>	7
3.1.4. <i>Intelligence</i>	7
3.2. DESIGNATED APPROVAL AUTHORITY (DAA).....	7
3.2.1. <i>Network Defense</i>	7
3.2.2. <i>Intelligence Requests</i>	8
4. IMPLEMENTATION CONSIDERATIONS	8
4.1. TIMEFRAME.....	8
4.2. ASSUMPTIONS	8
4.3. RISKS	10
5. CHALLENGES TO CYBER OPERATIONS FOR 24 AF.....	10
6. CYBER OPERATIONS AT THE OPERATIONAL LEVEL OF WAR.....	13
6.1. CONDUCTING CYBER OPERATIONS	13
6.2. OPERATIONAL DEFENSE OF THE AF GIG	14
6.3. MISSION ASSURANCE.....	14
6.4. COMMAND AND CONTROL OF CYBER OPERATIONS	15
6.5. COMMAND AND CONTROL OF NETWORK DEFENSE	15
6.5.1. <i>Cyberspace Operations in the CyOC</i>	17
6.5.2. <i>Cyberspace Integration in the CyOC</i>	17
6.5.2.1. Strategy Division	18
6.5.2.2. Combat Plans Division (CPD)	19
6.5.2.3. Combat Operations Division (COD).....	20
6.5.2.4. ISR Division	22
6.5.3. <i>Cyber Coordination Cell</i>	23
6.6. NETWORK OPERATIONS	23
6.6.1. <i>Cyber Control Order</i>	24
6.6.2. <i>Integrated Tasking Order</i>	26
6.6.3. <i>Maintenance Tasking Order</i>	26
7. CYBER REQUIREMENTS	28
7.1. CYBER PLANNING	28
7.1.1. <i>CyOC Planning and Analysis</i>	29
7.2. COMMAND AND CONTROL OF CYBERSPACE OPERATIONS.....	29
7.3. ASSESSING CYBER OPERATIONS	29
7.4. CYBERSPACE SITUATIONAL AWARENESS.....	30
7.5. CYBER AUTHORITIES	30
7.6. RELATIONSHIP WITH AFFOR STAFF	31
8. THE EVOLVING CHALLENGE.....	31
8.1. INTELLIGENCE SUPPORT TO CYBERSPACE OPERATIONS.....	31
8.2. NETWORK SITUATIONAL AWARENESS	31

8.3.	AIR FORCE NETWORK OPERATIONS (AFNETOPS): THE FOUNDATION OF CYBERSPACE OPERATIONS.....	32
8.3.1.	<i>AFNetOps</i>	32
8.3.2.	<i>Integration of Airborne Networks into AFNetOps C2 Construct</i>	32
8.3.3.	<i>Objective Gateways</i>	33
8.4.	CYOC SYSTEMS.....	34
8.5.	IO RANGE AND VISION.....	35
8.6.	TRAINING.....	36
8.7.	CYOC ROLE IN TACTICS DEVELOPMENT AND EVALUATION	36
9.	FLIGHT PLAN FOR CYBER OPERATIONS	36
10.	UNDERSTANDING THE CYBER RELATIONSHIPS	39
10.1.	CURRENT COMMAND RELATIONSHIPS	39
10.2.	PROPOSED COMMAND RELATIONSHIPS	40
10.2.1.	<i>Network Defense Relationships</i>	41
10.2.2.	<i>Network Attack Relationships</i>	42
10.2.3.	<i>Network Exploitation Relationships</i>	43
10.3.	RELATIONSHIP WITH AIR FORCE COMPONENT COMMANDS	43
10.5.	RELATIONSHIP OF THE COMMANDER, AFNETOPS WITH AIR FORCE UNITS	43
11.	CONCLUSION.....	44
12.	ACRONYM LIST	45

List of Figures

Figure 1, CyOC Construct	4
Figure 2, Network Operations.....	16
Figure 3, Immediate Defensive Actions	16
Figure 4, AOC and CyOC Comparison	17
Figure 5, Strategy Division.....	18
Figure 6, Combat Plans Division.....	20
Figure 7, Combat Ops Division	21
Figure 8, ISR Division	23
Figure 9, CCO and ITO Battle Rhythm.....	25
Figure 10, CCO vs. MTO	26
Figure 11, MTO Process.....	27
Figure 12, CyOC Systems	35
Figure 13, Milestones and Timelines.....	38
Figure 14, Current Command Relationships	40
Figure 15, Proposed Command Relationships.....	41

1. Introduction

"We can't do our jobs without control of cyberspace. Warfighters operating in any domain rely on cyberspace to command and control forces in the 21st century. It's also essential to Joint operations and our national security. We must still integrate capabilities, systems and warriors to establish cross-domain dominance--securing freedom from attack and freedom to attack. All Combatant Commands, Military Departments and other Defense Components need the ability to operate unhindered in the cyberspace domain; therefore, the Air Force needs to continue pressing forward with cyber as a domain with equal importance to Air and Space."

*-Maj. Gen. William T. Lord, Commander, Air Force Cyberspace Command
(Provisional)*

The cyberspace domain is a critical component of 21st century warfare and a crucial element in protecting our nation's security. The DoD defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers." It encompasses the entire range of capabilities¹ that operate within or enable access to cyberspace. Cyberspace contains communications networks, data management systems, software, hardware, facilities, ranges, tools, weapons and sensors. Whether disrupting enemy operations or defending against cyberspace attacks, activities in cyberspace provide the Air Force (AF) with the ability to defend and attack in conjunction with, or independently from, traditional kinetic methods. The Air Force will ensure it is able to protect Air Force networks, mitigate or eliminate network vulnerabilities and enable the integration of kinetic and non-kinetic capabilities.

Controlling cyberspace is a prerequisite to effective strategic, operational and tactical operations within and across the cyber domain. To meet the unique challenges encountered within the cyber domain, in September 2008, Air Force senior leadership decided to consolidate Air Force cyber capabilities in 24 AF and subordinate it to Air Force Space Command.

The purpose of this document is to describe how 24 AF, in its Component Numbered Air Force (C-NAF) role, will establish, operate, maintain, defend, exploit, and attack networks. Twenty-Fourth Air Force is the cyber warfighter responsible for conduct of Air Force cyber combat operations at the operational level of war. This operational concept will describe how 24 AF will fulfill its warfighter responsibilities and how it will command and control cyber. It must be acknowledged up front that 24 AF will not be able to employ many of the concepts and capabilities described in this operational concept when it is initially activated. Command relationships, especially with respect to

¹ The term capability encompasses doctrine, organization, training, materiel, leadership and education, personnel, and facility (DOTMLPF) constructs required to *fly, fight, and win* in air, space, and cyberspace.

Network Attack (Net-A) and Network Exploitation (Net-E), must be examined and modified. In addition, many of the capabilities necessary to enable elements of mission assurance and Network Defense (Net-D) are not fully fielded. Finally, the intelligence support for specific elements of cyber needs to evolve to support activities at the operational level of war. This concept will lay out a flight plan for cyber starting with current capabilities and responsibilities of Air Force cyber units to the initial priorities of 24 AF as it stands up as an operational NAF and finally to its vision for its full potential as the Air Force component for cyber.

2. Executive Summary

The Air Force has been involved in cyber operations, under different names and in various forms, for more than a decade. The Air Force was the first government organization to field a network intrusion detection device to help defend its networks at the enterprise level. It also pioneered the operationalizing of computer network defense when it conducted the DoD's first Net-D tactics development exercise, BLACK DEMON. It was also a leader in the development and operationalizing of many offensive cyber capabilities. However, most of these actions were focused at the tactical level of war and there was no entity within the Air Force with the sole mission and authority orchestrate a comprehensive approach to cyber. Air Combat Command, in its role as the Air Force lead for information operations, helped to continue to move the Air Force forward, but the Air Force still lacked an organization singularly focused on cyber at the operational level of war.

With the signature of Secretary of the Air Force Michael B. Donley on Program Action Directive 07-08, Change 3, the Air Force formalized a structure for the conduct of cyber at the operational level of war. This was an historic step, organizing the major components of network warfare under an operational warfighter focused solely on cyber. Air Force network operations (network defense, network exploitation, and network attack), will now be orchestrated under a C-NAF (24 AF) that is exclusively focused on cyber operations. In addition, Air Force Space Command, as the parent MAJCOM for 24 AF, will provide MAJCOM level advocacy for cyber.

Twenty-Fourth Air Force will be responsible for the conduct of cyber operations. Cyber operations are defined as "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid" (Joint Publication 1-02). Twenty-Fourth Air Force will establish, operate, maintain, defend our networks and exploit and attack threat networks. Although 24 AF will initially focus on computer network operations, this does not define the limit of their mission set. All networks must be defended, including telephone networks, data links, and other military networks. Twenty-Fourth Air Force must also be able to conduct offensive cyber operations against militarily relevant cyber targets. In order to meet this responsibility, 24 AF has developed a set of process to enable it to plan, execute, command and control, and assess full spectrum cyber operations.

As its first priority, 24 AF will concentrate on conducting defensive network operations at the operational level of war. Today, there are multiple organizations doing network operations and conducting network defense actions. The Air Force Network Operations Center (AFNOC) is responsible to Joint Task Force – Global Network Operations (JTF-GNO), as the Air Force’s network defense organization. It responds to JTF-GNO taskings to help secure the Air Force Global Information Grid (AF GIG). In addition, it works with JTF-GNO in responding to network intrusions and incidents through its operational control of the Air Force Computer Emergency Response Team (AFCERT).

While this organizational structure was an improvement over previous ones, it did not provide for network defense at the operational level. Network defense continued to be conducted by tactical units without the overall strategy necessary to synchronize and focus Net-D activities in a proactive fashion against a committed threat. To remedy this, 24 AF will elevate Net-D planning and command and control to the operational level of war under the command of the 24 AF Commander in his role as the Commander, AFNetOps. Twenty-Fourth Air Force will build an operational plan for the defense of the AF GIG that will integrate “operational art” with technical capabilities. It will also increase the focus on understanding the threat and its intentions, not just an understanding of what has happened in the past. This will require an increased emphasis on intelligence support to Net-D. To accomplish this, 24 AF will leverage its internal intelligence capabilities and work with the Air Force Intelligence, Surveillance, and Reconnaissance Agency (AFISRA). It will also work, in conjunction with AFISRA, with national intelligence agencies to maximize its understanding of the threat.

The AFNetOps Commander will also be responsible for ensuring the AF GIG, as an extension of Air Force weapons systems, is prepared to support global air, space and cyberspace operations. This will be accomplished as 24 AF develops the capability to provide mission assurance for Air Force component commands’ air, space, and cyber operations. The AFNetOps Commander will use the situational awareness and mission assurance capabilities of the CyOC to ensure that global network components essential for mission success are defended, survivable and available to support global air, space and cyberspace operations.

Twenty-Fourth Air Force will also leverage its network exploitation capabilities to support both offensive and defensive operations. Utilizing established authorities and working closely within existing intelligence structures, 24 AF will work with our national partners to provide timely intelligence to support its cyber mission.

Finally, 24 AF will give the Air Force an operational level entity to plan and command and control offensive cyber actions. Today, Net-A is conducted under the auspices of Combatant Commands. The Air Force trains and equips cyber forces to present to these commanders for employment. This will continue in the future. However, in its role as the Air Force Component Command to JFCC-NW or the future joint cyber command, if it is established, 24 AF will be able to maximize the potential of Air Force capabilities by synchronizing all Air Force cyber capabilities and directing them within the context of an overall Combatant Commander (CCDR) plan. Later, this document proposes a strategy for integrating 24 AF into JFCC-NW’s offensive scheme.

The 24 AF Commander cannot command his cyber forces unless he can control them. Today, there is no command and control (C2) organization to enable the C2 of cyber capabilities at the operational level. To remedy this shortfall, 24 AF will stand up an operations center. Based on the proven processes and procedures used by Air Force component command Air Operations Centers (AOC), this cyber operations center (CyOC), will enable the 24 AF Commander to command and control his forces in support of network operations. It will be a small, distributed control center rather than the traditional AOC. So, while not an AOC, the CyOC will effectively integrate Air Force cyber capabilities to produce effects in support of global Air Force and joint mission requirements. The CyOC will develop and direct processes to plan, coordinate, allocate, task, and assess cyberspace operations based on joint and 24 AF Commander guidance. In its role as the C-NAF to JFCC-NW or the cyber unified or sub-unified command (or whatever CCDR construct selected by the SECDEF), the CyOC will serve as the Air Force C2 organization for assigned cyber capabilities. In addition, like a traditional AOC, the CyOC will serve as the focal point for planning cyber operations at the operational level. This is especially important when we look to operationalize network defense.

The CyOC will employ a distributed CyOC concept referred to as the virtual CyOC. Specific cyberspace weapons systems expertise will be leveraged in the CyOC through the virtual CyOC construct. Unique, highly-qualified Airmen with cyberspace skills reside in the 67 Network Warfare Wing (67 NWW), the 688 Information Operations Wing (688 IOW), the 689 Combat Communications Wing (689 CCW), the National Air and Space Intelligence Center (NASIC), and other intelligence and operational organizations. Many of the personnel within these units are high-demand, low-density assets. They have unique cyberspace experience and expertise and cannot be physically reassigned to the CyOC without impacting the operational capability of those units.

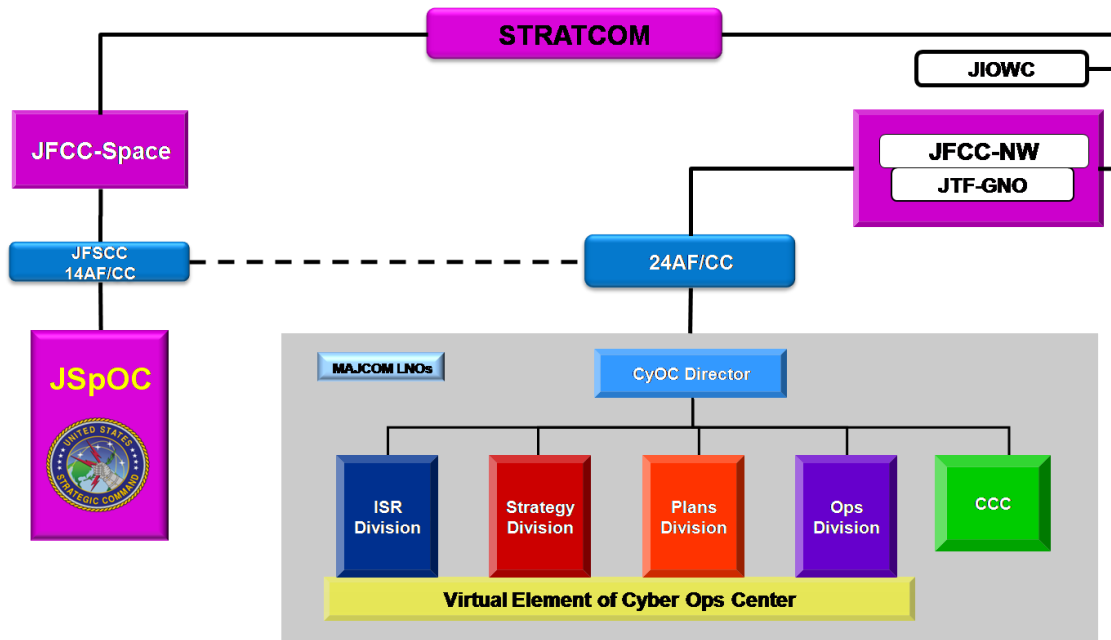


Figure 1, CyOC Construct

Therefore, they will be virtually integrated into CyOC processes from their home stations. Personnel with necessary planning and assessment skills will be included in CyOC strategic planning, combat plans and assessment functions. This will serve two purposes. First, it will ensure that the plans and response options developed in the CyOC will be executable by 24 AF subordinate units. The virtual CyOC construct will insure the 24 AF units to be tasked will have an input into the plans and courses of action (COA) being developed. Second, the virtual AOC construct will avail the CyOC of the unique expertise within 24 AF and other cyber units. This is essential to ensuring the viability of the cyber plans and COAs developed by the CyOC.

The CyOC requires a cyber common operating picture to provide the necessary situational awareness to accomplish its mission. The proposed CCS will provide cyber situational awareness to enable the CyOC to effectively C2 cyber forces / capabilities. However, it may be several years before the CCS realizes its full potential. In the interim, 24 AF will leverage existing systems in the CyOC to provide a nascent cyberspace situational awareness and C2 capability. This will include select AOC systems in addition to other more cyber related systems.

The CyOC will contain four divisions; strategy, plans, operations and intelligence, surveillance and reconnaissance (ISR), as well as a new entity, the Cyber Coordination Cell (CCC). These divisions are similar in structure and function to those of a traditional AOC, but are focused on cyber operations, not air operations. The CCC is a small cell that works to categorize and prioritize the vast amounts of information received by the CyOC. It is responsible for routing operational and maintenance tasks to the appropriate divisions within the CyOC and other AFNetOps units. In addition, it consolidates reporting data from 24 AF units for presentation to JTF-GNO. The following is the proposed mission statement of the CyOC:

“Plan, direct, coordinate, assess, and command & control cyber operations and capabilities in support of Air Force and Joint requirements.”

Successfully integrating the full range of offensive and defensive cyber operations in the CyOC is extremely challenging. Cultural, technological, political and educational barriers must all be overcome to achieve success. This document provides the foundation and initial considerations for enabling cyberspace activities within the CyOC construct. It proposes an organizational structure for the CyOC, identifies its core and enabling capabilities and describes the necessary organizational relationships and reporting structures to effectively integrate cyber planning, execution and assessment within the CyOC. Ultimately, through continued engagement and integration efforts, the CyOC will be able to effectively assist with production of global effects in cooperation with and for the CCDRs and the Air Force.

3. Legal Authorities of the AFNetOps Commander

Determining the legal authorities of the AFNetOps Commander is complex and requires a determination of the mission area and the respective role of the AFNetOps Commander

and his representatives. Once the mission area is determined, international law, domestic law and policy decisions establish the legal framework within which operational activities are evaluated. The primary focus of the AFNetOps Commander will be on defensive measures taken to protect the AF GIG from attacks, and defensive activities taken to respond to an attack in progress, enabling the Air Force to fight through network attacks. Since exceeding the legal boundaries of the designated mission area could have legal, diplomatic or political consequences, the AFNetOps Commander and his representatives should take care to remain within the legal boundaries established by that mission area.

3.1. Network Defense

Network defense actions are comprised of four distinct mission areas. These mission areas are: Service Provider, Law Enforcement, Intelligence and Warfighter. These mission areas are defined by the “purpose” or “intent” behind a particular response or action as well as the role an organization plays in providing network defensive capabilities. The AFNetOps Commander is capable of working within all four mission areas, but will typically operate within the Service Provider and Warfighter mission areas.

3.1.1. Service Provider

The Service Provider mission area generally encompasses any entity that provides an “electronic communications service” or “remote computing service.” As part of providing these services, service providers have a responsibility to protect their networks and systems to ensure they remain available to users. This responsibility ultimately falls to the AFNetOps Commander and his representatives. Representatives of the AFNetOps Commander are defined as personnel who are in positions specifically designated to perform service provider duties, and includes personnel in AFNetOps organizations, base Network Control Center personnel, system administrators, and client support administrators. The AFNetOps Commander and his representatives are subject to search and seizure laws and statutory limitations when acting on the behalf of Law Enforcement personnel or agencies. However, potentially incriminating information discovered as a result of routine service provider duties or activities inherent to those typical of a service provider can be provided to law enforcement agencies pursuant to the Service Provider Exception to the Electronic Communications Privacy Act. When potentially incriminating information is found, personnel acting in a service provider role can continue to take appropriate measures to protect the network and ensure efficient operation, as long as their actions are not at the request of law enforcement personnel. Whenever questions arise as to whether network personnel actions are in support of law enforcement or counterintelligence investigations, network personnel should consult with their Staff Judge Advocate for guidance on how to proceed.

3.1.2. Warfighter

The Warfighter mission area is divided into three distinct categories; Net-A/Net-D), and Net-E). The AFNetOps Commander will likely be focused on Net-D activities, or “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.” In this mission area, the AFNetOps Commander is responsible for the preservation of a capability, and has the right of self defense. Care should be taken, though, to ensure actions taken in self defense do not enter into the NetA or NetE mission area and are within the SROE guidelines.

3.1.3. Law Enforcement

It is likely the AFNetOps Commander will be asked by law enforcement personnel to participate in investigations involving illegal activity on information systems. In accordance with the Title 18 of United States Code, the AFNetOps Commander may share network information obtained while performing system administrator duties with Law Enforcement personnel and can assist investigators in collecting and preserving evidence when done in accordance with Title 18 and Constitutional requirements. Law Enforcement personnel are allowed to conduct investigations and monitoring of personnel under the Computer Trespasser Exception to the Federal Wiretap Act with the consent of the AFNetOps Commander or his delegate. The AFNetOps Commander and those serving under him must be careful to remain within the boundaries of the law and should consult with his Staff Judge Advocate.

3.1.4. Intelligence

In this mission area, the AFNetOps Commander assists with the collection of information related to a person’s or group’s activities on the AF GIG. Intelligence collection agencies are subject to strict congressional oversight and limited by the Foreign Intelligence Surveillance Act, Executive Order 12333, DoD Directive 5240.1, DoD Regulation 5240.1-R, and AFI 14-104. This is an especially sensitive area of law and policy and network personnel should consult with their Staff Judge Advocate.

3.2. Designated Approval Authority (DAA)

3.2.1. Network Defense

The AFSPC Commander has the responsibility for serving as the DAA for all Air Force information systems, other than those under the purview of the SAP/SAR DAA. The AFNetOps Commander advises the AFSPC Commander on the operational consequences of certifying various systems for operation on the AF GIG. The DAA is responsible for ensuring all information systems that reside on or connect to the AF GIG meet standards defined in AFI 33-115, Volume 1, Network Operations, and AFI 33-202, Volume 1, Network and Computer Security through Change 4, and to recommend their removal when they do not. In addition, the AFNetOps Commander assists the AFSPC Commander in balancing the technical, operational, and managerial Information Assurance controls to protect the AF GIG and to support AF operational missions that rely on the AF GIG. This authority is extremely broad and is the primary source of authority for most decisions.

3.2.2. Intelligence Requests

The AFSPC Commander, as the DAA for the AF GIG, has the additional responsibility for serving as the single point of contact for information assurance, (IA) related intelligence requests from Air Force and DoD intelligence agencies. The 24 AF/A2, working with the ISR Division of the CyOC, will develop Priority Intelligence Requirements (PIR) for the AFSPC Commander.

4. Implementation Considerations

4.1. Timeframe

In October 2008, CORONA directed the consolidation of Air Force cyber operations in a warfighting NAF, 24 AF. This NAF will be subordinate to Air Force Space Command.

In anticipation of the 24 AF activation, the AFCYBER (P) Commander directed development of this operational concept for cyber operations at the operational level of war. The operational concept includes a section describing an organization to enable cyber C2. The CyOC will serve as the C2 node for cyber operations conducted by 24 AF. It is anticipated the CyOC IOC date will be linked to the 24 AF activation date. However, recent intrusion incidents on Air Force and DoD networks highlight the need to elevate the defense of the AF GIG to the operational level of war. Therefore, the CyOC may start performing aspects of its defensive mission using personnel from the Air Force Network Operations Center (AFNOC) personnel while operating from the 608th AOC facility at Barksdale AFB sometime in 2009. The remainder of the concept will be implemented before 24 AF reaches Full Operational Capability (FOC).

4.2. Assumptions

Several assumptions guided the development of the cyber operational concept. They include:

- The current command relationships, including force apportionment, and allocation, between 24 AF units and joint commands will continue as is until changed and approved. This is expected to be associated with the activation of the new joint cyber command.
- The 24 AF Commander will be the component commander to the joint cyber command when that command is activated.
- The AFNetOps Commander will exercise his existing authorities to defend the AF GIG. In addition, the AFNetOps Commander will also implement Joint Task Force – Global Network Operations (JTF-GNO) guidance.
- The Deputy Chief of Staff (DCS) for Intelligence, Surveillance and Reconnaissance (ISR) (AF/A2) will retain responsibility for providing overarching policy, guidance and oversight for full-spectrum, multi-source intelligence planning, programming,

budgeting and execution of the Air Force portion of the National Intelligence Program (NIP).²

- The CyOC will have visibility (real time constant awareness) of the entire AF GIG prior to reaching full operational capability (FOC).
- As the lead command for AFNetOps, AFSPC will direct and accomplish an authoritative and structured network inventory before CyOC FOC.
- The CyOC will stand up with existing AFNOC assets and personnel. Future CyOC personnel will have completed all designated training.
- Where needed, the CyOC will leverage existing baseline AOC systems to the maximum extent possible and will add specific required systems to support cyber planning and execution.
- The CyOC will not have the desired personnel and experience levels in the AFNOC at IOC. Personnel and billets from other 24 AF units will not be reassigned to increase CyOC manning. Subject matter experts (SMEs) may support the CyOC via virtual means as required from many other units.
- Training will be developed in parallel with the evolving cyberspace C2 tactics, techniques and procedures (TTP).
- The CyOC will support Air Force component commands to produce effects within the CCDR's area of responsibility (AOR) in accordance with established command relationships. Twenty-Fourth Air Force will be responsible for ensuring the requisite portions of the AF GIG are available and prepared to support theater operations.
- The 24 AF will have responsibility, as the Air Force component to the joint cyber command, for planning and apportionment of global offensive and defensive cyberspace operations.

In addition to the assumptions used in the development of this concept, the following facts are foundational to the concept:

- The AFNetOps Commander will have command authority over the entire AF GIG.
- The 24 AF Commander will also serve as AFNetOps Commander.
- Net-D will be the priority mission for 24 AF.

² Program Action Directive 07-08, Change 3, pg 7.

4.3. Risks

There are numerous risks involved in operationalizing the cyber mission under 24 AF. The following are the most significant risks associated with the conduct and C2 of 24 AF cyber operations:

- There is a lack of adequate manning for the CyOC and the 24 AF staff. While the Program Action Directive (PAD) codifies the billet structure for the CyOC and the AFFOR staff, this does not guarantee the requisite experienced personnel are available to fill these billets. AFSPC/A1, 24 AF/A1, and the Air Force Personnel Center will have to endeavor to put the most highly qualified cyber trained personnel in each billet.
- A lack of available training presents a risk to the accomplishment of the 24 AF mission. While many current unit training programs do an excellent job of preparing their personnel for the unit's specific cyber role, they do not address the skills necessary for the conduct of cyber operations from the operational level of war. These training programs can be leveraged to help meet near term training needs.
- Twenty-Fourth Air Force will not have the situational awareness or C2 systems necessary to accomplish all aspects of its mission at IOC. While there are several cyber related systems being used or developed by various organizations, there is no single system or set of systems that provide the 24 AF Commander adequate AF GIG situational awareness. Multiple systems will need to be utilized to provide the best possible situational awareness while the Cyber Control System (CCS) is developed and fielded.
- The Air Force has made great strides communicating a common understanding of cyber and cyber operations. However, there is still considerable variance concerning the nature of cyber and what mission areas are included as part of cyber. This will significantly affect how cyber operations are planned and executed. Twenty-Fourth Air Force must take the lead in building an Air Force-wide consensus on what constitutes cyber operations.

5. Challenges to Cyber Operations for 24 AF

“The threats to our information are real—they are multi-faceted, sophisticated and increasing daily. Today we have a “Defense-in-Depth” approach to assuring information—based largely upon firewalls and software patches—attempts to keep intruders out and data safe. Tomorrow, a “Defense-in-Breadth” approach is required to assure that our information capabilities and information critical components are trusted throughout their lifespan to achieve Decision/Mission Superiority.”³

³ John G. Grimes, The Department of Defense Interim Information Assurance Strategic Plan, March 2008

The United States Air Force has, more than any other air force, mastered the ability to apply global power, global reach and global vigilance across the domains of air and space. Due to the initiative to establish an Air Force cyber capability, the Air Force is now taking concrete steps to apply global power, reach, and vigilance in the cyberspace domain as part of its mission to *fly, fight, and win* in air, space and cyberspace.

Achieving its mission alongside its joint partners and within the constraints of the standing national and military objectives, the Air Force has identified the following cyberspace requirements:

- Establish/maintain AF cyber components
- Operate/defend AF cyber components
- Exploit enemy vulnerabilities
- Attack enemy networks, systems, peripherals and infrastructure.⁴

To accomplish these objectives and realize the full potential of cyberspace operations, 24 AF should prepare to perform the following tasks:

- Control and configure the AF GIG to support Air Force operations in cyberspace. In addition, 24 AF must be able to ensure the availability of the network as a part of weapon system(s), and be ready to support air, space and cyberspace operations. Also, it must maintain network situational awareness to support all facets of cyberspace operations.
- Develop and publish a strategy for the defense of the AF GIG. The strategy division will prepare defensive strategies for the AFNetOps Commander approval; develop plans to implement the network defensive strategy and direct defensive activities in support of these plans.
- In close coordination with Joint Force Component Command – Network Warfare (JFCC-NW) or the proposed joint cyber command, identify Air Force priorities for Net-A target sets. Twenty-Fourth Air Force should maintain the cyber target folders, lead the development of the capabilities to prosecute these targets, develop the TTPs for employment and exercise these capabilities in the joint environment.
- Twenty-Fourth Air Force strives to serve as the cyber component command to the future joint cyber command structure. Twenty-Fourth Air Force will be able to plan, coordinate, and support regional and trans-regional operations in its supporting role under established command relationships. It must be able to integrate multiple capabilities resident with 24 AF cyber units. This requires the CyOC to be able to

⁴ Program Action Directive 07-08, Change 3, page 5.

select the appropriate capability, or combination of capabilities, to produce the desired effect.

- Support time sensitive planning (TSP) for cyberspace operations. As the CyOC systems, capabilities and processes mature, the timeframe for TSP must be reduced to a matter of minutes.
- Participate in Air Force and joint exercises, to include those focusing primarily on cyberspace operations and also those that integrate air, space and cyberspace. This will help mature and socialize the art of cyberspace warfare. This includes participation in tactics development exercises and operational test and evaluation of cyberspace capabilities.
- Extend visibility and control of the terrestrial segment of airborne and space networks to ensure their availability to support operations. In addition, the CyOC should be prepared to support self-forming airborne networks and space networks in the future as threat and defensive systems mature.

Twenty-Fourth Air Force should develop the operational capability to integrate, synchronize and execute cyberspace operations across the full spectrum of conflict. It should foster strong ties with sister service organizations, government agencies, industry and academic institutions to share intelligence, a common strategy, technology and intellectual capital. Finally, it should work to include the CyOC as part of the globally-linked AOC weapon system. This will be necessary to enable the CyOC to orchestrate simultaneous regional and trans-regional cyberspace effects and to defend the AF GIG.

Security constraints may provide additional complications. Often cyberspace activities occur in Special Access Programs (SAP) requiring compartmentalized clearances. However, cyberspace warfighting capabilities must be understood, at some level, by all CyOC personnel. Adherence to SAP access controls may present challenges when attempting to effectively integrate capabilities. Additionally, the authority to employ SAP cyberspace capabilities is often very restrictive requiring permission from the highest levels of the government or DoD.

The challenge of simultaneously employing cyberspace assets in multiple theaters requires theater AOCs be linked to support worldwide distributed operations because the cyberspace domain is not constrained by geographic boundaries. The goal of effective distributed operations is to directly support the operational commanders to achieve their objectives. A globally linked C2 architecture provides reach-back capability between regional commanders, cyberspace forces and intelligence agencies.

The rapid growth and extensive networking of information-based technology has created a growing national and military dependence on cyberspace. Militarily inferior adversaries have the potential to utilize cyberspace capabilities to strike the U.S. across a broad range of targets with speed, relative anonymity, and minimal cost. For U.S. forces, the organized, globally connected compilation of terrestrial, airborne, and space-based

capabilities operating within and through cyberspace are essential warfighting capabilities that must be developed, maintained, and protected.

6. Cyber Operations at the Operational Level of War

Twenty-Fourth Air Force's mission requires the seamless integration of cyberspace capabilities to provide the joint warfighter with a robust set of options to produce desired effects in their area of responsibility. This requires the availability of the AF GIG to support all Air Force operations. The 24 AF Commander must defend all the components of the AF GIG to accomplish this requirement. This includes computer networks, telephone networks, wireless communications and data links. Twenty-Fourth Air Force must also support offensive cyber operations. Unlike traditional weapons platforms, cyberspace capabilities can be tasked within a short period of time to support multiple CCDRs on demand. For example, a network attack capability can be used to generate effects in one COCOM, and then be re-tasked to service targets on the other side of the globe – all within a very short period of time.

Twenty-Fourth Air Force should provide the Air Force with the capability to plan, apportion resources, command and control cyber operations and assess full spectrum cyber operations at the operational level of war. Several 24 AF offensive units conduct their missions under abnormal command relationships. The goal is to be able to eventually command and control the capabilities resident with 24 AF units when requested in support of the joint force commander.. To accomplish that goal, 24 AF, the CyOC and subordinate units must present a compelling reason for the SECDEF and the Joint Chief's to approve realigning command structures by demonstrating the value added that 24 AF brings to the cyber fight. The included concepts will enable 24 AF to fulfill mission requirements and provide an extensive range of integrated capabilities, enabling the Air Force to provide a broad range of options to our service and national senior leadership.

6.1. Conducting Cyber Operations

Twenty-Fourth Air Force must approach cyber warfare in the same way other operational warfighters approach combat within their domain. The 24 AF Commander builds operational level plans in support of the joint warfighter. This includes the requirement to build and update a plan for the defense of Air Force portion of the DoD GIG. Since there is currently no joint strategic plan for the defense of the DoD GIG, an independent plan must be developed by the 24 AF Commander to fulfill his responsibilities as Commander, AFNetOps. This Net-D operations plan will serve as the foundation for operational planning in the CyOC. In addition to planning cyber operations, the 24AF Commander must be able to command his forces to enable him to execute his plans. Twenty-Fourth Air Force will be required to operate globally, 24 hours a day, 365 days a year in perpetuity. It must be able to employ offensive cyber capabilities in support of the joint warfighter anywhere and anytime. It must engage globally in defense of the AF GIG to ensure its availability to support the Air Force mission. To accomplish this, existing planning and C2 models require modification to fit the mission of 24 AF. The following paragraphs will discuss the concept for conducting cyber operations in 24 AF.

6.2. Operational Defense of the AF GIG

With the activation of 24 AF, the AFNOC will morph into the CyOC and the Air Force will transition from a systems based approach to network defense to an operational approach to network defense. Today, Net-D is primarily based on a set of sensors that block known malicious code or alarm once a malicious activity has been detected. This approach is reactive and will never achieve Air Force Net-D goals. With the activation of 24 AF, “operational art” and technology will be integrated to enable a more threat based approach to network defense.

The 24 AF Commander will develop an operational plan for the defense of the AF GIG that will be threat based. It will be developed using the normal planning process and will identify such items as commander’s intent, defensive priorities, assigned assets, threat assessments, and his operational scheme for defense of the AF GIG. It will drive future operational level plans and daily plans for the defense of the AF GIG. Working with the CyOC and AFFOR staff, the Commander will develop guidance to apportion and allocate scarce defensive resources in anticipation of threat activities based on a robust threat assessment and operational priorities. In addition, assets like those in the 92 IOS which are used today to investigate an incident once it has been detected could instead be deployed proactively to ensure high priority defensive assets are secured.

If an incident is detected, the 24 AF Commander will “fight through” the attack. The Combat Operations division of the CyOC will quickly coordinate possible courses of action with 24 AF Net-D units through the virtual CyOC construct. The goal is to give the Commander options beyond simply taking the affected unit off-line. Options could include deploying a response team isolate the threat and focusing the efforts of existing Net-D units on the target under attack. Future options could also include deceptive measures and more active responses.

6.3. Mission Assurance

Mission assurance will be one of the most important functions of 24 AF. It will be the responsibility of the 24 AF Commander to ensure that the AF GIG is available to support global Air Force Operations (air, space, and cyber). He must ensure that the network, as an extension of the weapon system, is ready to support Air Force Component Commanders and the MAJCOMs. Today, the portions of the AF GIG necessary to support Air Force operations are likely not all within the component commanders area of responsibility (AOR). For example, part of the infrastructure necessary to support a Predator mission in the AFCENT AOR may be located within the CONUS.

As part of his operational plan for the defense of the AF GIG, the Commander must have situational awareness on all global Air Force operations and will take steps to ensure the defense and availability of the AF GIG to support those operations. This may include deploying assets preemptively to ensure specific portions of the AF GIG are protected and defended. In addition, the CyOC will coordinate AFNetOps actions to ensure that we do not inadvertently impact a part of the AF GIG that is currently supporting a critical mission half way around the world.

It must be acknowledged that the CyOC will not possess the network mapping tools necessary to map Air Force operations to the supporting architecture in a timely manner to support mission assurance. This capability must be developed and will be fully implemented by the time 24 AF reaches its full operational capability.

6.4. Command and Control of Cyber Operations

To enable command, a commander must be able to control the forces assigned to him. This is a particularly difficult task in the cyber domain. Existing command relationships for Net-A prohibit the operational commander from apportioning his forces. In addition, lines of command are muddled and unclear resulting in sub-optimized force application. In addition, squadron commanders often have multiple masters further confusing issues. Finally, confusion about lines of authority for the AFNOC to reach into an Air Force base and direct or remotely install a patch or take a defensive action are only recently becoming understood.

6.5. Command and Control of Network Defense

The 24 AF Commander, as the Commander, AFNetOps has the authority to reach into the global AF GIG to perform his network defense mission. In addition, the Commander is responsible for ensuring the AF GIG is available to support the Air Force's global mission. In performing network defense activities, the 24 AF Commander has operational control of the AF GIG and can reach down to the base network control center or communications squadron to direct or implement a defensive action. For normal network taskings (installing patches, etc.), actions will be directed by the CyOC through the 67 NWW to Air Force bases. The CyOC will inform the bases and MAJCOMs that are affected of any actions taken or directed via a routine message to the base command post. In addition, base communications squadrons will also be notified (Figure 2**Error! Reference source not found.**). The MAJCOM liaison officers located in the CyOC will help the CyOC coordinate any specific mission requirements that the affected base or MAJCOM might have.

When it is determined that part of the AF GIG is currently under attack, (Figure 3**Error! Reference source not found.**) the operations division of the CyOC will immediately consult with 24 AF Net-D units and JFT-GNO to help determine the severity of the event. If necessary, it will direct defensive measures to protect the entire AF GIG from compromise. If it is necessary to take an action at a specific Air Force base, the CyOC will notify the affected MAJCOM and wing commander via immediate message. If the action will impact a Component Command AOC, the Component Commander will also be notified via immediate message. Because of the criticality of ensuring defense of the AOC systems while simultaneously not adversely impacting theater operations, there will also be direct coordination between the CyOC and the affected AOC.

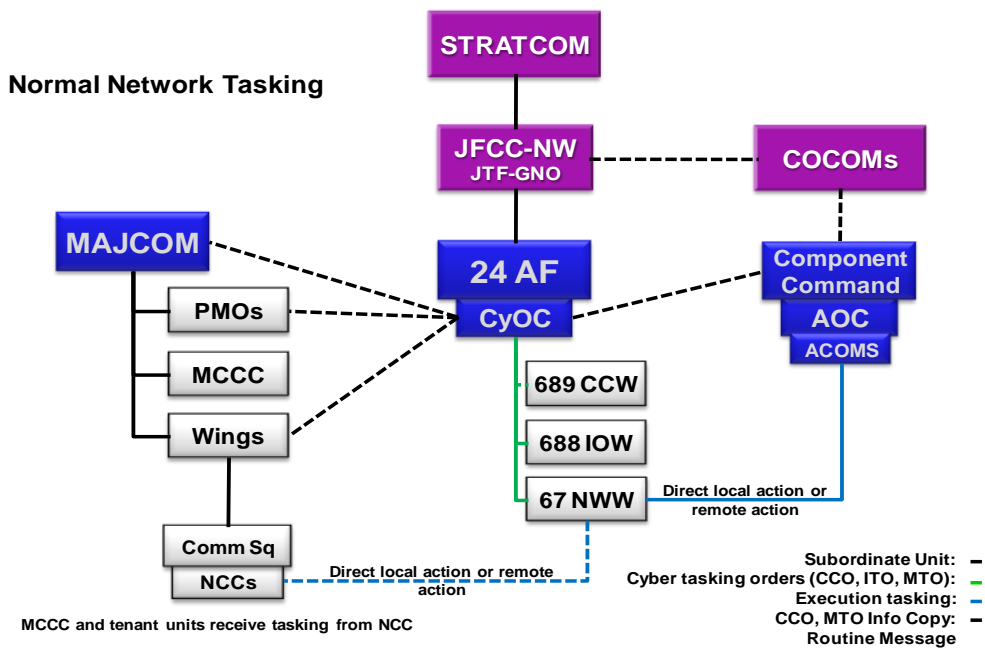


Figure 2, Network Operations

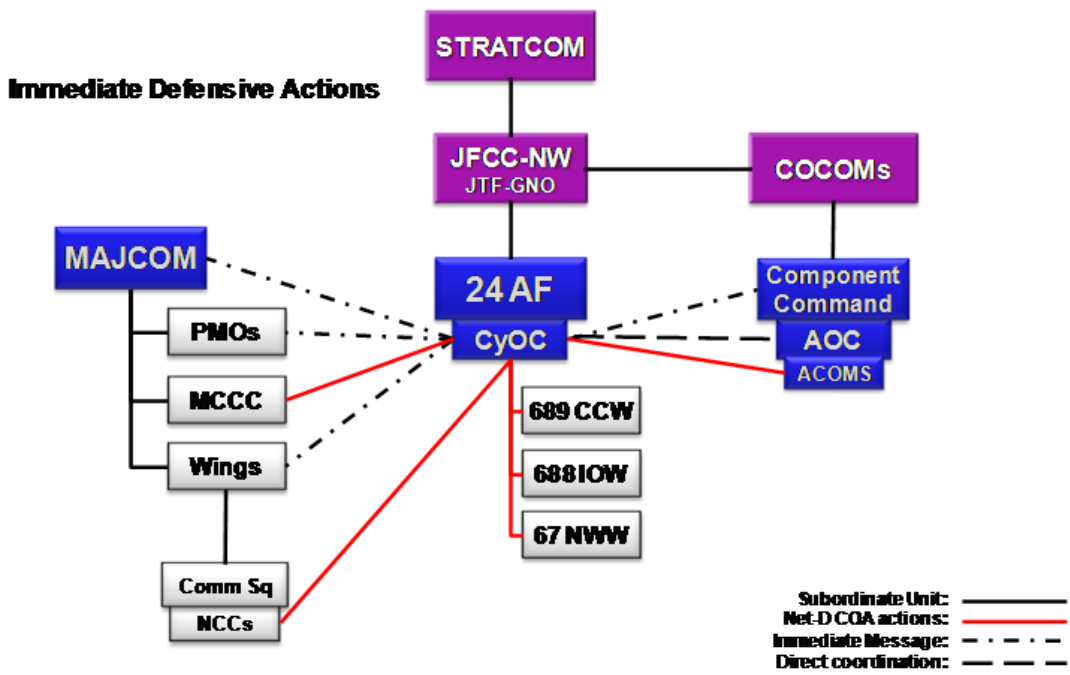


Figure 3, Immediate Defensive Actions

6.5.1. Cyberspace Operations in the CyOC

AOCs have included cyberspace operations/capabilities in their integrated tasking orders (ITO) for years. USCENTCOM made extensive use of cyberspace operations in both Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF). However, their focus was regional, and generally involved using a specific capability to produce a specific effect. Additionally, they did not defend cyberspace outside their own networks. The CyOC will have responsibility for global offensive and defensive operations as tasked by USSTRATCOM.

Figure 4, AOC and CyOC Comparison, compares the organizational structure and processes of a notional Component AOC, the AFNOC and the CyOC. The most significant variation in organizational structure for the CyOC is the addition of the Cyber Coordination Cell (CCC), discussed later in this document. The CyOC will also add AFNetOps planning and strategy guidance, similar to the guidance already produced by a Component AOC, to operationalize NetOps.

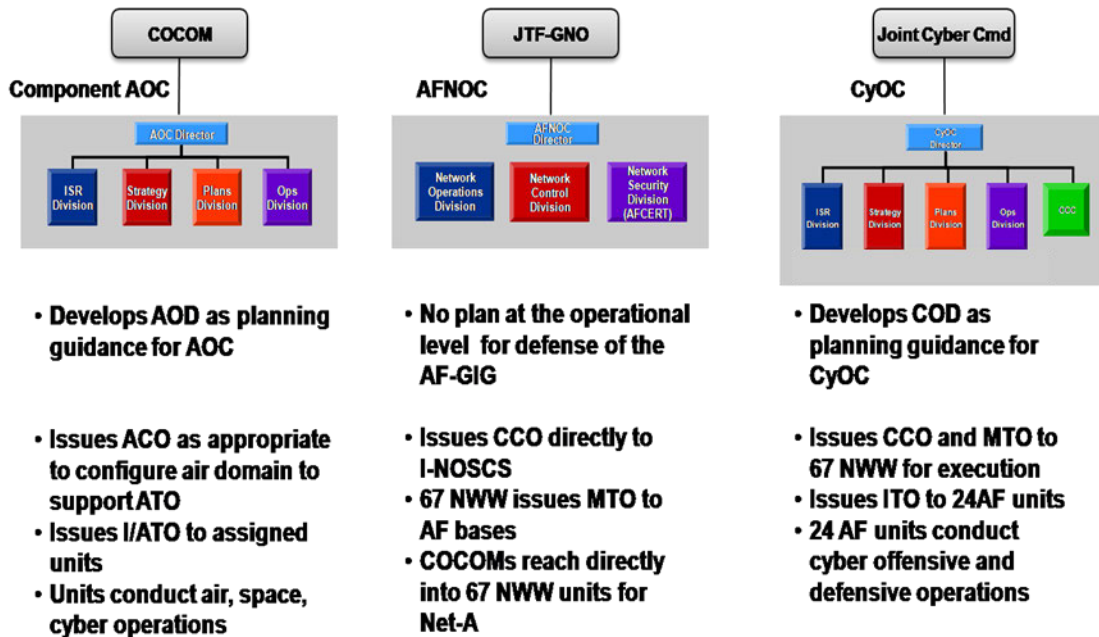


Figure 4, AOC and CyOC Comparison

6.5.2. Cyberspace Integration in the CyOC

Today, there is not a single Air Force organization responsible for Air Force defensive cyberspace strategy across the AF GIG. The CyOC is the C2 organization that will plan

and execute the Air Force's AF GIG defensive strategy. The AFNetOps Commander will provide the CyOC strategic guidance for protecting the AF GIG and the CyOC and AFFOR staffs will transform that guidance into a defensive plan, monitor execution of the plan and make adjustments as required in real-time. These actions will ensure the Air Force has freedom of maneuver in cyberspace.

The following paragraphs explain the CyOC divisions.

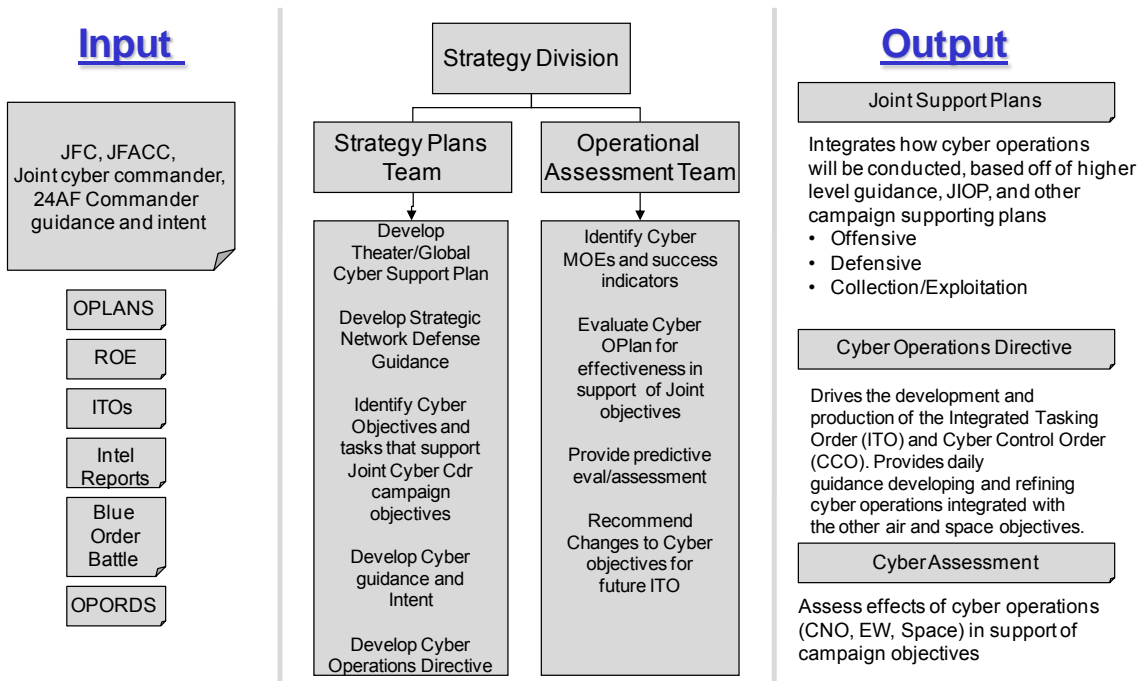


Figure 5, Strategy Division

6.5.2.1. Strategy Division

The strategy division supports the achievement of theater objectives by developing, refining, disseminating, and assessing the JFACC air and space strategy.⁵ As part of the CyOC Strategy Division, personnel focus on long-range planning of cyberspace operations, as well as participate in the development, refinement, dissemination, and assessment of the progress of the cyberspace strategy. Cyberspace activities will be integrated to produce an overall non-kinetic strategy in support of combat operations. Figure 5 describes the inputs, outputs, and tasks of the CyOC Strategy Division. Offensive and defensive operations in the form of network warfare operations will be integrated as needed into the overall strategy to achieve the desired battlespace effect.

⁵ Air Force Instruction 13-1 AOC, Volume 3, 1 August 2005, Operational Procedures – Air and Space Operations Center, page 14.

Based on guidance contained in the AF GIG defense plan, the strategy division will produce the Cyber Operations Directive (COD) to describe the overall strategy for integrating and assessing cyberspace operations and communicate this strategy to the plans, operations, and ISR divisions, as well as subordinate or tasked units to facilitate planning and preparations.

The major inputs to the strategy division include JTF-GNO plans, theater ITOs, rules of engagement, intelligence threat assessments, blue order of battle, and Air Force operational plans for the defense of the AF GIG. These inputs will be used by the division's teams: strategy guidance, strategy plans, operations assessment, information operations and special technical operations team to produce global integrated operations plans.

6.5.2.2. Combat Plans Division (CPD)

“The CPD applies operational art to develop detailed execution plans for air and space C/operations. Based on C/JFC objectives and apportionment, the AOD, forces made available for C/JFACC tasking, and the operational environment, these execution plans apply specific air, and space capabilities and assets to accomplish JFACC tasks in fulfillment of the C/JFC mission. The end result is publication and dissemination of the ATO and other planning/tasking documents.”⁶ As part of the CyOC combat plans division, personnel will participate in the development of detailed plans for the application of cyberspace resources based on the guidance stipulated by the CyOC Strategy Division. Figure 4 addresses combat plan's cyberspace activities during the planning process and its production of the ITO and CCO. The combat plans division considers and plans full spectrum operations, including Cyberspace operational courses of actions (COAs) for the next 24 – 48 hours (tomorrow's war). The combat plans division will coordinate activities with the CCC and virtual planning components to support development of an ITO, Cyber Control Order (CCO), and Special Instructions (SPINS). Computer Network Operations (CNO), both offensive and defensive operations are integrated to meet joint objectives.

⁶ Air Force Instruction 13-1 AOC, Volume 3, 1 August 2005, Operational Procedures – Air and Space Operations Center, page 23

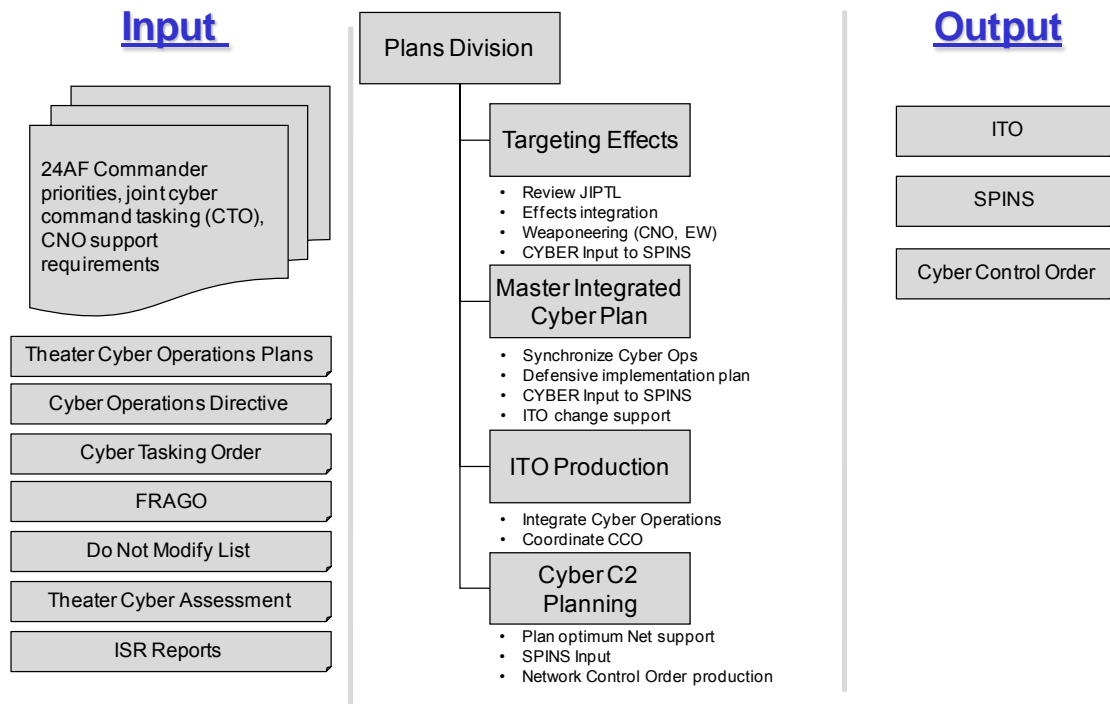


Figure 6, Combat Plans Division

The major inputs to the combat plans division include joint cyber operations plans, the COD from the Strategy Division, the CTO, and other inputs from JTF-GNO. These inputs are used by combat plans in four processes; targeting effects, a cyber focused Master Integrated Cyber Plan development, integrated tasking order development and NetOps C2 Planning.

The primary outputs of combat plans are the ITO, SPINS, and the CCO. The plans division will rely on reachback support from SMEs and units outside the CyOC: the 67 NWW, 688 IOW, 689 CCW and Space units providing the requisite cyberspace expertise in their respective platforms.

6.5.2.3. Combat Operations Division (COD)

“The Combat Operations Division (COD) is responsible for monitoring and adjusting execution of the current ATO. In doing so, the COD maintains situational awareness of the battlespace and constant contact with subordinate, TACS elements and assets, as well as other assets available for tasking. In general, the COD responds to battlefield dynamics by command and control of air and missile defense operations and information operations (IO), by modifying the published ATO through adding, deleting, retargeting,

or changing a sortie's mission („re-roling“).⁷ Personnel in the CyOC Combat Operations Division will participate in the monitoring, C2 and assessment of cyberspace operations directed by the ITO. They will also maintain situational awareness of the defensive posture of the AF GIG and adjust defensive activities as necessary in accordance with the defensive plans developed by the plans division. Combat operations division personnel will also assist in real-time prioritization, operational analysis and recommendations for ITO changes in reaction to battlespace situations for all defensive and offensive operations.

The operations division will maintain situational awareness of the status of operations from the other component command AOCs. This is necessary to ensure the network is supporting ongoing air, space and cyberspace operations world-wide. If part of the

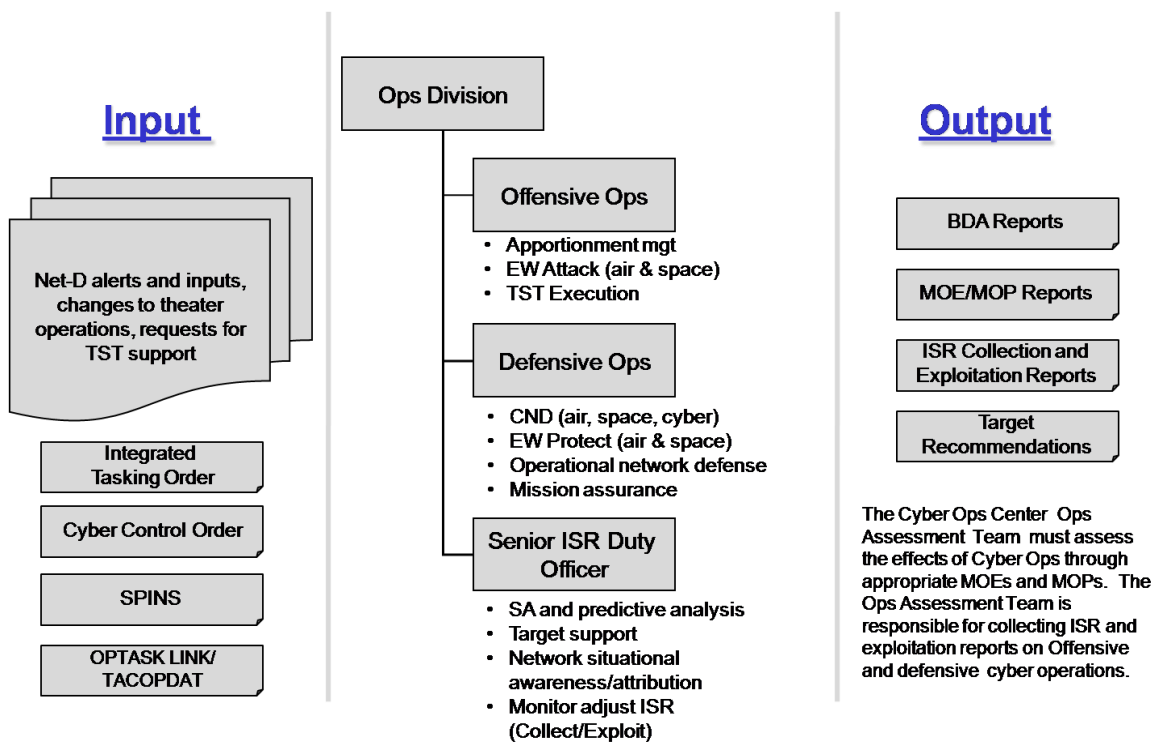


Figure 7, Combat Ops Division

AF GIG is under attack, or if an action taken by blue forces is impacting the functionality of the AF GIG, the combat operations division must direct actions necessary to ensure the availability of the AF GIG to support global operations. Figure 5 addresses the inputs, outputs, and tasks required for the combat operations division to perform its mission.

⁷ Air Force Instruction 13-1 AOC, Volume 3, 1 August 2005, Operational Procedures -Air and Space Operations Center, page 38, modified to include aspects of CyOC and cyber operations

The major inputs to the combat operations division include the Integrated Tasking Order, and integrated SPINS. These inputs are used by the division's three teams: Offensive Operations, Defensive Operations, and the Senior Intel Duty Officer to produce four primary outputs.

The primary outputs of the combat operations division are: Battle Damage Assessment (BDA) reports, Measures of Effectiveness (MOE)/Measures of Performance (MOP) reports, ISR Collection and Exploitation Reports and Target Recommendations.

6.5.2.4. ISR Division

“The ISRD provides the C/JFACC, AOC and subordinate units with predictive and actionable intelligence, ISR operations, and targeting in a manner that drives the Air Tasking Cycle. A common threat and targeting picture is critical to planning and executing theater-wide air and space operations to accomplish C/JFACC objectives. The ISRD also provides the means by which the effects of the air and space operations are measured.” The ISR Division develops knowledge of the operational environment. “This knowledge of the operational environment, in concert with C2, enables the C/JFACC to anticipate future battlespace conditions, establish priorities, exploit emerging opportunities, and act with a degree of speed and certainty not matched by our adversaries.”⁸

The CyOC ISR Division (ISRD) will provide intelligence and analytical support for the planning and C2 of all operations controlled by the CyOC. Their role will expand significantly to include support for the development of the commander's estimate for the defense of the AF GIG and cyberspace threat assessments. They will generate the CyOC's collection requirements that will be forwarded to Intel agencies for collection and analysis. Personnel in the ISR division will work with AF ISR Agency personnel, 24 AF units, and other agencies to produce the Intelligence Preparation of the Battlespace (IPB) plan in support of CyOC missions. They will also be responsible for Intel support for the defense of the AF GIG. This will require extensive threat analysis to include threat strategy and intent, capabilities, and the status of current cyberspace threats. This information must be shared with the other AOCs and units involved with defense of the AF GIG. ISRD personnel will also support mission assessment to determine if the MOEs are met. Figure 8 identifies the inputs, outputs and tasks for the ISRD supporting cyberspace operations.

⁸ Air Force Instruction 13-1 AOC, Volume 3, 1 August 2005, Operational Procedures – Air and Space Operations Center, page 66

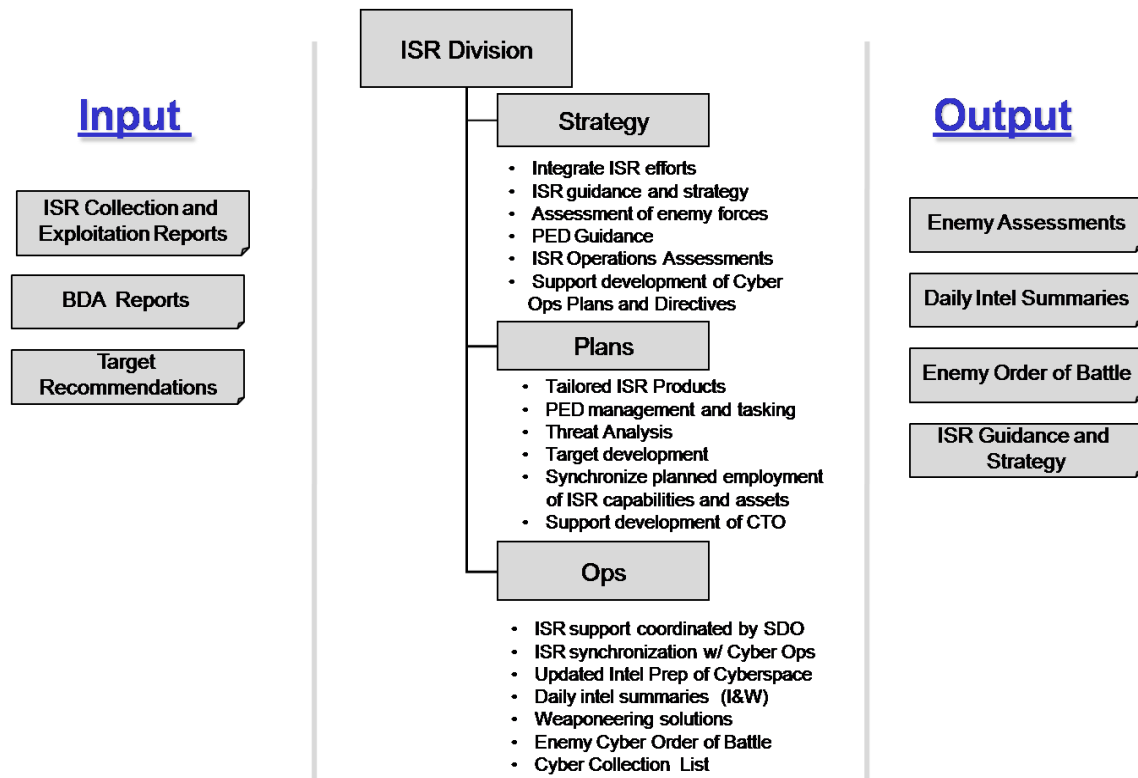


Figure 8, ISR Division

6.5.3. Cyber Coordination Cell

The CCC is the situational awareness hub for the CyOC and will be the single point of entry for corresponding with the CyOC. As such, the CCC will be responsible for filtering direction and guidance from JTF-GNO, requests for cyber capabilities, and correspondence regarding CCOs and MTOs. For example, the CCC will determine if a directed network action should be forwarded to the plans division for inclusion in the CCO, sent to the 24 AF staff for a policy decision, or included in the MTO and then forwarded to the 67 NWW for execution. The 67 NWW will track MTO compliance and provide compliance statistics to the CCC to maintain awareness of maintenance activities on the AF GIG (deconflicting any maintenance activities to enable combat operations).

6.6. Network Operations

To effectively C2 the AF GIG, it is essential for the CyOC to have processes to issue orders to subordinate and peer units. These include the CCO and the MTO. The following sections describe the contents of each of these three network control mechanisms.

6.6.1. Cyber Control Order

The CCO configures the cyberspace domain to support operations in much the same way the Airspace Control Order (ACO) configures the air domain to support air operations. It ensures the portion of the network required for conducting specific line items in the I/ATO are protected, defended, available, and survivable during the mission timeframe. It should also include additional actions to ensure back-up measures are in place to cover unforeseen contingencies, increasing the overall reliability of the network to support operations. The CCO includes time critical tasks, those that occur inside the battle rhythm of the I/ATO cycle. The CCO is synchronized with the ITO. Some cyberspace operations might execute prior to other effects to proactively ensure the network is available to support air, space and cyberspace operations. The CCO shifts resources, proactively modifies the net, and allows for flexible response actions. The CCO prepares the battlespace for full spectrum effects options, while the ITO directs cyber operations within the battlespace.

The CCO development process begins within the strategy division of the CyOC 72 hours from ITO execution. The combat plans division synthesizes cyberspace plans based on the strategy developed by the combat strategy division. Campaign planners coordinate the campaign plan and draft ITO tasks, and assess both the ability of the network to support the ITO tasks and the impacts of the ITO on the AF GIG.

The combat plans division will conduct three primary tasks in planning AFNetOps. First, it will evaluate the full requirements of the ITO and identify the desired effects. Secondly, and perhaps the most critical of the three steps, it will plan and conduct trade-offs on the best possible network resources, capabilities and configurations to support desired ITO effects. Decisions must be made on quality of service (QoS), bandwidth allocation, redundant pathways, available relay support and course of action (COA) development to ensure subnets expected for use are available, secured, defended and survivable. COAs must be developed to determine response actions in a degraded network environment. Finally, the combat plans division will establish and map network requirements to specific ITO requirements and task units to execute the network plan through the CCO. The CCO communicates COAs to address critical and imminent NetOps that enable air, space and cyberspace operations.

Refer to Figure 9, below, as an example of the ITO and CCO battle rhythm flow.

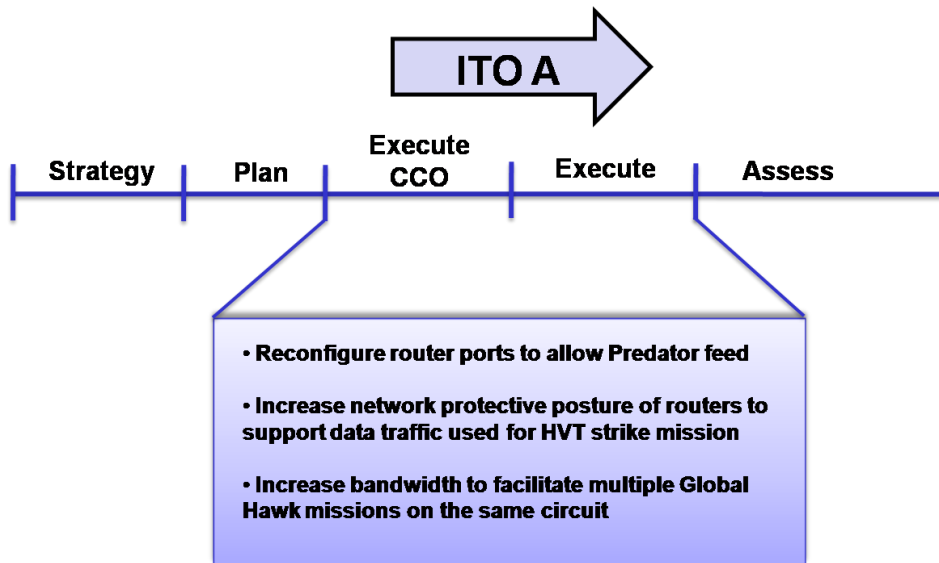


Figure 9, CCO and ITO Battle Rhythm

It is important to note there is a fundamental difference between CCO and MTO-related tasks. Figure 10, highlights these differences and describes the notional criteria used by CCC personnel to differentiate between tasks appropriate for the CCO, and those tasks appropriate for the MTO. Cyber control cell personnel must be able to accurately gauge a task and direct it to the appropriate *responsible* office. This chart is notional in that it does not include all criteria used to differentiate between a CCO and MTO task. Additional criteria will be developed as this concept matures.

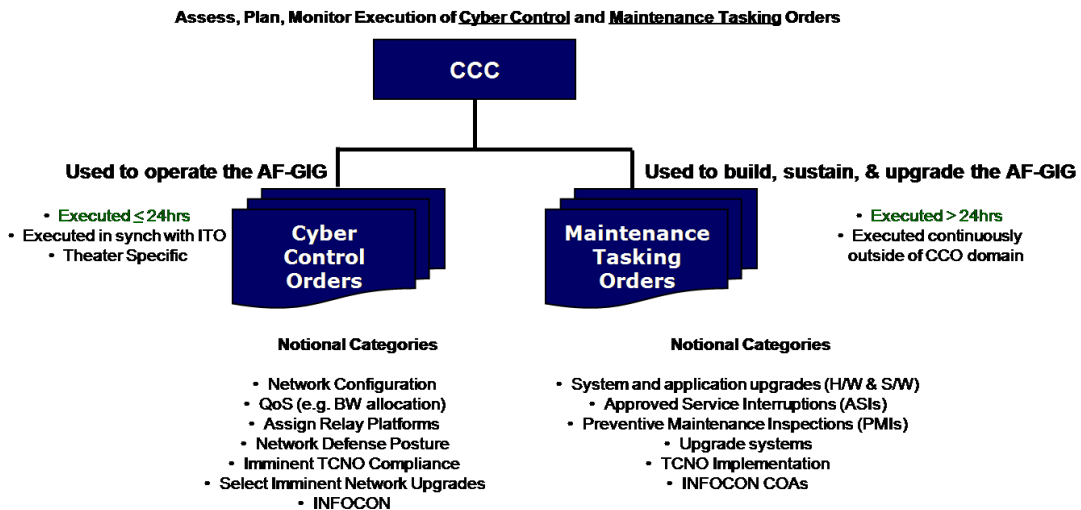


Figure 10, CCO vs. MTO

6.6.2. Integrated Tasking Order

The ITO is the primary document for tasking defensive and offensive cyber operations. It will be used to task 24 AF subordinate units to perform cyber operations. One example of an ITO tasking would be to task the 92 IOS to perform a blue team assessment on a specific network asset.

Combat plans division personnel will be responsible for developing cyberspace tasks for ITO inclusion. All ITO tasks will be reviewed during the daily Master Integrated Cyber Plan briefing and the ITO will then be forwarded to 24 AF wings for execution. The CyOC Combat Operations Division will be responsible for tracking the current status of all ITO tasks.

6.6.3. Maintenance Tasking Order

The MTO is a proactive mechanism to build, sustain, secure, and upgrade components of the AF GIG in alignment with DoD standards. These maintenance tasks are critical for the long-term survivability of the AF GIG. Maintenance activities address the overall general health and welfare and fundamental security aspects of the network and are not specifically aligned to combat operations or I/ATO activity. The MTO differs from the Network Control Order (NCO) in several ways. First, maintenance activities are those defined as being outside of a 24-hour I/ATO cycle; where they will require an extended timeframe for compliance. Conversely, network activities conducted in response to an ITO timeframe would be tasked through an NCO. Second, MTO activities do not

directly impact near-term air, space, or cyberspace operations. Finally, MTO actions may include policy or other non-operational issues.

To develop an effective MTO process that provides for a well defended AF GIG, 24 AF must first ensure to the extent possible, the Air Force network conforms to a standardized configuration schema. This is necessary to increase the overall effectiveness of system patches and will enhance the defensive posture of the network. Adherence to the configuration standards should be monitored by 24 AF and enforced by the AFNetOPs Commander.

The MTO process illustrated in Figure 11 ensures tasks are properly assigned and accomplished.

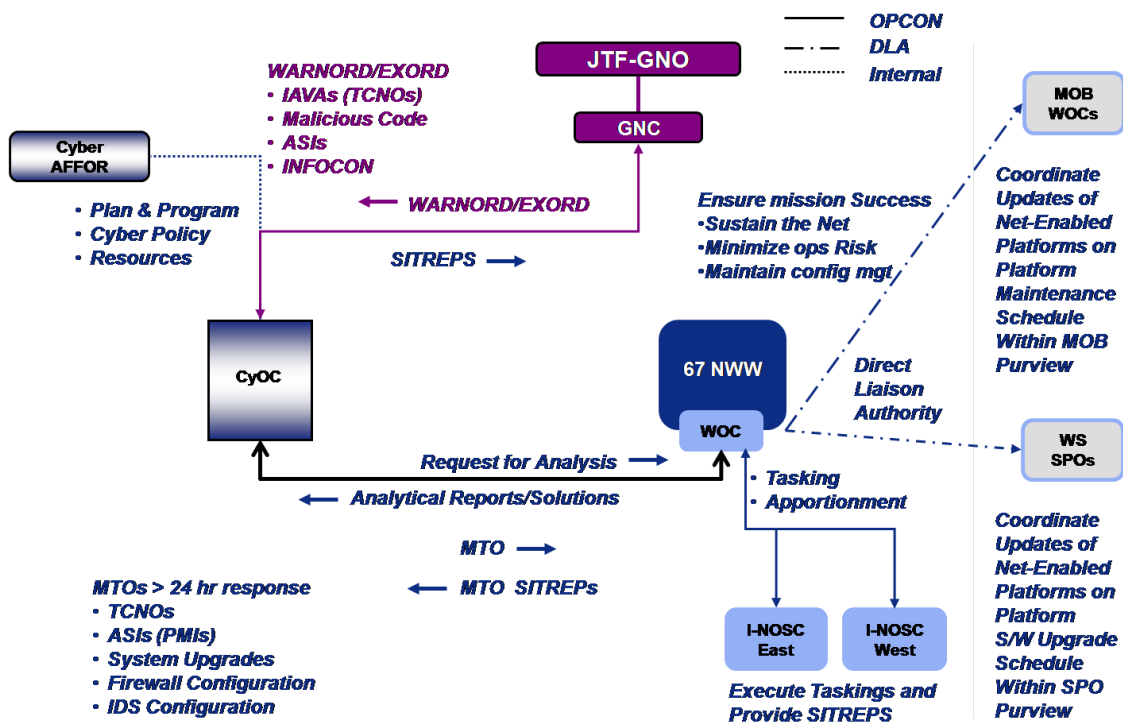


Figure 11, MTO Process

Maintenance taskings can originate from multiple sources, both internal and external to the Air Force. Primarily though, they will originate from the Joint Task Force Global Network Operations (JTF-GNO) or from divisions within the CyOC. JTF-GNO will release Warning Orders (WARNORD) and Execution Orders (EXORD) addressing global network effects to some vulnerability, event or operation. Situational reports up-channeled from the Integrated Network Operations and Security Centers (I-NOSCs) may also trigger taskings for an MTO. Another source for initiating MTO tasks is the development of new DoD, Joint or Air Force policy.

The CCC will process all cyberspace-related tasks. If the CCC determines the task is maintenance related as defined above, they will coordinate the task with the CyOC divisions to ensure it doesn't interfere with on-going or planned operations. After coordinating the task, the CCC will generate the MTO and forward it to the 67 NWW for execution. The MTO will include SPINS that dictate the compliance time frame, any "black-out" periods to avoid interfering with an operational activity, and any other information specific to each task within the MTO. The 67 NWW will be responsible for coordinating task activities with subordinate cyberspace-related units, developing the task, distributing the task to subordinate units, tracking task completion and forwarding compliance statistics to the CCC for situational awareness. To accomplish this task, the 67 NWW will utilize the AFNetOps Commander approved Change Management Technical Order (CMTO). An inherent part of the procedures highlighted in this CMTO will be a "backout plan." If a change to the network does not execute as planned, 67 NWW personnel will execute the backout plan to restore the network to the previous state capable of supporting combat operations.

As an example, the JTF-GNO releases a WARNORD to the service components to address some vulnerability, malicious code activity, or upgrade. The WARNORD provides the service components the opportunity to address, evaluate, assess, and report on the feasibility of the activity, before directing execution through an EXORD.

The CCC will receive the WARNORD and forward it on to the operations division of the CyOC for execution. Based on inputs from all service components, the JTF-GNO may release an EXORD via a Communications Tasking Order (CTO). The CCC evaluates the CTO against any planned or ongoing operations to assess possible impacts and adjusts the execution timeline accordingly. If the urgency of the CTO is sufficiently high (e.g. there is an immediate threat), the CCC will alert all CyOC divisions so adjustments to operations can be made via a CCO. At that time, the CCC releases the MTO to the 67 NWW. Effected organizations will comply with the MTO and respond with a SITREP updating the 67 NWW and ultimately the CCC.

7. Cyber Requirements

7.1. Cyber Planning

The CyOC's goal is to effectively plan for full spectrum global cyberspace operations. Twenty-Fourth Air Force units with their limited resources must be integrated into the planning process to ensure all Air Force capabilities are addressed in CyOC plans. When considering the effects desired by a COCOM, the CyOC must be able to integrate a variety of capabilities to produce an effect. For example, this could eventually involve using Compass Call assets to conduct attacks against networks, such as radio communications networks, while other units conduct computer network attacks (combined with kinetic strikes as required) to produce a single integrated effect. The CyOC must also have the ability to integrate these global cyberspace options to support regional component commanders, giving them the capability to integrate kinetic and non-kinetic options.

7.1.1. CyOC Planning and Analysis

There are several activities that will be conducted as part of planning for network operations. They include, but are not limited to, the following:

- **Mission Analysis.** During mission analysis, the operations and network planners develop the communication/network systems estimate. Operations personnel (perhaps the Interface Control Officer) assign specified and implied tasks to be performed by the network planners, managers, and technicians.
- **Information Needs Analysis.** Information needs are analyzed by working closely with all functional communities to develop information exchange requirements, which identify products to be transmitted and received, as well as the throughput, quantity and characteristics of those products.
- **Interoperability and Compatibility Analysis.** Planners identify interoperability, compatibility, and supportability requirements and assess them against documented capabilities, assessing any shortfalls or deficiencies for operational and mission impact.
- **Capability Analysis.** Based on these first three areas, planners conduct a capability analysis to identify the communications equipment and networks with the capability to support the operational plan. This analysis is a daily assessment during all phases of the operation.

7.2. Command and Control of Cyberspace Operations

The CyOC must have the ability to monitor ongoing cyberspace operations and adjust as necessary to ensure Commander, AFNetOps goals are accomplished. This is especially true for the defense of the AF GIG. The CyOC must have the ability to recognize attacks beyond the AF GIG boundary, determine the intent of the attack, attribute the attack to its source and defend its mission essential resources. It must also have the ability to produce deterrence options to dissuade the threat from attacking. To accomplish this, the CyOC must have situational awareness, the authority to coordinate and synchronize forces and the ability to C2 cyberspace forces across the entire AF GIG. Operations in cyberspace are not limited to a specific geographic region, therefore, the Commander, AFNetOps must be able to operate across the entire Air Force portion of the GIG, irrespective of traditional regional AOR boundaries.

7.3. Assessing Cyber Operations

Along with the ability to C2 cyberspace operations, the CyOC must be able to assess the effectiveness of any operations under its control. There are two aspects to cyberspace

combat assessment. First, the CyOC must be able to assess the intent and effects produced by the threat in a timely manner. When the AF GIG is supporting COCOM operations in a specific AOR, the CyOC must be able to detect and respond to an attack against the AF GIG before friendly operations are hindered or disrupted. This requires near real-time situational awareness of the entire GIG including DoD portions beyond the AF GIG. Second, the CyOC must be able to assess the effectiveness of its offensive operations through the development and assessment of valid MOEs. The CyOC should be able to leverage all available information to determine if the desired effect was produced.

7.4. Cyberspace Situational Awareness

To enable C2 and to support cyberspace assessment, situational awareness in the cyberspace domain is essential. The CyOC must have the systems and information to provide global situational awareness on computer networks across the electromagnetic spectrum. This will require a close relationship with the Air Force Intelligence, Surveillance and Reconnaissance Agency (AF ISR Agency) and the entire intelligence community. Intelligence and sensor data must be instantaneously shared with the CyOC to ensure a common view of operations within the cyberspace domain. Furthermore, this information must be made available to 24 AF units involved in these operations.

There are several components of CITS Block 30, which offer some situational awareness of the AF GIG. However, these systems were not singularly designed to provide a holistic view of the network. The CITS Block 30 Enterprise Manager of Managers (EMoM), Fault Management System (FMS), and Host System Management (HSM) subsystems are „event-generating“ systems that will be logically grouped together within the Event Management System (EMS).

The Security Information Management (SIM) is an event correlation engine within the Security Management system. The SIM collects data from all IA devices on the network and aggregates and correlates security-related events retrieved from the Security Management system. The correlated security information contains a detailed series of information identifying a probable cause of the security event.

The EMoM system will act as the main event presentation and display tool for the Incident Management System (IMS).

7.5. Cyber Authorities

To accomplish its mission, the 24 AF Commander must have the authorities to operate within the domain to defend the entire AF GIG when under attack. This will require close coordination with the other Air Force Component Commands and MAJCOMs. New Air Force policy documents and instructions may be required to define operational relationships between the 24 AF Commander and other Air Force units. Authorities for offensive operations are included in the EXORD or OPORD for a specific operation. In the future, if more aggressive defensive responses or counter-offensive operations are authorized, authorities would have to be clearly defined and understood.

7.6. Relationship with AFFOR Staff

The Twenty-Fourth Air Force Forces (AFFOR) Staff is responsible for providing support functions for CyOC personnel. Each directorate has a specific function and as such, provides specific areas of support.

The cyberspace forces within the CyOC will be administratively controlled by the 24 AF AFFOR staff. The 24 AF AFFOR staff will provide administrative and logistical support for all cyberspace forces assigned to the CyOC.

To permit comprehensive situational awareness and seamless C2 of all cyberspace forces, the CyOC requires a broad range of capabilities. Many of the current tailored AOC and functional AOC baseline systems and tools will need to be resident in the CyOC. In addition, new systems, tools, and interfaces will need to be developed to meet the evolving requirements of the CyOC.

8. The Evolving Challenge

8.1. Intelligence Support to Cyberspace Operations

Cyberspace operations require a high degree of sophisticated, timely, and technical intelligence. The intelligence required may come from a variety of sources. The CyOC will need to receive information from theater and national level agencies (e.g. NSA) for computer network intelligence. The AF ISR Agency will be a critical part of the CyOC's success. NASIC provides computer network intelligence support to key 24 AF units. This information will be necessary to successful computer NetOps. Finally, AF ISR Agency's GLOBAL HARVEST, an information operations database, provides crucial cyberspace-targeting information.

To reach its full potential, the entire CyOC may need to operate at the TS/SCI level. This will allow the necessary systems and information to be available on the CyOC floor and facilitate activities in the combat operations division. Obviously, converting the entire CyOC to a TS/SCI environment will be a lengthy process and will limit access for those not cleared, but may ultimately improve planning, enhance C2 and increase assessment efficiency.

8.2. Network Situational Awareness

The CyOC cannot defend or fight on the network without battlespace visibility. To be effective in computer NetOps, the CyOC must be able to accomplish the following:

- Characterize adversary threats in near real-time
- Realize patterns and intentions of disparate adversary actions
- Share automated models of adversary and friendly networks

- COA planning and network modeling
- Cyber reconnaissance for active and passive defense
- Cyber MOE/BDA
- Adversary COA development
- Attack sensing and warning (AS&W) outside the AF GIG

TREASUREMAP is a national capability for building dynamic network models which enable cyberspace situational awareness and NetOps. This classified system will be integrated into the CyOC to provide a basic network visualization tool and to facilitate integration with JTF-GNO and other national agencies.

8.3. Air Force Network Operations (AFNetOps): The Foundation of Cyberspace Operations

8.3.1. AFNetOps

Air Force Doctrine Document (AFDD) 2-5, defines AFNetOps as the integrated planning and employment of military capabilities to provide the friendly net environment needed to plan, control and execute military operations and conduct service functions.

AFNetOps provides operational planning and control. It involves time-critical, operational-level decisions that direct configuration changes and information routing. AFNetOps risk management and C2 decisions are based on a fused assessment of intelligence, ongoing operations, commander's intent, blue and gray forces disposition, net health, and net security. AFNetOps provides the three operational elements of information assurance, network/system management, and information dissemination management.

The AFNetOps Program Action Directive 07-10 states that the AFNetOps Organization (Cyber Coordination Cell) is designed to enhance the enterprise management, situational awareness, network defense, and C2 of all Air Force terrestrial, space, and airborne networks (collectively known as the AF GIG) in support of air, space and cyberspace capabilities across the full range of military operations. Currently, the AFNetOps construct is focused on the terrestrial segment of the AF GIG. Follow-on efforts that expand cyberspace operations will include integration of the AFNetOps capability to manage, monitor, and defend and C2 airborne and space networks as part of the AF GIG.

8.3.2. Integration of Airborne Networks into AFNetOps C2 Construct

As described in the ACC/A6 Airborne Network Modernization Initiatives Report, there are a number of modernization efforts currently impacting airborne network capabilities. These initiatives include:

- The Joint Tactical Radio System (JTRS) is building a complete mobile wireless network infrastructure. AFNetOps must collaborate with that effort to most effectively address the defensive aspect/tactical component of the Air Force's cyberspace AOR.
- Requirements for a tactical networks management system are being defined and specifics include network planning and C2 capabilities. These requirements are specified in a draft Capability Development Document addressing the Airborne Network Control System (ANCS). AFNetOps should efficiently integrate ANCS capabilities with the 24 AF CCS and CyOC weapons system for effective NetOps C2.
- There are a growing number of unique and limited airborne network initiatives that have or are planning to connect to the GIG. AFNetOps will be required to provide relevant operational support to these systems within current constructs. The systems requiring operational support include the Joint Surveillance Target Attack Radar System, AWACS, Rivet Joint, and Beyond Line of Sight capabilities, mid-term Battlefield Airborne Communications Node, Rapid Attack Information Dissemination Execution Relay, and Objective Gateway (OG) efforts; but this list is not all inclusive. Additionally, fifth generation F-22 and F-35 data links will also require AFNetOps support. Airborne networks such as Network Centric Collaborative Targeting (NCCT) are tying together airborne C2ISR platforms with ground systems. AFNetOps must support C2ISR networks such as NCCT by providing assistance with information assurance, network/system management and information dissemination management.

8.3.3. Objective Gateways

Existing capabilities and follow-on, unique network initiatives are contributing to an expanding heterogeneous network, which is inherently difficult to manage, monitor, defend and C2. As a first step to integrate these platform centric capabilities, the Air Force initiated development of Objective Gateways (OGs). The OG will provide interconnection and interoperability between platforms and systems using similar and dissimilar data links, voice radios, civil systems and GIG elements to achieve network-centric capabilities, facilitating broad information exchange of targeting, C2, situational awareness, surveillance and intelligence information. The OG will create a bridge between bandwidth-constrained legacy tactical data networks, space networks and the bandwidth/service-rich GIG.

As an initial step, AFNetOps should develop and integrate capabilities to manage, monitor, defend and C2 OGs. This may be accomplished through development efforts of the JICO Support System and/or the ANCS and enables the AFNetOps capability to manage, monitor, defend, and C2 the Airborne Network interface to the AF GIG.

As OGs become a homogeneous aspect of the GIG and future capabilities such as JTRS are integrated into Air Force platforms, the network becomes easier to manage, monitor,

defend, and C2. This will enable AFNetOps organization to control more of the AF GIG, as it expands throughout the airborne subnets.

8.4. CyOC Systems

To permit comprehensive situational awareness and seamless C2 of all cyberspace forces, the CyOC requires a broad range of capabilities. Many of the current tailored AOC and functional AOC baseline systems and tools will need to be resident in the CyOC. In addition, new systems, tools and interfaces will need to be developed to meet the evolving requirements of the CyOC.

To begin automating the creation and dissemination of network taskings and directives, the CyOC will use off the shelf workflow software and web-based tools to collaborate, task, and direct Air Force cyber forces. ESC plans on eventually developing and fielding a comprehensive C2 and network awareness tool called the Cyber Control System, (CCS).

The following functions are needed to efficiently operate the CyOC:

- Persistent network mapping with logically displayed up-to-date network status
- Constant network monitoring, not just routine traceroutes and pings, but actual network performance monitoring
- Predictive port use models – network activity divided into every port, every minute, every day – unusual port activity will help predict attacks
- Information sharing between 24 AF units, an easy to use collaboration tool to facilitate deliberate and crisis action planning, exercises, capabilities / operational based research,
- Effective intelligence feeds – easily disseminated to all effected units
- Open source network and software vulnerability information – from national threat level conditions to the latest US-CERT data
- Command and control functions separated from publically accessible networks – designed to update system settings, reboot equipment, and to conduct forensic analysis as required
- Network information database for on-the-fly network analysis, algorithm testing, and forensic analysis
- Disciplined, authoritative network inventory with live data to feed the up-to-date network map (see SAF/XCI report on OBY)

A list of CyOC baseline systems required for the CyOC is in Figure 12, CyOC Systems.

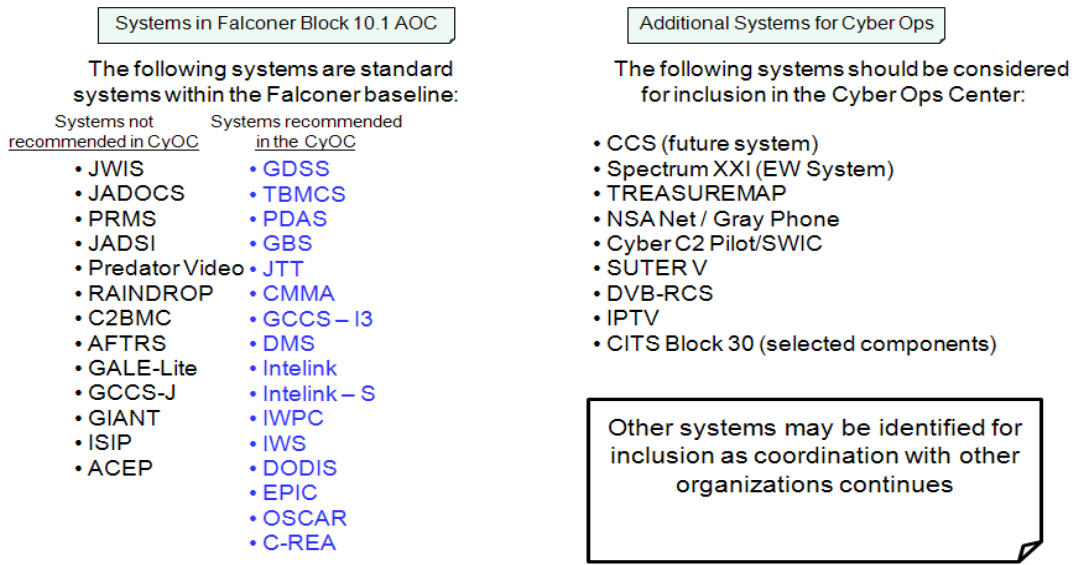


Figure 12, CyOC Systems

8.5. IO Range and VisION

The Joint Forces Command’s IO Range will provide the CyOC access to the largest cyberspace range in the DoD. This will enable:

- Participation in joint and Air Force cyberspace exercises
- Participation in cyberspace-related Advanced Concept Technology Demonstrations
- Participation in 24 AF tactics development exercises at the joint and Air Force level
- Participation in RED FLAG and other multi-domain exercises conducted at IO Range nodes
- Participation in operational test and evaluation (OT&E) of cyberspace, CyOC, and kinetic systems tested within the IO Range environment

When the IO Range service delivery point is installed in the CyOC, this will also provide the CyOC access to Virtual Integrated Support for the Information Operations eNvironment (VisION). VisION is a follow-on program that incorporates the capabilities of the Information Operations Planning Capability – Joint (IOPC-J) and the Joint Integrative Analysis and Planning Capability (JIAPC). VisION rides on the IO Range

backbone and will provide the CyOC access to the collaborative planning environment provided by VisION. As VisION matures, it will become the DoD's cyberspace planning capability, bringing together intelligence stakeholders, warfighters and developers.

8.6. Training

Development of a mature cyberspace career force is an imperative for effective full-spectrum combat operations. While a detailed cyberspace career force development plan is in place and coordination with all appropriate organizations is underway, there is an existing significant shortfall in personnel that must be bridged through an enhanced understanding of the CyOC mission.

Several actions are required to establish a training program enabling the effective stand-up of the CyOC. First, individual training requirements for each crew position in the CyOC need to be identified based on the individual task requirements. Then, an inventory of the currently available CyOC and AFNOC training materials needs to be performed. This inventory should include all types of existing courseware, regardless of format.

Once the training inventory is completed, a training plan should be developed allowing all personnel to receive their required formal training prior to CyOC IOC. This should include completion of the CyOC Initial Qualification Training course. Exercises should be conducted at regular intervals during the training to identify shortfalls and reinforce the training. Training completion should be properly documented and progress monitored on a regular basis.

The Exercise CYBER STORM II After Action Report (AAR) highlights some of the current shortcomings that can be addressed, at least in part, through enhanced training. CYBER STORM II was conducted from 11–14 March 2008 and is a National Cyber Exercise examining processes, procedures, tools and organizations in response to a multi-sector coordinated attack through, and on, the global cyberspace infrastructure. Among the areas for improvement highlighted in the AAR are: monthly scenario interaction and discussion, an increase in 608th AFNOC operational experience, increase attendance at cross-functional training events, and an increase in the opportunity for AFNOC personnel to brief their processes and capabilities.

8.7. CyOC role in Tactics Development and Evaluation

The CyOC will be a necessary component to cyberspace tactics development in the Air Force. With its central role in Air Force cyberspace operations, it will support the development of cyberspace C2 tactics. The AFIOC currently supports cyberspace tactics development and in conjunction with the CyOC will develop cyberspace C2 tactics.

9. Flight Plan for Cyber Operations

Optimally, the processes and system requirements for the CyOC would be developed and sequenced before any implementation work begins. However, the unusual time

constraints require the simultaneous identification of system requirements and the development of the processes and procedures in parallel with implementation actions. In addition, training curriculum must be developed as the procedures are defined; therefore, it is recommended that a detailed implementation plan be developed as the operational concept is refined and approved. In addition, units with the requisite expertise, such as the 67 NWW, and Air Force Information Operations Center (AFIOC), and the AF ISR Agency should be leveraged to provide cyberspace training to CyOC personnel.

The key milestones and timelines recommended for the CyOC to reach its operational goals are in the table below. This list is not exhaustive, but highlights key events that must happen on the road to operationalizing cyber in 24 AF.

	Near Term (Next 6 Months)	Mid Term (7 Months to IOC)	Long Term (IOC to FOC)
Training	Develop/Validate formal training program for CyOC	Conduct initial exercise to validate and train concept	
	Conduct cyber training for CyOC and AFFOR staffs	Conduct full spectrum cyber exercise	
Personnel	Begin administrative process to obtain SCI clearances for all CyOC personnel	Man CyOC and AFFOR staffs to IOC levels	Man CyOC and AFFOR staff to FOC levels
		New Cyber Career Field implemented	
Technology	Refine the intelligence operational architecture to support cyber with emphasis on Het-D		
		Complete work on intelligence operational architecture	
		Develop process and acquire systems to map cyber operations to AF-GIG architecture	Finalize systems necessary to map AF operations to AF-GIG architecture
			Field first spiral of the Cyber Control System (CCS)
			Field follow-on CCS spirals integrated common operational picture for cyber ops)
Communications	Begin socializing operational concept with key stakeholders	Socialize AF cyber operational concept with joint organizations	
Operations	Define 24AF operational IOC and FOC criteria		
	Develop deliberate plan for defense of the AF-GIG		
	Identify and acquire existing systems to feed Het-D situational awareness	Field Het-D situational awareness systems in transitional CyOC	
		Develop 24AF Stan/Eval program	Implement 24AF Stan/Eval program
Transition	Begin integration of virtual elements of the CyOC		
	Develop transition plan for migration of CyOC to final location		Transition CyOC to permanent location

Figure 13, Milestones and Timelines

10. Understanding the Cyber Relationships

10.1. Current Command Relationships

The current command relationships for cyber are not clearly defined for all elements of cyber and where they are defined, they do not necessarily follow normal protocols for supporting and supported command relationships. As shown in **Error! Reference source not found.**, Current Command Relationships, squadrons within 24 AF are currently OPCON directly to certain CCDRs, allowing the CCDRs to directly task flights within a squadron. This abnormal relationship can preclude the proper apportionment of forces to support Joint Functional Component Command – Network Warfare (JFCC-NW) and the other CCDRs. It also limits the options to produce the most effective application of all cyber capabilities to produce a desired effect for the warfighter.

The AFNOC is in a supporting role to JTF-GNO for Net-D. Within this construct, the Air Force Computer Emergency Response Team (AFCERT), in its role as the Network Security Division of the AFNOC, has a supporting relationship with JTF-GNO. Specific details are contained within Unified Command Plan (UCP) 02. The AFNOC takes the joint guidance from JTF-GNO as well as Air Force Net-D directives and implements them through the MTO and the CCO. The AFNOC issues the CCO to the 67 NWW for implementation through the I-NOSCs. The 67 NWW develops the MTO in coordination with the AFNOC and implements through its subordinate units.

In today's construct, the Air Force is not involved in Net-A at the operational level of war. While some Air Force component commands may be involved in planning offensive operations within their AOR, no single command has responsibility for apportionment and planning for offensive cyber at the operational level. Air Force units respond directly to joint requirements and in some cases, CCDRs reach down within squadrons for tasking.

Intelligence support for cyber is not currently organized under one command. NASIC provides tactical level intelligence support directly to the 33 NWS for Net-D. Intelligence support at the operational level is limited to what the AFNOC ISR Division can provide. This small division (approximately 5 to 6 personnel) submits its collection requirements to JTF-GNO for processing. However, because of their relatively low priority for Net-D, few of their requirements are satisfied. For offensive operations, the 67 NWW leverages its relationship with NSA and AF ISR Agency to obtain intelligence support. In addition, collection requirements for specific operations can be validated and submitted through the supported CCDR.



Figure 14, Current Command Relationships

10.2. Proposed Command Relationships

A recent SECDEF decision subordinated JTF-GNO to JFCC-NW, consolidating offensive and defensive cyber operations under a single command subordinate to USSTRATCOM. As the DoD continues to move toward a joint command for cyber operations, it is expected that it will be a unified or sub-unified command similar in structure to the existing JFCC-NW organization that exists today. The anticipated command relationships for such a structure are shown in **Error! Reference source not found.** below. In this structure, the Air Force should work to normalize command relationships at the joint level and within the Air Force.

In the proposed structure, 24 AF will serve as the component command to the new joint cyber command. The 24 AF commander will serve as the component commander to the joint cyber command and also serve as the AFNetOps Commander. In this capacity, he/she would have responsibility as the operational level warfighter for both offensive and defensive cyber operations.

Intelligence units supporting tactical cyber units in 24 AF will continue to provide that support to those units. In addition, 24 AF will work with its organic and external intelligence organizations to enhance intelligence to 24 AF at the operational level. Using the virtual CyOC construct, 24 AF leadership will leverage intelligence from geographically separate units. In addition, leveraging its component command role, 24

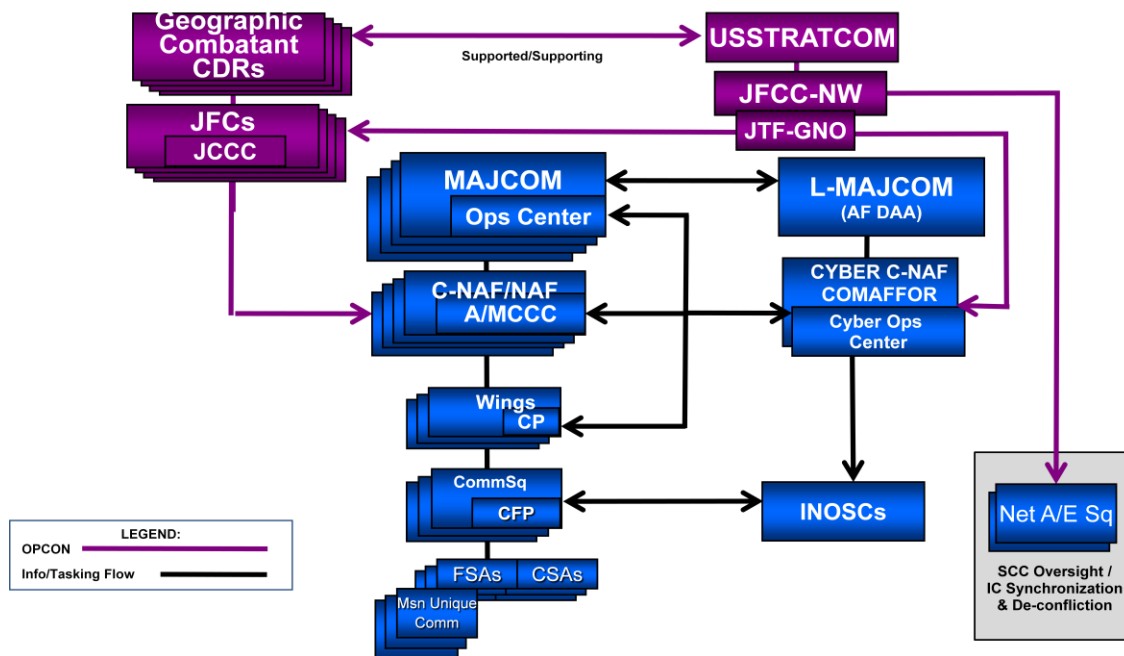


Figure 15, Proposed Command Relationships

AF will submit collection requirements in support of its joint responsibilities through the joint cyber command.

10.2.1. Network Defense Relationships

Twenty-Fourth Air Force will be responsible for Net-D at the operational level. This is new for the Air Force. Today, Net-D is conducted at the tactical level, but defensive operations are not planned and controlled from the perspective of an operational level commander. The 24 AF Commander will be responsible for the development and maintenance of a deliberate plan for defense of the AF GIG. Normally, the Air Force plan for the defense of the AF GIG would be a supporting annex to the joint plan for defense of the DoD GIG. Unfortunately, no such plan exists at the operational level. JTF-GNO has CONPLANS, but they are not operational plans for the defense of the GIG and they are reactive in nature, not proactive plans for defense of DoD networks assets.

The CyOC will enable the command and control of Net-D forces. In this role, the CyOC staff will take the commander's daily guidance, existing strategic guidance, joint direction, and intelligence inputs to refine the Cyber Operations Directive, publish the MTO, CCO, and ITO as part of the operational defense of the AF GIG.

Twenty-Fourth Air Force will exercise operational control of all Air Force networks. This is necessary to ensure the entire network is defended. This control will be exercised

from the CyOC through the I-NOSCs and other 24 AF units. Air Force MAJCOMs will continue to perform the maintenance actions on their networks, but this work will be performed in accordance with the CyOC orders.

To increase the defensive posture of the AF GIG and effectively adapt to a wide range of threats, 24 AF will rely on the Partnership With Industry program to help understand system vulnerability resident on Defense Industrial Base (DIB) partners. The CyOC must also develop processes to rapidly and actively adjust AF GIG defenses in response to incidents occurring on DIB partner networks.

In its mission assurance role, 24 AF will work with the MAJCOMs and deployed units to ensure network availability in support of air, space and cyber operations. This may impact certain base network activities, such as Authorized Service Interruptions. It will be the responsibility of 24 AF through the CyOC to ensure all AF GIG components supporting a mission are ready and available. The goal is to prevent a piece of the network at a CONUS base from being degraded or otherwise impacted when that part of the AF GIG is directly supporting ongoing operations elsewhere.

10.2.2. Network Attack Relationships

Current Net-A relationships are codified in joint documents and war plans and 24 AF cannot modify those relationships without involvement of the affected joint commands. Currently, 24 AF units have supporting relationships with JFCC-NW and other COCOMs. These relationships, in some cases, are very non-standard and should be modified. This is unlikely to happen until the new joint command is activated and the Joint Staff takes a comprehensive look at all Net-A command relationships. There are several considerations that will likely affect future command relationships for Net-A:

- Any Net-A operations that are planned and command and controlled by 24 AF will be as a component command to a joint cyber command.
- Net-A and Net-E will continue to be closely linked, and any Net-E operations conducted by 24 AF will under the authority of the Director of NSA and overseen by the AF SCC, AF ISR Agency.
- Future support to CCDRs will likely be through the joint cyber command in its supporting relationship with the COCOM.
- The goal of 24 AF is to provide joint warfighters with effective cyberspace capabilities, producing desired effects. When 24 AF's credibility and capabilities expand, it will create a compelling need to align offensive AF cyber units within the CyOC's span of control.

In order to ensure 24 AF is in a position to provide real value added to the joint warfighter, the following strategy is proposed for 24 AF support to the joint cyber command. Twenty-Fourth Air Force should work with JFCC-NW to identify Air Force relevant targets on their Joint Integrated Prioritized Target List (JIPTL) and take

responsibility for those targets. This would include developing and maintaining the target folders, developing, testing and updating the capabilities necessary to service those targets, and training and certifying Air Force personnel to deliver these capabilities within the constraints codified in the war plans developed by the joint cyber command. Then, 24 AF should develop the processes and procedures to plan and execute those capabilities through the CyOC. Finally, they must be trained and exercised in a joint environment.

10.2.3. Network Exploitation Relationships

Network exploitation is conducted under the authority of the Director, NSA. It is possible for 24 AF units to conduct Net-E within those authorities in support of joint and Air Force missions. Twenty-Fourth Air Force units will also coordinate exploitation requirements with their national agency partners in support of 24AF's Net-D mission.

10.3. Relationship with Air Force Component Commands

As the Air Force component commander to USSTRATCOM for cyberspace, the 24 AF Commander will interact with other Air Force component commanders in either a supporting or supported role depending on the joint cyber command's role. In addition, the CyOC will coordinate cyberspace operations with the component command's AOC when defensive operations are being conducted to protect the AF GIG. The CyOC will also maintain situational awareness of operations within the combatant command AORs to ensure the network is prepared to support ITOs within those AORs.

The primary interface between the CyOC and the Air Force Component Commands will be the Director, Cyber Forces (DIRCYFOR). Analogous to the DIRMOBFOR or DIRSPACEFOR, the DIRCYFOR is the 24 AF commander's representative in the AOC. He will ensure component command requirements are communicated to the CyOC and will serve as the primary interface between the CyOC and the AOC during cyber combat operations, especially Net-D operations.

10.4. Relationships with Combatant Commands

Normally, the CyOC will support other CCDRs based on the existing supporting/supported relationship established in specific OPLANS. In addition, it is expected that CCDRs will no longer directly task and command and control 24 AF units. Instead, they will coordinate with the CyOC through the joint cyber command or their component commands (via the DIRCYFOR) for the planning and command and control of 24 AF capabilities, and the CyOC will deliver those capabilities based on standing supported and supporting relationships.

10.5. Relationship of the Commander, AFNetOps with Air Force Units

In addition to its relationships with the CCDRs, the CyOC has additional responsibilities as the commander, AFNetOps. In this role, he is responsible for defense and

management of the Air Force portion of the GIG as a weapons system. This role carries two significant responsibilities: the operational defense of the AF GIG and ensuring the AF GIG is prepared and ready to support global Air Force operations. These are global responsibilities. Air, space or cyberspace operations in an AOR may require actions in another AOR to ensure mission success. A threat can attack part of the AF GIG in one region to deny critical mission data to another region (along with potentially gaining access to other parts of the DoD GIG). Therefore, the Commander, AFNetOps must have a global perspective as he protects and maintains the AF GIG. This may require minute-by-minute coordination with the component command AOCs and A6s during defensive operations and critical mission execution. However, the nature of the cyberspace domain requires a single commander with authority to operate across the domain in support of global Air Force mission requirements.

11. Conclusion

With the creation of 24 AF and the CyOC, the Air Force has taken the lead in making cyberspace capabilities a potent combat force for the joint warfighter. As the CyOC matures in its role as the integrator of cyberspace capabilities for the Air Force, it will bring to reality many of the goals of Air Force cyberspace efforts over the past several years. The challenge is daunting but the benefits for the Air Force are significant. This operational concept is the first step in outlining the processes and methods the CyOC will use to reach these goals.

12. Acronym List

AAR	After Action Report
ACC	Air Component Commander
ACEP	AOC Communications Enhancement Package
ACO	Airspace Control Order
AFDD	Air Force Doctrine Document
AFFOR	Air Force Forces
AF GIG	Air Force Global Information Grid
AFIOC	Air Force Information Operations Center
AF ISR Agency	Air Force Intelligence Surveillance and Reconnaissance Agency
AFNetOps	Air Force Network Operations
AFNOC	Air Force Network Operations Center
AFTRS	Air Force Tactical Receiver System-Ruggedized
ANCS	Airborne Network Control System
AOC	Air and Space Operations Center
AOD	Air Operations Directive
AOR	Area of Responsibility
AS&W	Attack Sensing & Warning
ATO	Air Tasking Order
AWACs	Airborne Warning and Control System
BDA	Battle Damage Assessment
C2	Command and Control
CDD	Capability Development Document
CCC	Cyber Coordination Cell
CCO	Cyber Control Order

CCS	Cyber Control System
CMMA	Collection Management Mission Application
C-NAF	Component Numbered Air Force
COA	Course of Action
C2BMC	Command Control, Battle Management and Communications
CNO	Computer Network Operations
COCOMs	Combatant Commands
CTO	Communications Tasking Order
CyOC	Cyber Operations Center
DAA	Designated Approval Authority
DCO	Defense Collaboration Online
DIRCYFOR	Director, Cyber Forces
DLA	Direct Liaison Authorized
DMS	Defense Message System
DoD	Department of Defense
DODIS	Department of Defense Information System
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facility
ELINT	Electronic Intelligence
EMS	Electro-Magnetic Spectrum
EMoM	Enterprise Manager of Managers
EW	Electronic Warfare
EXORD	Executive Order
FMS	Fault Management System
FOC	Full Operational Capability
GALE-Lite	Generic Area Limitation Environment – Lite System

GBS	Global Broadcast Service
GCCS-I3	Global Command and Control System Integrated Imagery and Intelligence
GCCS-J	Global Command and Control System – Joint
GDSS	Global Decision Support System
GIANT	GPS Interference and Navigation Tool
GIG	Global Information Grid
HSM	Host System Management
IBS - N	Integrated Broadcast System - Network
IOC	Initial Operating Capability
IOD	Integrated Operations Directive
I-NOSC	Integrated Network Operations and Security Center
IPB	Intelligence Preparation of the Battlespace
IPOC-J	Information Operations Planning Capability-Joint
ISIP	Intelligence Support Interface Program
ISR	Intelligence Surveillance and Reconnaissance
ISRD	ISR Division
ITO	Integrated Tasking Order
IWPC	Information Warfare Planning Capability
IWS	Information WorkSpace
JADSI	Joint Air Defense Systems Integrator
JAOP	Joint Air Operations Plan
JFACC	Joint Forces Air Component Commander
JFC	Joint Force Commander
JIAPC	Joint Integrative Analysis and Planning Capability
JIOP	Joint Integrated Operations Plan

JTF	Joint Task Force
JTF-GNO	Joint Task Force – Global Network Operations
JTRS	Joint Tactical Radio System
JTT	Joint Targeting Toolbox
JWIS	Joint Weather Impacts System
MICP	Master Integrated Cyber Plan
MOB	Main Operating Base
MOE	Measure of Effectiveness
MOP	Measures of Performance
MTO	Maintenance Tasking Order
NASIC	National Air and Space Intelligence Center
Net-A	Network Attack
Net-D	Network Defense
Net-E	Network Exploitation
NSA	National Security Agency
NTO	Network Tasking Order
NW	Network Warfare
NWOps	Network Operations
OEF	Operation Enduring Freedom
OG	Objective Gateway
OIF	Operation Iraqi Freedom
OPORDs	Order of Battle and Operations Order
OPTASKLINK	Operational Tasking Link
OT&E	Operational Test and Evaluation
PAD	Program Action Directive

PDAS	Planning and Decision Aid System
PMOs	Program Management Offices
PRMS	Personnel Recovery Mission Software
ROE	Rules of Engagement
SA	Situational Awareness
SAP	Special Access Program
SIM	Security Information Management
SME	Subject Matter Expert
SPINS	Special Instructions
SPJ	Self-Protected Jamming
SPO	Systems Programs Office
SOJ	Stand-Off Jamming
STO	Special Technical Operations
TACOPDAT	Tactical Operational Data
TBMCS	Theater Battle Management Core System
TM	TREASUREMAP
TSP	Time Sensitive Planning
TST	Time Sensitive Targeting
USAFCENT	United States Air Forces Central
USSTRATCOM	United States Strategic Command
WARNORD	Warning Order
WS	Weapon System
WOC	Wing Operations Center

XXIII. Appendix 3, System Interface Description/System Node Connectivity Description (SV-1/2)

Appendix 3, *System Interface Description/System Node Connectivity Description (SV-1/2)*, presents the architectural depictions of the projected Air Force Cyberspace mission as described by the HQ USAF PAD 07-08 Change 3: "Phase I of the Implementation of the Secretary of the Air Force Direction to Organize Air Force Cyberspace Forces," 20 February 2009. It addresses the objective organizational changes that placed the cyberspace mission under the responsibility of AFSPC.

System Interface Description/System Node Connectivity Description (SV-1/2)

This Appendix presents the architectural depicts of the projected Air Force Cyberspace mission as described by the Headquarters United States Air Force (HQ USAF) Program Action Directive (PAD) 07-08 change 3, Phase 1 Implementation of the Chief of Staff of the Air Force Direction to Organize Air Force Cyberspace Forces, 20 February 2009. This is the fifth spiral development delivery of the architecture, which addresses the objective organizational changes that puts the Cyberspace mission under the organize train and equip (OTE) responsibility of Air Force Space Command (AFSPC) and establishes the 24th Air Force (24AF) to support operations and maintenance (O&M).

The System Interface Description/System Node Connectivity Description links together the operational and systems architecture views by describing the assignments of system nodes and their connectivity to the operational nodes described in the Air Force Cyberspace Mission Architecture Operational Node Connectivity Description. System nodes include the allocations of specific resources (people, platforms, facilities, and systems) that are being addressed for implementing specific operations. In general, the system nodes described in this architecture either a) originate or terminate the Network Operations (NetOps) Information Exchange Requirements that are defined in the AF NetOps Domain Architecture Operational Information Exchange Matrix or, b) they provide the communications capabilities that support Information Exchange Requirements of the warfighter and functional applications not detailed here.

This version of the System Interface Description/System Node Connectivity Description captures an overview of internal Cyberspace system nodes, systems, and system communications and their connectivity to other internal Cyberspace system nodes or external system nodes. Both organizational and functional views of system node connectivity are provided.

This current description is a work in-progress; efforts to capture the entire system scope will continue well into Calendar Year (CY) 2010 as the scope of Cyberspace activities and systems evolves. Figure 1 captures an overview of the 24th AF Cyberspace Mission Systems in the 2009 - 2010 timeframe.

This System Interface Description/System Node Connectivity Description is currently focused on those systems managed by and used by the AFNetOps Community of Interest (CoI) within the Cyberspace

mission area. Systems used for cyber intelligence, reconnaissance, exploitation, and offensive operations are represented by unclassified notations due to security classification concerns. Further development is required to extend this product to the full scope of the Cyberspace mission.

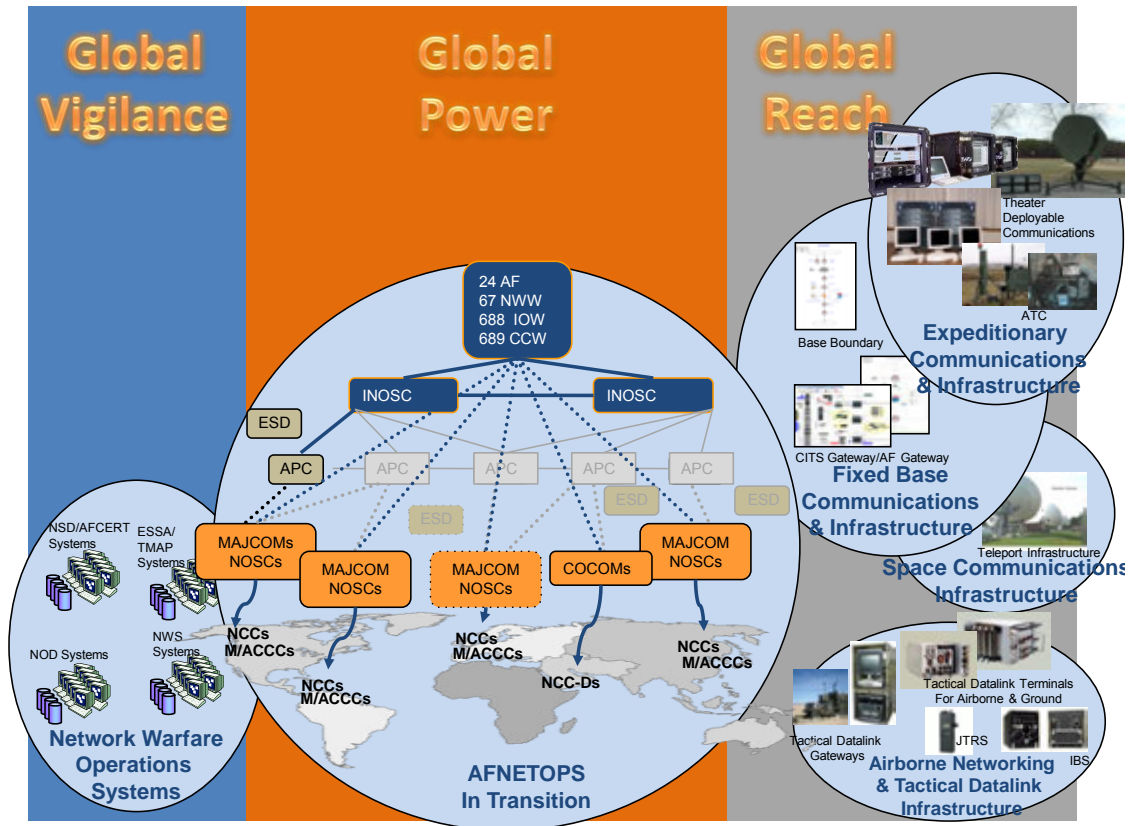


Figure 1. Overview of 24AF Cyberspace Mission Systems at Standup

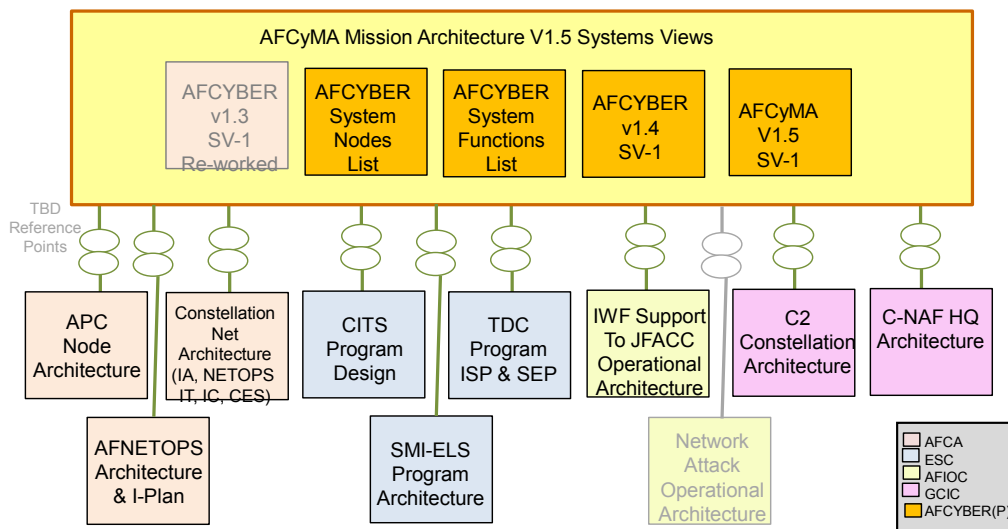
The System Interface Description/System Node Connectivity Description is a mission architecture that supports development of guidance to ensure seamless command and control (C2) of cyber assets in the air, space, terrestrial and cyberspace environments. It describes the expected physical system nodes (major systems that will be used by personnel within the cyberspace mission areas) and their high-level connectivity in the 2009 – 2010 timeframe.

This System Interface Description/System Node Connectivity Description along with other architectural products—the Overview and Summary (AV-1); Integrated Dictionary (AV-2); High Level Operational Concept Graphic (OV-1), OV-2; Organizational Relationships Chart (OV-4); Operational Activity Model (OV-5); Systems Functionality Description (SV-4); and the Technical Standards Profile/Forecast (TV-1/2)

provide content that can be used to answer questions concerning the cyberspace mission to conduct computer network operations and to operate and defend the Global Information Grid.

Rather than duplicating relevant enterprise and program-level architectures for these systems and the mission areas they support, the Cyberspace Mission Architecture identifies “reference points” to those relevant architectures (& other references) (see **Error! Reference source not found.**). The system node connectivity is illustrated with non-specific connectivity, most of which is provided by fixed base infrastructure systems (e.g., Combat Information Transport System (CITS)). The high-level system nodes represent overviews of systems used at operational nodes. These system node overviews can be “drilled” into to provide more granular views by referencing the related architectures and other sources to add detail to system nodes and their interfaces.

AFCyMA V2.0 System View Sources



As of 14 Mar 2009

Figure 2. AFCyMA V1.5 System Views Primary Architectural Sources

Cyberspace Mission Organizational System Node Connectivity Figure illustrates the top-level Cyberspace Mission system node connectivity for the Cyberspace organizational operational nodes. The connectivity shown is primarily via Nonsecure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet) and supports day-to-day operation and management of Air Force fixed base communications and information infrastructure.

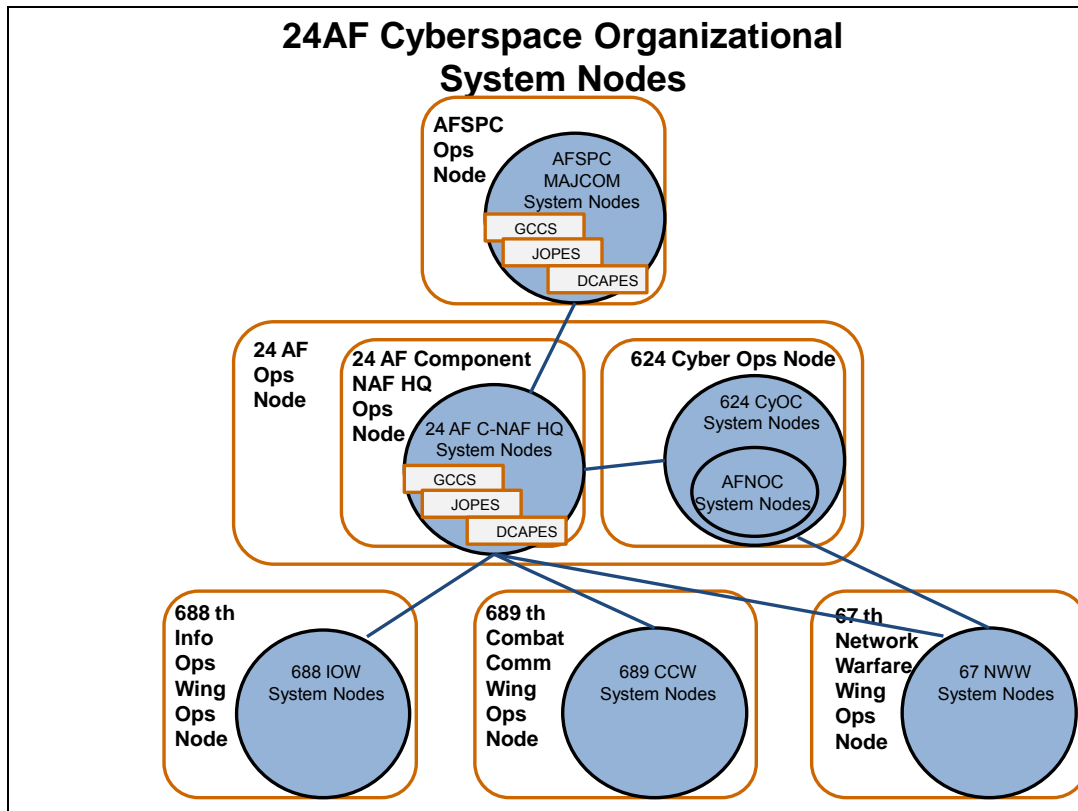


Figure 3. 24 AF Cyberspace Mission Organizational SV-1 for Internal Connectivity

Figure 4 lists the Cyberspace mission systems. AFSPC is responsible for various aspects of these systems to include acquisition, sustainment, management, training, testing, maintenance, experimentation, research and development conducted by multiple, Cyberspace organizational operational nodes. These systems support AFSPC and 24AF operations as well as AF organizations external to AFSPC.

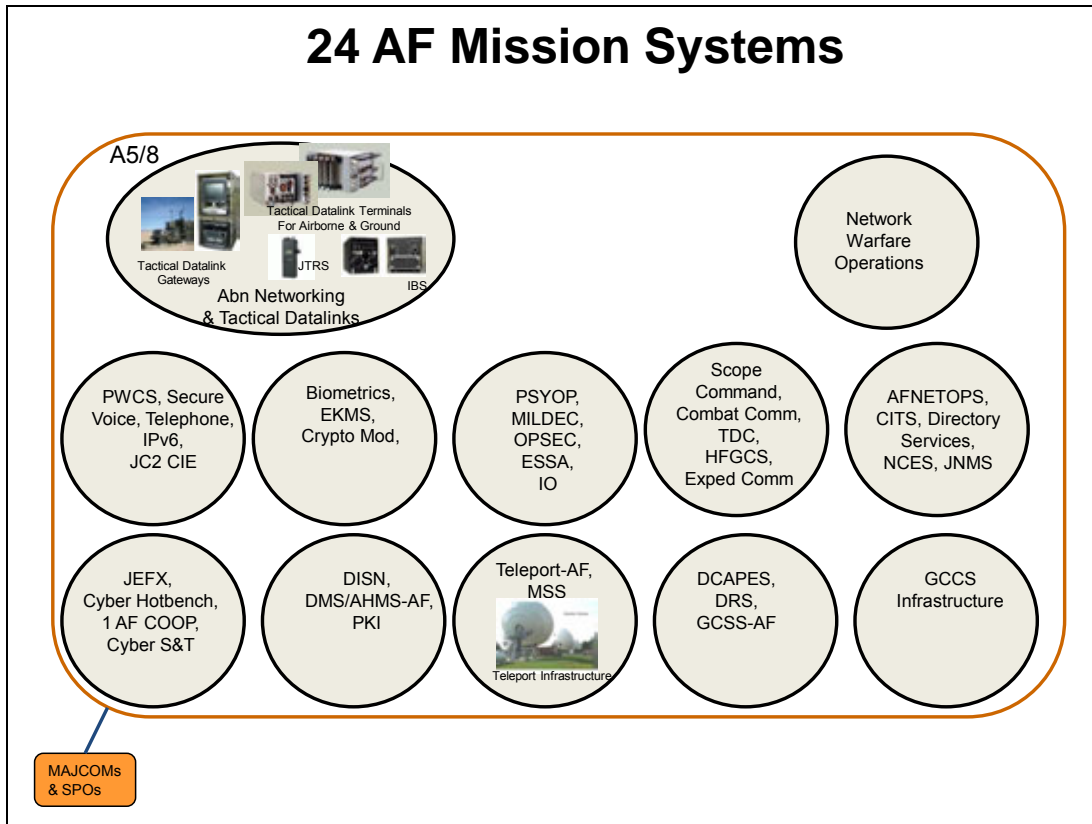


Figure 3. 24AF Cyberspace Mission Systems

Figure 4 through Figure 6 illustrate summary views of 24AF Cyberspace mission system node connectivity for the 67th Network Warfare Wing (67 NWW), 688th Information Operations Wing (688 IOW), and the 689th Combat Communications Wing (689 CCW) and internal operational nodes. Some interfaces to external nodes are shown as interfaces to orange colored organizational nodes. These system node relationships have been derived from the PPlans¹ for each organization. The connectivity shown is primarily via NIPRNet and SIPRNet for day-to-day operation and management of Air Force fixed base communications and information infrastructure.

¹ AFCYBER(P) Programming Plan 08-02, 450 EWW Activation, 22 May 2008; AFCYBER(P) Programming Plan 08-03, 689 Cyberspace Wing Activation, 17 July 2008; Memorandum for HAF/A1, 688 Information Operations Wing Organizational Change Request, not dated.

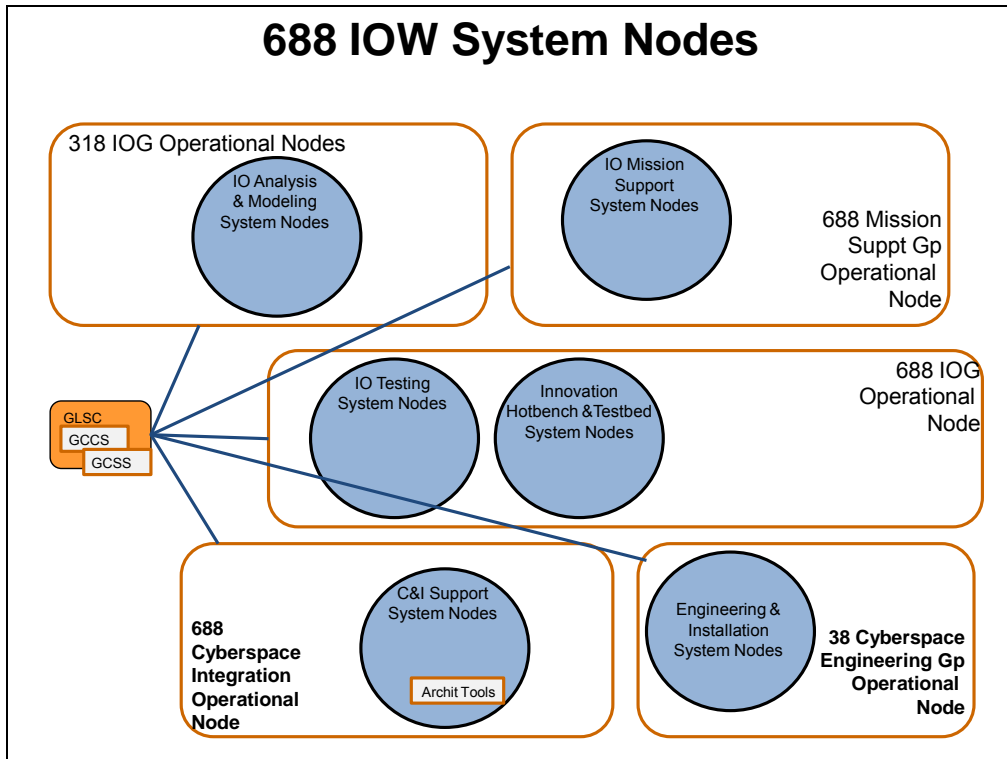


Figure 4. 688 IOW Organizational SV-1 for Internal Connectivity

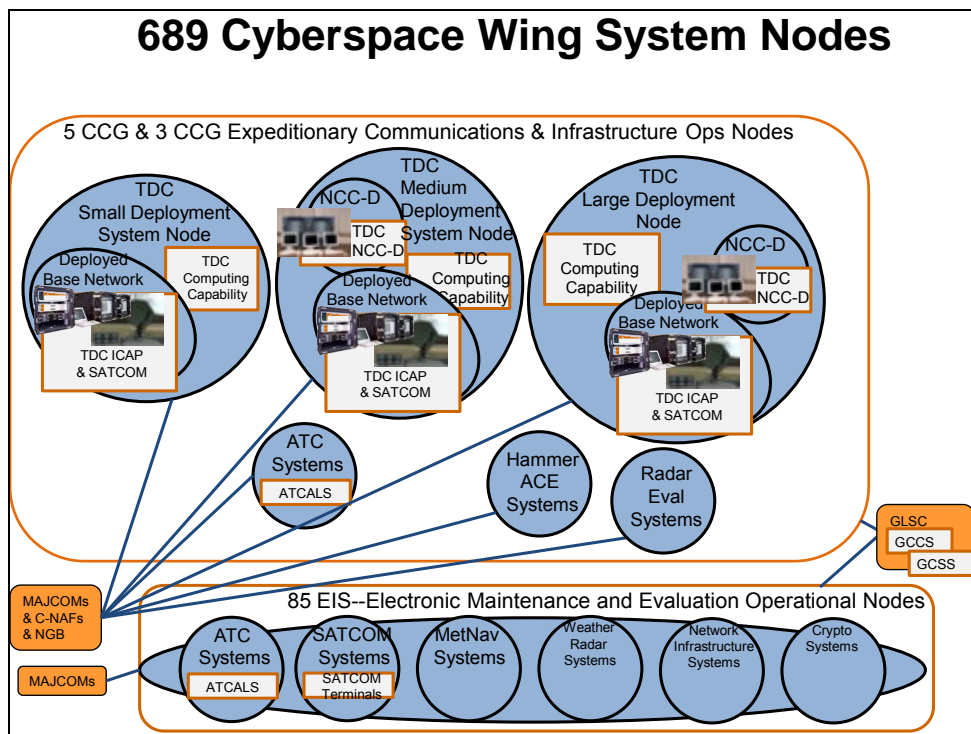


Figure 5. 689 Cyberspace Wing Organizational SV-1 for Internal Connectivity

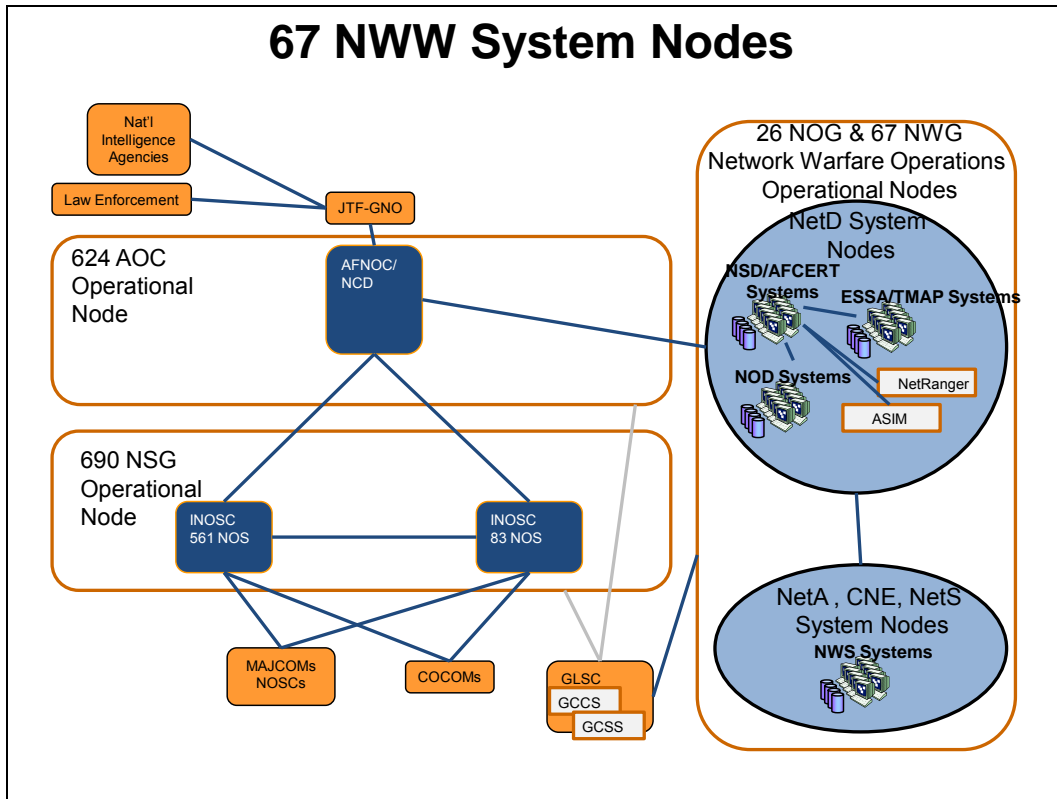


Figure 6. 67 NWW Organizational SV-1 for Internal Connectivity

This version of the Air Force Cyberspace Mission Architecture supersedes earlier versions of the AFCYBER architecture. Updates are based in part on Change 3, to PAD 07-08, dated 20 February 2009. More detail information on the Air Force Cyberspace Mission family of architectural views can be obtained from the Air Force Communications Agency.

NOTES:

1. This draft document is being provided to help inform decisions related to the establishment of the new 24th AF along with its cyberspace mission. This document will be finalized once it is reviewed and approved by the appropriate General Officer's Steering Group (GOSG).
2. In order to reduce complexity and improve document configuration management detailed architectural descriptions of the system nodes in this document may be obtained from other system/node-level segment architectures and other sources listed in references. Figure 2 identifies the primary architectural references.

XXIV. Appendix 4, Expeditionary Communications and Information (EC&I) Enabling Concept

Appendix 4, *Expeditionary Communications & Information (EC&I) Enabling Concept*, describes how the Air Force provides EC&I capability in support of the Joint Forces Air Component Commander and the AFFOR commander. It is based on the approved SAF/XC EC&I Enabling Concept Document. This enabling concept details the minimum expeditionary communications structure necessary to meet Air and Space Expeditionary Task Force (AETF) Force Module (FM), Theater Information Infrastructure, and direct mission support requirements. Additionally, this document standardizes the vocabulary used to describe EC&I forces.

UNCLASSIFIED

EXPEDITIONARY COMMUNICATIONS AND INFORMATION

ENABLING CONCEPT DOCUMENT



SAF/XC

5 Oct 06

OPR: SAF/XCID
Certified by: SAF/XC (Lt Gen Michael Peterson)

UNCLASSIFIED

1. PURPOSE

- 1.1. The purpose of this Enabling Concept is to describe how the Air Force provides expeditionary communications and information (EC&I) capability in support of the Air Force Joint Forces Air Component Commander (JFACC) and the Air Force Forces (AFFOR) commander. In addition, this document standardizes the vocabulary used to describe EC&I forces. This vocabulary set provides the foundation upon which to build a future vision for our EC&I force and develop the principles to deploy those forces within a mature Air Force Network Operations (AFNETOPS) environment.
- 1.2. This Enabling Concept also demonstrates how EC&I forces are used to maximize Agile Combat Support (ACS) and Global Mobility throughout the spectrum of warfare. This is an Air Force-level Enabling Concept created to outline EC&I capabilities and describe how these capabilities are employed to support Air Expeditionary Wings (AEW), above-wing-level functions (including theater infrastructure, AFFOR, and Air and Space Operations Center (AOC) augmentation), and additional missions directed by Combatant Commander or equivalent authority. Definition and apportionment of requirements are documented in the *Expeditionary Communications and Deployable Air Traffic Control and Landing Systems Program Guidance Letter*. This Enabling Concept uses the format directed in AFPD10-28.
- 1.3. After reviewing background on EC&I, this document provides the strategic and operational assumptions that are the foundation for current and near-term EC&I employment. The document then identifies the enablers that allow EC&I forces to accomplish their assigned missions. It begins with a brief description of the various services provided by deployed EC&I forces, and then discusses the sequencing of capabilities during each phase of the deployment.
- 1.4. The EC&I Enabling Concept is a living document and will continue to evolve in response to changing Air Force roles and missions and potential reductions in resources. It lays out the construct that describes how processes use capabilities to create the EC&I effects required for successful operational activity.

2. SCOPE

- 2.1. This Enabling Concept's main focus is on wing-level EC&I forces. It describes those EC&I forces that provide the enterprise information environment for an expeditionary operation ranging in size from a small forward operating location to an approximately 3,000-person airbase. If an AOC is located at the base it will receive communications support from the airbase's EC&I forces. In fact, it is understood that although airbase EC&I forces are attached to the wing they will support any/all communications requirements at their location as theater leadership dictates. This document does not address the Concept of Operations for communicators assigned to other functional areas (e.g. aviation platforms, GTACS, Intel, etc).
- 2.2. The Air Expeditionary Task Force (AETF) Force Module (FM) concept (AFI 10-401, *Air Force Operations Planning and Execution*) serves as the framework for systematic

deployment of conventional EC&I forces. Special operations EC&I forces generally deploy in a similar systematic fashion but are not included in the generic AETF FMs. Special Operations EC&I forces however, are included in the Special Operations Forces Mission Platform Package of the AETF Generate the Mission FM.

- 2.3. Appendix B provides a description of the EC&I forces that support above wing-level missions such as the AFFOR, theater information infrastructure (TII), engineering and installation (EI), postal transportation and other directed missions.

3. BACKGROUND

- 3.1. This document uses the term "expeditionary communications" to broadly describe Air Force EC&I systems, forces (i.e., capability packages including personnel, equipment, or both,) and formations capable of deploying in support of a combatant or joint force commander. The term also describes those services provided or enabled by EC&I forces such as intra-site and ground-air communications, Global Information Grid access, air traffic control, postal, multimedia documentation, and enterprise information management. Each unit that provides expeditionary communications capability may not provide all the above services.
- 3.2. EC&I forces employ different primary skill sets depending upon the maturity of the local enterprise information environment. EC&I forces focus on activating expeditionary communications during initial phases of a deployment, then transition to expanding and robusting services to achieve full operating capability, then set up for perpetual rotational sustainment of these systems and services, to include commercialization and hand-off to reachback service providers. This document describes EC&I forces fulfilling these roles as activation, robusting, and sustainment forces.
- 3.3. The common acronym "TDC" (Theater Deployable Communications) is often confused and used interchangeably to mean expeditionary communications and EC&I forces. TDC actually describes an AF program that procures specific equipment for some expeditionary communications unit type codes (UTCs). TDC does not cover all expeditionary communications equipment (e.g., Global Broadcast System, ground-air-radios, land mobile radios.) Appendix A lists expeditionary communications equipment provided by the TDC program.

4. TIME HORIZON, ASSUMPTIONS AND RISKS

4.1. Time Horizon

- 4.1.1. This document describes expeditionary communications in a non-AFNETOPS-enabled environment and will remain in effect until AFNETOPS reaches maturation after FY08; i.e., when the Integrated Network Operations and Security Centers (I-NOSCs) are capable of assuring, controlling, and providing services at acceptable risk and quality, and within an agreed command relationship for expeditionary enterprise information environments. The

“Future Considerations” section further addresses the implications of an AFNETOPS-enabled environment on EC&I forces.

4.2. Assumptions

4.2.1. Strategic Assumptions:

4.2.1.1. Expeditionary Culture -- Aerospace forces will need to engage across the range of military operations from peacetime engagement through major combat operations (MCO). These forces must react in minimum time and reach their destination with the right amount of aerospace power to produce desired effects. As part of this Aerospace Expeditionary Force (AEF), EC&I professionals must be ready to deploy quickly and effectively because the warfighter requires rapid, secure, and reliable expeditionary communications.

4.2.1.2. Range of Military Operations -- EC&I forces will operate in a continuum of engagements ranging from “steady-state” rotations in an “in-garrison-like” environment through MCO in a bare base environment. Full and seamless communications are essential to ensure a consistent flow of information from the warfighter to the strategic decision maker and to enable reachback to in-garrison forces and distributed operations.

4.2.2. Operational Assumptions: This set of operational assumptions provides a greater level of fidelity in capabilities and effects necessary to meet the challenges of providing EC&I capabilities.

4.2.2.1. EC&I Infrastructure -- Air Force personnel will be tasked to deploy to locations that have varying levels of EC&I infrastructure. EC&I forces may deploy to and operate from a range of locations to include bare bases, en route facilities at international airports, host nation installations, forward operating locations, and main operating bases.

4.2.2.2. Threat environment -- Air Force personnel will be tasked to deploy to locations that have varying threat levels. The operational environment at these locations can vary from permissive (i.e., host country military and law enforcement agencies have control as well as intent and capability to assist operations) to semi-permissive (i.e, host government forces, whether opposed to or receptive to operations, do not have totally effective control of the territory and population in the intended operations area.) Generally, conventional EC&I forces do not operate in truly-hostile environments in which hostile forces have control, intent, and capability to effectively oppose or react to operations. However, special operations EC&I forces are able to operate in a hostile operational environment.

4.2.2.3. Conventional EC&I activation forces:

- 4.2.2.3.1. Must be able to operate in permissive to semi-permissive environments to relieve air base opening forces.
- 4.2.2.3.2. Operate primarily “inside the wire” but must be capable of limited organic site defense and force protection.
- 4.2.2.3.3. Generally require base operating support (BOS). Some EC&I forces (e.g., Deployable Independent Comm Element) have organic BOS for up to 3 days and can operate indefinitely with resupply.
- 4.2.2.3.4. Will meet individual and UTC readiness levels defined in AFI 10-403 for their position.
- 4.2.2.3.5. EC&I activation forces must be ready to deploy within 24 hrs of tasking notification.

4.2.2.4. Conventional EC&I robusting forces:

- 4.2.2.4.1. Operate “inside the wire” and require BOS.
- 4.2.2.4.2. Some robusting forces may be trained to activation force standards to enable full operational capability in semi-permissive environments.
- 4.2.2.4.3. Will meet individual and UTC readiness levels defined in AFI 10-403 for their position.
- 4.2.2.4.4. Must be ready to deploy within 72 hrs of tasking notification.

4.2.2.5. Conventional EC&I sustaining forces:

- 4.2.2.5.1. Conventional EC&I sustaining forces operate “inside the wire” and require BOS.
- 4.2.2.5.2. Must be able to operate in permissive to semi-permissive environments to activate specialized expeditionary communications services (e.g., multimedia, postal, enterprise information management), round out EC&I unit capabilities, and relieve EC&I activation and robusting forces.
- 4.2.2.5.3. Will meet individual and UTC readiness levels defined in AFI 10-403 for their position in the AEF schedule.
- 4.2.2.5.4. Certain sustainment forces (i.e., those providing specialized expeditionary communications services) must be ready to deploy within 72 hrs.

- 4.2.2.6. Airlift: EC&I forces will have sufficient airlift allocated to deploy so communications and ATCALS will be available to the warfighters when required. EC&I forces will gradually build expeditionary capabilities at bare bases as depicted in the AETF FMs.
- 4.2.2.7. Spectrum: Theater spectrum managers will effectively manage frequency assignments to prevent interference among deploying forces, host nation, and coalition partners.
- 4.2.2.8. Satellite/Gateway Reachback: The supported Combatant Commander will allocate satellite bandwidth and gateway access to support deployed operational requirements.
- 4.2.2.9. Reachback Architecture: EC&I forces will implement a satellite “spoke” architecture at AEW locations. The AFFOR A6 will designate appropriate AEW locations to implement a “hub and spoke” architecture if required.
- 4.2.2.10. Power and Environmental Control: Expeditionary civil engineers will not support EC&I power and environmental control requirements for the first 30-45 days of deployment. Expeditionary civil engineers will assume EC&I power production and environmental control sustainment after this period. Expeditionary Power/HVAC personnel deploying with Combat Comm units (6KLS1 UTC) during activation phase, should work closely with Expeditionary Civil Engineers to ensure seamless transition from initial activation to sustainment power/environmental control support.
- 4.2.2.11. Modular/Scalable Equipment: Expeditionary Communications and Information forces provide modular, expandable and contractible communications architectures, capable of movement and reactivation in theater. These modular packages will be employed IAW the AETF FM construct (potentially augmented with theater-level capabilities). At AEWs, EC&I capabilities will form into an expeditionary communications squadron (ECS) or expeditionary communications flight (ECF) organization that mirrors applicable portions of a garrison communications squadron.
- 4.2.2.12. Deployment Sequencing: AETF FMs do not execute sequentially and are designed to overlap. AETF FM timelines are not rigid; however, they do provide a benchmark for planners to follow when building Time-Phased Force Deployment Data for operations plans.

- 4.2.2.13. AETF FM Force Structure: By meeting the target force structure defined by the AETF FM planning guidance, the AF can theoretically execute the following:
 - 4.2.2.13.1. At maximum surge, activate five bases simultaneously (eight with ARC mobilization), and a maximum of 25 bases in rapid succession (40 with ARC mobilization).
 - 4.2.2.13.2. Indefinitely sustain a maximum of five expeditionary airbases under normal Air Expeditionary Force (AEF) rotations and without mobilization.
 - 4.2.2.13.3. Sustain three additional airbases (total of 8) by extending rotations to 179-days without mobilization.
 - 4.2.2.13.4. Sustain a maximum of 12 airbases without mobilization under 1:1 dwell conditions; i.e., half the force engaged in deployed operations while the other half executes garrison operations, then alternating them. Ability to sustain airbases in a 1:1 dwell scenario would decrease over time due to lack of reconstitution and training time.

- 4.2.2.14. Stay-behind Equipment: Once forces have established an expeditionary base information infrastructure (BII), EC&I equipment will remain in-place until it is commercialized, replaced by Combat Information Transport System (CITS) equipment, or the mission is complete.

- 4.2.2.15. Commercialization Strategy: The theater A6 (e.g., CENTAF/A6) is responsible for commercialization of communications infrastructure on behalf of the COMAFFOR. The A6 and A6 staff will manage/direct commercialization. Theater communications squadron commanders will assist with commercialization execution.

- 4.2.2.16. Sustainment: The AF will be able to support an airbase's expeditionary BII for the original deployment plus approximately 18-24 months. It can support a CITS-based infrastructure indefinitely with sufficient sustainment manpower.

- 4.2.2.17. Supplies: Units will deploy with sufficient equipment and spare parts to sustain EC&I systems for 30 days. As required, supporting commands may establish forward supply points to cut transportation time for critical parts. The supported command will assign appropriate priority to replacement parts to ensure EC&I systems remain operational.

- 4.2.2.18. Funding: Funds will be available to upgrade and sustain communications resources, and ensure new systems remain interoperable with current systems, as they are fielded.

- 4.2.2.19. Equipment Disposition: Once replaced, technologically current EC&I equipment will be redeployed to meet requirements at other sites in the supported theater or returned to the supporting command. Obsolete EC&I equipment will be disposed of per applicable export regulations. Supporting commands will reconstitute EC&I forces using Emergency/Special Purpose (ESP) funding associated with the operation.

- 4.2.2.20. Access Devices (Information Appliances): The majority of AEW users will provide their own information appliances (e.g. land mobile radios, notebook computers, secure telephone equipment, and other office equipment). Users who do not provide their own appliances will request issuance of equipment through the ECS plans and implementation flight (SCX). While waiting for their requests to be filled, users may request temporary use of available assets to conduct limited operations from lower-priority users by appropriate command authority.

- 4.2.2.21. C&I forces apportioned to non-C&I functional communities and embedded in non-C&I UTCs are self-sustaining. With the exception of forces postured to associate UTCs, C&I forces apportioned to C&I UTCs (6K) will not be used to augment non-C&I UTCs.

4.3. Risks

- 4.3.1. Networks: EC&I forces provide multiple EC&I systems to establish connectivity with theater command centers and reach-back locations. These systems range from dial-up satellite telephones, dedicated single-channel satellite radios, and wide area networks over dedicated multi-channel satellite ground terminals.
 - 4.3.1.1. Dial-up and single-channel systems provide only limited throughput and are not adequate to support large customer populations.
 - 4.3.1.2. Wide area networks provide better throughput. Disruption to wide area networks or denial of service over dial-up or single-channel systems may result in severe degradation to total loss of expeditionary communications services for the AEW.
 - 4.3.1.3. To mitigate these risks, EC&I forces implement a robust, information assurance architecture. IA provides the needed availability, integrity, and confidentiality to allow authorized users to access the information they need to carry out their mission while preventing unauthorized users from denying, degrading, or exploiting that mission.
 - 4.3.1.4. They also deploy a secondary intra-theater communications path, primarily via a second satellite ground terminal, to diversify wide area network connectivity. They further deploy multiple dial-up and single-channel systems to increase probability of successful connections.
- 4.3.2. Readiness: Expeditionary communications Unit Type Codes (UTCs) may not be fully equipped due to a lack of funding, previous deployment, or fielding of centrally-managed equipment. These shortfalls may be partially overcome by extraordinary measures, such as combining equipment from multiple like UTCs or just-in-time procurement from commercial sources. However, delivery delays, product faults or substandard supply chains may reduce AF EC&I capability or logistics sustainability.
- 4.3.3. Information Technology: Users' dependence on new information technology (IT) drives tremendous growth in infrastructure demands. Without investment in development and fielding of new systems, the expeditionary BII will be unable to meet the demands of user applications.

5. DESCRIPTION OF THE MILITARY CHALLENGE

5.1. Continuous Evolution

- 5.1.1. EC&I systems comprising the expeditionary BII are the AEW commander's principal tool for receiving, storing, protecting, processing, transporting, displaying, exchanging, and disseminating digitized information. EC&I systems and forces must provide authorities at all levels with timely and adequate information to plan, direct, and control their activities.
- 5.1.2. As the demand for improved performance increases and new technology becomes available, EC&I systems and forces must continuously evolve to support combat operations within the framework of ACS strategies:
 - Lighter, leaner, more rapidly deployable forces
 - More timely planning and execution capability
 - Agile, responsive, effective sustainment
 - Responsive, well integrated ACS C2
 - Improved interoperability
 - Increased bandwidth usage efficiency
- 5.1.3. As we consolidate/centralize network operations and network defense within the AFNETOPS transformation, we must pursue compatibility with the evolving AFNETOPS and CITS visions for current and future AF and joint comm infrastructure and equipment. We must also promote greater joint consideration, compatibility and integration into these primarily AF-centric programs.

5.2. Agile Forces

- 5.2.1. EC&I forces participate in every level of operation ranging from civil support through major combat operations (MCO).
- 5.2.2. It is critical that war planners and warfighters clearly understand EC&I functional capabilities and AETF FMs to ensure the right forces are called out at the right time and in the right sequence to support the given operation.

6. SYNOPSIS

- 6.1. **EC&I Mission:** The mission of EC&I forces is to provide operational commanders with communication capabilities throughout the full spectrum of conflict and non-combat operations. EC&I forces support air operations by enabling command and control (C2), intelligence, logistics, medical, and other mission support functions from initial deployment through redeployment. The objective is to communicate information rapidly, accurately, and securely to achieve interoperability between deployed AF, joint, and coalition elements throughout the theater and reachback C2 centers.
- 6.2. **EC&I Effects:** EC&I effects are achieved through a diverse suite of systems and capabilities that provide operational commanders with the means to command and control forces in all deployed environments. EC&I also provide the systems required to launch and recover aircraft from a deployed air base in all weather conditions. They range in size from small quick reaction "fly-away" packages to man-portable or

vehicular-mounted single-channel radio systems, to large initial and robusting theater air base communications and air traffic system suites. These capabilities are fundamental to contingency operations, humanitarian relief efforts, or disaster control activities. EC&I forces deploy in a phased manner to activate, robust, and sustain EC&I capabilities.

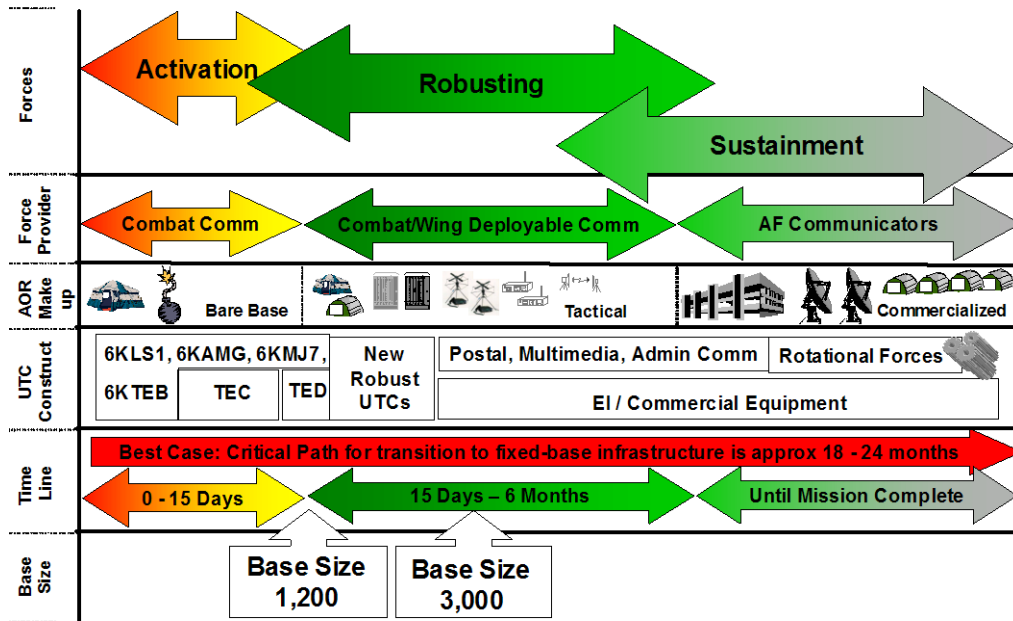


Figure 1 shows relationships between EC&I activation, robusting, and sustainment forces.

7. DESIRED EFFECTS

7.1. Information Superiority and Agile Combat Support: EC&I effects enable information superiority and ACS. EC&I forces provide the speed and precision of information required to sustain flexible and efficient combat operations.

7.2. Warfighter Functions: EC&I forces and infrastructure enable the warfighter to perform the following functions:

7.2.1. Command & Control: Exercise authority and direction over assigned and attached forces in the accomplishment of the mission.

7.2.2. Maintain Situational Awareness: Receive, monitor, integrate, and disseminate information on global actions, critical events, and crisis areas, to include the status of friendly and non-friendly forces, rules of engagement (ROE), treaties, agreements, and physical environmental conditions.

7.2.3. Decide: Make decisions within bounds of authority for the correct application of the military instrument of power in order to achieve desired effects.

7.2.4. Receive Tasking: Obtain commander's Intent/COA/plan in a timely, clear, concise, verifiable, and if necessary, secure and/or interactive manner in a

recipient-defined, actionable format such that mission execution (strategic, operational, and tactical) is not delayed.

- 7.2.5. **Disseminate:** Distribute information collected through surveillance and reconnaissance or decisions reached by appropriate authority.

8. NECESSARY CAPABILITIES

- 8.1. **MCL Tasks:** The Master Capabilities Library (MCL) outlines the EC&I capabilities required to enable ACS and information superiority and are listed below:

- Provide Net Centric Enterprise Information Environment
- Establish local communications infrastructure
- Engineer communications infrastructure and manage projects
- Establish support infrastructure for expeditionary communications
- Establish reach-back infrastructure
- Establish expeditionary communications C2 infrastructure
- Establish voice and data infrastructure
- Establish information management infrastructure
- Establish command and control infrastructure
- Establish visual information infrastructure
- Establish postal operations infrastructure
- Establish air traffic operations infrastructure
- Provide ATC Equipment Support

- 8.2. **Force Mix:** The mix of active and reserve forces must ensure force generation capabilities can support steady state operations. This includes increasing the percentage of military forces available in the rotational base and structuring the force to minimize the need to involuntarily mobilize reserve component members. The AETF FM construct establishes an objective ratio of 5:3 AD to Air Reserve Component (ARC) FMs. However, additional AD or ARC forces are generally not justified by shortfalls in one component, if sufficient forces are available from the other component to cover the shortfall.

9. ENABLING CAPABILITIES

- 9.1. **ACS Effects:** The following ACS effects enable EC&I:

- 9.1.1. **Readied Forces:** EC&I forces organized, trained, and equipped to execute the full spectrum of military operations.
- 9.1.2. **Prepared Forces:** EC&I forces packaged to maximize operational flexibility and responsiveness.
- 9.1.3. **Positioned Forces:** EC&I forces prioritized, right-sized, and poised to support the Combatant Commander.

- 9.1.4. **Employed Forces:** Fully-supported EC&I forces applied to specific military objectives.
 - 9.1.5. **Sustained Forces:** EC&I capabilities continuously engaged to facilitate persistent operational effects.
 - 9.1.6. **Recovered Forces:** EC&I forces must be recapitalized upon return because the equipment deployed typically remains at the expeditionary airbase. Recovered forces must also utilize alternative training sources to maintain their readiness.
 - 9.1.7. **Commercial Sustainment:** EC&I activation forces rely on sustainment forces to relieve their operations and allow them to reconstitute. EC&I forces rely heavily on commercially available equipment or contract logistics support for long-term operations and to reduce personnel rotations.
- 9.2. Supporting Functional Areas:** In addition, EC&I forces also rely on experts in other functional areas for support. These external entities include:
- 9.2.1. **Civil Engineering (CE):** Most of the equipment supporting EC&I services have fairly strict environmental requirements. Among these requirements is stable 110/220 volt, 50/60Hz electrical power; a dry shelter sealed against dust and blowing sand; and air temperatures between 41 and 77 degrees Fahrenheit. While EC&I forces bring an initial capability in the form of tents, environmental control units, and generators, meeting the growing communications requirements of a deployed location dictate that the expeditionary communications unit rely on civil engineering for sustained base operating support. EC&I planners (SCX) should work closely with CE in determining installation layout and coordinating digging efforts.
 - 9.2.2. **Contingency Contracting:** EC&I forces must be able to obtain material locally at a deployed location. EC&I logistics details typically contain enough expendable material, such as wire and connectors, to provide a robust, initial capability. As deployed locations continue to grow or mission changes require the relocation of facilities, these supplies are quickly used up. Acquiring expendable supplies locally reduces need for airlift and speeds delivery time. EC&I planners must identify sources of supplies and services early in the planning process as alternatives to deploying forces. EC&I forces must execute and manage local contracts to produce the commander's desired effects in terms of quantity, quality, and timeliness of EC&I services through sustainment and redeployment.
 - 9.2.3. **Logistics Readiness:** Timely receipt of replacement parts is critical to ensuring the availability of EC&I services. EC&I force packages will first pull parts from materiel readiness spares package (MRSP) kits or other available spares. However, as EC&I forces consume these assets, they must replace them in a timely manner to ensure they can respond to a future system failure. EC&I forces also rely on vehicles and specialized equipment support, such as a 10K All Terrain forklift, for positioning and erecting various EC&I systems.

EC&I forces may further rely on inter-service and host nation agreements to provide BOS services.

- 9.2.4. **Security Forces:** EC&I forces rely on security forces capabilities for site and self-defense training in garrison and force protection when deployed.

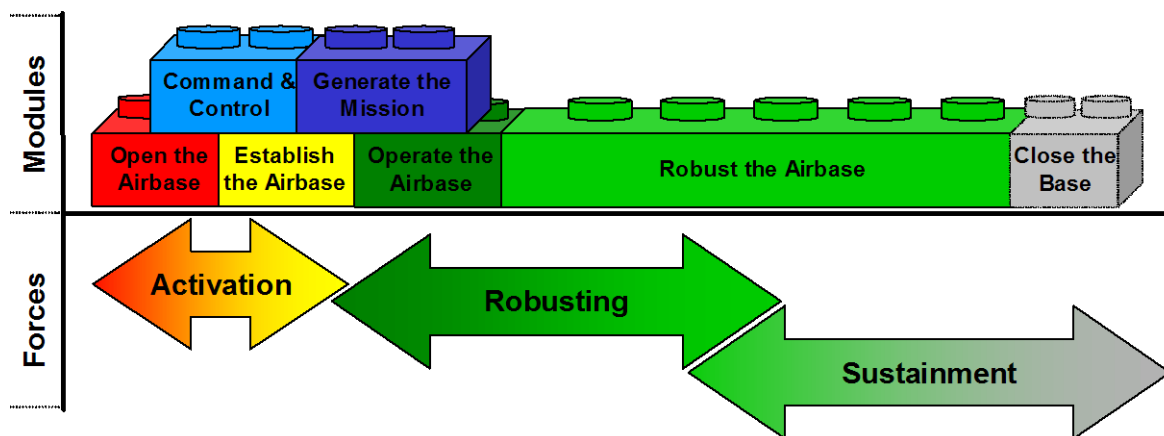
10. DEPLOYMENT STRATEGY

- 10.1. EC&I Force Employment:** AF forces rely on robust EC&I services and infrastructure to provide airpower to the Combatant Commanders. EC&I forces employ in various ways to activate, robust, and sustain EC&I services and infrastructure across the range of military operations.
- 10.2. Activate:** EC&I forces activate the EC&I infrastructure at locations where such infrastructure does not exist. Where long lead times are available, EC&I forces rely on a combination of military and contracted EI forces to engineer, procure, and install EC&I infrastructure. In bare base environments, EC&I rapid response units deploy in standardized packages of equipment, supplies, and forces to activate a temporary EC&I infrastructure.
- 10.3. Robust:** EC&I forces also expand and solidify existing EC&I infrastructure. During bare base activation, robusting forces fall in with activation forces to assist with operating and expanding the temporary EC&I infrastructure, and then assist with the transition of this infrastructure to a more permanent garrison or commercial standard EC&I infrastructure.
- 10.4. Sustain:** EC&I forces operate and maintain both permanent and temporary EC&I infrastructures, as well as provide general and specialized EC&I services. Sustainment forces provide the primary workforce for main operating bases and mature contingency locations. At bare bases, they relieve EC&I infrastructure activation and robusting forces, as well as activate specialized EC&I services (such as deployed air traffic control and landing systems (DATCALs), postal, multimedia, and administrative communications). They also assist with the transition to commercial standard EC&I infrastructure and oversee commercialized EC&I infrastructure and services.
- 10.5. Theater-level EC&I Forces:** Some EC&I forces provide systems and capabilities applied to support theater-level (above wing-level) or directed missions, intra-theater connectivity requirements, and/or special environmental conditions (e.g., terrain challenges, obstructions, geographic separations). These forces also constitute an “operational reserve” of EC&I capabilities available to support AF operations.
- 10.6. First 400 Feet Forces:** Some EC&I forces align organizationally with the customer they support (whether administratively assigned to the communications unit or not). These “First 400 Foot” EC&I forces activate and sustain tailored communication services as well as integrate the EC&I infrastructure into their customers’ operations.

11. SEQUENCED ACTIONS

- 11.1. Readiness:** EC&I forces prepare for deployment through career development course, skill-level upgrade, UTC task qualification, crew position, and operational readiness training, while supporting operational forces and missions from garrison facilities.
- 11.2. Pre-Deployment:** Pre-deployment begins upon receipt of strategic warning message or observation of an event constituting strategic warning. EC&I personnel participate in site surveys and pre-deployment planning to understand initial-deployment communications requirements and develop plans to support the deployment.
- 11.3. Deployment:** Deployment begins when forces depart their home base for the deployed location. EC&I assets incrementally deploy in support of the buildup in the operational area. AETF FMs describe the sequence of actions that activate, robust, and sustain an expeditionary airbase. The AETF FMs, however, do not incorporate all capabilities the Air Force maintains to support the National Military Strategy. AETF FMs do not address airfield seizure forces that secure and prepare the airfield for receipt of Open-the-Airbase forces. Additionally, AETF FMs do not address theater-level missions, intra-theater connectivity requirements, or directed missions, such as en route support for global reach laydown, consequence management, or network security and operations.

Figure 2 below displays an overview of how the EC&I activation, robusting, and sustainment forces tie into the AETF Force Modules described in AFI 10-401, Ch 6.



11.3.1. Open the Airbase Force Module:

11.3.1.1. Warfighter Requirement: This module provides the capability to receive cargo and passengers, protect the force, and maintain initial C2 regardless of the follow-on mission or aircraft type.

11.3.1.2. Communication Capability:

- Organic, customer-provided communications
- Assessment for bed down of EC&I activation forces and specialized EC&I services

11.3.1.3. EC&I Force Providers:

- Contingency Response Groups
- Combat Communications units

11.3.1.4. Summary:

CRG or equivalent forces will arrive first (possibly before the deployment order) to assume control of the airbase from seizure forces or to establish U.S. presence, assess and survey the airbase, address host nation issues, prepare the airfield for initial operations, and relay specific requirements for follow-on forces. Where Host Nation air traffic control and landing systems are not available or not suitable for U.S. military use, special operations forces (SOF) can provide initial air traffic control services for the airfield. If special operations DATCALs are unavailable or unnecessary, DATCALs from Establish the Airbase FM may roll forward to provide more sustainable air traffic services. Similarly, SOF can provide other initial EC&I capabilities to support SOF as well as co-located conventional forces until base-operating support is operational. CRG organic EC&I forces provide limited initial EC&I capabilities for reach-back and local C2. CRG air traffic controllers and EC&I forces provide limited, radio-based terminal air traffic control. A combat communications engineering team arrives to survey, secure, and prepare a suitable location to facilitate the beddown and rapid activation of the temporary EC&I infrastructure arriving early in follow-on AETF FMs. Forces in this module redeploy after forces arriving in follow-on FMs have the capability to assume their functional responsibilities.

11.3.2. **Command-and-Control (C2) Force Module:**

11.3.2.1. Warfighter Requirement: This module contains the capabilities to establish a deployed wing C2 structure to include the AEW (or AEG) command element and an initial maintenance group, mission support group, operations group, and medical group staff. No DATCALs arrive with this FM.

11.3.2.2. **Communication Capability:** EC&I forces establish an infrastructure to C2 and mission area processing by first establishing an initial center to provide limited EC&I services, and then expanding the infrastructure to provide EC&I services at three additional enclaves. Currently fielded equipment provides the following capabilities:

- 175 NIPR/SIPR
- Reachback to CONUS (SATCOM)
- Limited Network Control Center functionality
- LMR infrastructure
- 6 DSN Trunks
- Initial ground-to-air networks

- Expeditionary giant voice
- Global Broadcast System (GBS)
- EC&I command and equipment accountability

11.3.2.3. Force Providers:

- Combat communications units
- EC&I forces embedded in other functional areas

11.3.2.4. Summary: An EC&I activation unit typically arrives in this FM to begin building the “permanent” EC&I infrastructure (including a satellite link to the Global Information Grid, a Network Control Center, and organic power). EC&I activation forces in this module rapidly activate initial comm-info services (e.g. dial-up and dedicated C2 satellite, radio, and public address systems; unclassified and classified data and voice networks, and client support administration), initially at a single location, and then expanding to up to three additional locations. C2 FM forces are critical to enabling the AEW to assume C2 of the airbase from Open-the-Airbase FM forces. EC&I forces embedded in staff elements also arrive to perform operations in C2 facilities.

11.3.3. Establish-the-Airbase Force Module:

11.3.3.1. Warfighter Requirement: This module contains limited forces to bring the base to an initial operating capability.

11.3.3.2. Communication Capability: Currently fielded equipment provides the following capabilities:

- Base infrastructure expansion:
 - 280 Voice Lines
 - 256 NIPR/SIPR
- Deployable Air Traffic Control and Landing Systems (DATCALS)
- Fully-Capable Network Control Center (messaging, network services, application services, configuration management, help desk)
- Communication Security account crew
- Multimedia documentation
- EI Systems Telecommunications Engineering Manager

11.3.3.3. Force Providers:

- Combat communications
- Wing communications units
- EI units

11.3.3.4. Summary: DATCALS forces in this module activate systems and provide procedures for terminal air traffic control and precision and non-precision instrument approach for assigned and transitioning aircraft. EC&I robbing units fall in on activation units to continue

the expansion of the EC&I infrastructure to support a total population of about 1,200. These EC&I forces also provide initial multimedia still and video documentation services, plus additional client support administration services for base customers. Engineering Installation units provide capability to analyze emerging requirements and begin engineering the transition of the AEW into a CITS-like infrastructure.

11.3.4. Generate-the-Mission Force Module:

11.3.4.1. Warfighter Requirement: This module contains the capabilities to establish the aviation and direct aviation support packages necessary to achieve desired military effects as requested by the combatant commander.

11.3.4.2. Communication Capability:

- Extend EC&I infrastructure to functional users
- EC&I support required for particular mission areas to generate military effects

11.3.4.3. Force Providers:

- Wing communications units
- Embedded EC&I forces
- Combat communication units as required for special missions

11.3.4.4. Summary: EC&I forces assigned to aviation units and supporting communications units arrive to provide the EC&I services necessary to integrate the supported aviation package(s) into the EC&I infrastructure (e.g., organic client support administrators, “First 400 Foot” EC&I packages, weapons system video technicians, or “Reach Forward” EC&I elements may provide required EC&I capabilities). These EC&I forces are typically dependent on the host unit for movement of equipment, workspace, refueling, feeding, force production, billeting, and other support. However, “Reach Forward” EC&I forces may be significantly more self-sufficient.

11.3.5. Operate-the-Airbase Force Module:

11.3.5.1. Warfighter Requirement: This module contains the mission support forces needed to achieve a light and lean full operating capability.

11.3.5.2. Communication Capability: Currently fielded equipment provides the following capabilities:

- Base infrastructure expansion (based on currently fielded equipment):
 - 12 DSN Trunks

- 480 Voice Lines
- Expanded LMR Infrastructure
- 530 NIPR/SIPR
- Post Office establishment
- Robust information assurance operations aligned with the DoD IA Strategic Goals: Protect Information; Defend Systems and Networks; Provide Integrated Situational Awareness.
- Robust communications focal point capability

11.3.5.3. Force Providers:

- Wing communications units
- Combat communication units as required for special missions.
- Air postal units.

11.3.5.4. Summary: Wing or combat communications units and/or air postal squadron UTCs arrive to round out the EC&I infrastructure and client service administration to support approximately 3,000 to 3,500 people, as well as activate postal and base-wide administrative services. As operations begin to normalize, EC&I efforts begin to focus more on customer support than EC&I infrastructure expansion. As a result, EC&I robusting and sustaining units can begin to assume primary responsibility during this force module as these personnel have both the skills required to operate the tactical equipment and provide customer service functions as performed at home station

11.3.6. **Robust-the-Airbase Force Module:**

11.3.6.1. Warfighter Requirement: This module contains the capabilities required to equip the airbase for indefinite operation and mitigate risks maintained by keeping earlier force modules “light and lean.”

11.3.6.2. Communication Capability:

- Robust NCC function (Help Desk, Config Mgt, Network Services, Computer Network Defense)
- Expand SATCOM Services: increase bandwidth, assured connectivity
- EI forces transition base to fixed-like infrastructure
- Robust Multimedia Functions
- Client support for offices throughout the AEW
- EI TII forces begin engineering transition to fixed-like base

11.3.6.3. Force Providers:

- Wing communications units
- Combat Communications forces
- Engineering and Installation forces
- Postal units
- Contractor employees

11.3.6.4. Summary: This force module serves to round out the objective wing structure. EC&I forces in this module include EC&I systems to provide redundancy for critical communications connectivity, round out the expeditionary communications unit's maintenance, planning, and client support administration capabilities, and complete multimedia capabilities. During this period, the AFFOR and supporting MAJCOM should be looking for ways to make the EC&I infrastructure permanent and/or reduce reliance on tactical equipment. They should also plan to relieve deployable equipment and people so they can return to home station and reconstitute their wartime capabilities so they are prepared to support the next contingency. Options the AFFOR and supporting MAJCOM may consider include using EI teams to install more permanent capabilities or contracting out EC&I forces and services

11.3.7. Rotational Sustainment Forces:

11.3.7.1. Due to skill-set differences, forces required to sustain EC&I infrastructure and services often differ significantly from those required to activate the infrastructure and services. Sufficient EC&I sustainment forces must be postured to sustain AEWs throughout the Air Expeditionary Force (AEF) cycle, permitting rotational sustainment of the EC&I force while allowing redeployment and resetting of EC&I activation and robusting forces.

11.3.7.2. Many sustainment forces will be deployed under UTCs that differ from those originally tasked under the AETF Open, C2, Establish, and Operate FMs. UTCs deployed during these FMs typically include equipment, as well as personnel practiced in their deployment and setup. Sustainment UTCs may be personnel-only, and should be more attuned to operating and maintaining systems in the demanding environment of a growing base.

11.3.7.3. With the exception of short-term deployments, personnel should expect to leave equipment in-place when redeployed. As forces that activated the base are redeployed, the supporting command must begin to reconstitute the forces to ensure they are prepared for the next contingency.

11.3.7.4. Force Providers:

- Wing communications units
- Combat Communications forces
- Engineering and Installation forces
- Postal units
- Above Wing-level organizations
- Contractor employees

11.3.8. Close-the-Air base Force Module:

11.3.8.1. As operations scale down at a deployed location, EC&I forces will scale back also. In many ways it will be a reverse of the base establishment and build up as operational units redeploy, equipment and material must be gathered, prepared for shipping, and sent out in accordance with COMAFFOR and MAJCOM disposition instructions. EI forces may be required to remove and prepare fixed communications infrastructure for shipment. As functional units redeploy and the base population continues to shrink, the EC&I infrastructure will be reduced, and EC&I personnel will also begin to redeploy. Basic EC&I services, such as unclassified and classified computer network connectivity and telephone support will continue until no longer required, when the infrastructure needed for these services will be packed and shipped as well. EC&I forces and services at final closure will consist of man-portable communications assets, such as a communications fly-away kit (6KTEA), plus a visual documentation team.

11.3.8.2. Force Providers:

- Wing communications units
- Combat Communications forces
- Engineering and Installation forces
- Postal units
- Contractor employees

12. COMMAND RELATIONSHIPS

12.1. The deployed C2 structure will be consistent with OPLANs and other applicable guidance defining deployed C2 relationships. Command relationships must be established and defined early in the development of any contingency, as they are essential to ensuring all parties fully understand their roles in the contingency effort.

12.2. Joint and Combined Task Forces Support -- The J-6 is responsible for satisfying theater-level communications and information requirements of the Joint Task Force (JTF) headquarters and all deployed forces. At the Combatant Command/JTF level, the J-6 normally establishes a Joint Communications Control Center (JCCC) to manage combined or joint in-theater communications assets. Operational control (OPCON) of all in-theater military communications and information systems and organizations resides with the J-6 unless delegated to a lower level by the Joint Force Commander. The J-6 delegates Tactical Control (TACON) to the lowest level of command necessary to accomplish the operational mission.

12.3. AFFOR Component Support -- The A-6 is responsible for establishing communications and information systems connectivity to support air component requirements throughout the theater. Additionally, the A-6 is responsible for satisfying component-level communications and information requirements of the Air and Space Operations Center (AOC). The A-6 normally establishes a Network Operations and

Security Center (NOSC) at the AFFOR (or a reach-back location) to manage and control the AF portion of the theater networks. In addition, the A-6 exercises tactical control (TACON) over assigned and augmenting component communications and information assets as delegated by Commander, AF Forces (COMAFFOR).

- 12.4.** Aerospace Expeditionary Wing (AEW) Support -- The AEW commander designates an AEW/A6 [A6?] to assume responsibility for all matters regarding employment, sustainment, and redeployment of communications and information assets in support of the AEW's mission. The AEW/SC normally establishes a Network Control Center-Deployed (NCC-D) as the focal point for management and problem resolution for site communications and information systems.
- 12.5.** Command Relationships for Gained Forces -- Communications and Information forces deployed from an Air Force Reserve Command (AFRC) or Air National Guard (ANG) unit in support of contingency operations are under TACON of the AEW/SC, with the exception of air traffic control which will be transferred to the operations group, if established. This subordinate relationship holds true regardless of rank or whether these forces deploy as units, in work centers, or as individuals. The A6 or AEW/SC exercises TACON over assigned augmenting force personnel. Gained forces activated in support of contingencies are under OPCON of the gaining theater commander. In cases short of mobilization, ADCON of Air Force Reserve Command or Air National Guard forces remains with the unit's non-mobilized authority (AFRC/CC for reservists and the 201 MSS/CC for ANG members)
 - 12.5.1.

13. SUMMARY

- 13.1.** This Enabling Concept provides the foundation upon which to build and deploy EC&I forces and capabilities. EC&I units must continue to display an expeditionary mindset, and be ready to deploy quickly and effectively to support operational missions. Although specific EC&I services provided and forces employed may differ based on specific MAJCOM missions, the basic EC&I premises remain the same. EC&I forces must be able to operate in varying operational (permissive to semi-permissive) and C2 environments (AF, joint, and/or combined). EC&I forces plan to deploy as depicted in the AETF FMs. EC&I activation units respond rapidly but phase in capability in a modular, scalable fashion based on requirements, available bandwidth, and available airlift. Robusting forces fall in on activation forces to expand EC&I capabilities, and sustainment forces activate and maintain specialized EC&I services as well as relieve activation and robusting forces during AEF rotations. EC&I forces also provide theater level and first 400 feet capabilities.
- 13.2.** The AFFOR and host MAJCOM should plan to replace EC&I forces and equipment with more permanent military or commercialized capabilities. Finally, as forces redeploy, communications planners should reduce sustainment requirements by incrementally releasing assets no longer required to support the mission.
- 13.3.** AFNETOPS implementation will provide some manpower efficiencies to the AF but must overcome several challenges before it can fully support expeditionary operations and reduce EC&I sustainment requirements. EC&I forces will continue to activate and

robust network services at expeditionary locations even after AFNETOPS implementation.

//signed//

MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

APPENDIX A: EQUIPMENT COVERED BY THE 'TDC' PROGRAM

The TDC Program is run by ESC with ACC as the Lead Command. TDC suites provide access to secure and non-secure data networks (Secret Internet Protocol Router Network (SIPRNET) and Non-Secure Internet Protocol Router Network (NIPRNET), Joint Worldwide Intelligence Communications System (JWICS)), video teleconferencing (VTC), C2 Radio Support, switched telephone network and messaging services. TDC services will connect to the Defense Information Infrastructure and provide Wide Area Network (WAN) transmission connectivity through multiband (X, C, Ku) super high frequency (SHF) satellite radio.

Basic Access Module	Circuit Extension Kit
Cellular Hub Module	PMUX 400 Configuration Kit-Port Interface
Large Voice Module	PMUX 400 Configuration Kit-Trunk Interface
Remote Base Transceiver Module	PMUX 400 Configuration Kit-Voice
Secure Voice Module	PMUX 800 Configuration Kit-Port Interface
STE-R Module	PMUX 800 Configuration Kit-Trunk Interface
Cellular Antenna Kit	PMUX 800 Configuration Kit-Voice
Cell Phone Kit	Transmission Modules and Kits
Cell O&M Center Kit	Laser Module
Cell TRX Card and Power Amplifier Kit	RF Microwave Module
DSVT Kit	Antenna Mast Kit
Echo Cancellation Kit	RF Microwave Antenna Kit
Lightning Protection Kit	Tripod Kit
Voice Configuration Kit-International	Multi-Purpose Modules and Kits
Voice Configuration Kit-Local Base Interface	ICE NIPRNET Module
Voice Configuration Kit-Radio Interface	ICE SIPRNET Module
Voice Configuration Kit-Subscriber Extension	ICE Transmission Module
Voice Configuration Kit-Subscriber Loop	SPICE Baseband Module
Voice Configuration Kit-T1 Trunk	SPICE NIPRNET Module
Voice Configuration Kit-TRI-TAC Interface	SPICE SIPRNET Module
Data Modules and Kits	System Kits
Crypto Interface Module	Cable Maintenance Kit
Red Data Module	Cable, Data and Phone
TSSR Interface Unit	Cable, FO
Crypto Configuration Kit	Fireberd Kit
INE Kit	Laptop Computer Kit
LAN Kit	Large UPS Kit
Router Kit	Material Handling Equipment
VOIP Kit	Printer Kit
Muxing Modules and Kits	Remote Frames Kit
Crypto Module	Small UPS Kit
FCC-100 (Satellite) Module	Telephone Kit
FCC-100 (Tactical) Module	Video over IP Kit
FTSAT Baseband Module	STEs
PMux 400 Module	NCC-D
Pmux 800 Base Module	NCC-D Heavy Module
Pmux 800 Expansion Module	NCC-D Light Kit

APPENDIX B: DESCRIPTION OF EC&I FORCES

AFFOR Component Support. The WFHQ A6 is a staff function and as such does not include the organic communications equipment or personnel to support the WFHQ, to include the AOC. AFFOR staff and AOC communications requirements are satisfied by the Headquarters Support Group/Squadron and host communications activity. Local and outside communications augmentation personnel may provide additional WFHQ communications support functions. The WFHQ A6 represents the WFHQ on communications matters to COCOM / JCS / MAJCOM / HQ USAF and other agencies/organizations, while maintaining authority over functional reporting, and the deployment and maintenance of systems and associated infrastructure; thus ensuring there are cohesive and clear lines of component authority over AFFOR network systems. The A6 staff is responsible for all theater communications planning, monitoring, and reporting across the full range of military operations. This includes the capability to plan, integrate, and control WFHQ directed activities to deploy, maintain, sustain and employ communications in support of contingency operations while representing the WFHQ on C4 integration matters with other staffs, COCOM, and other outside agencies. The AFFOR is manned for a nominal level of effort in its Area of Responsibility. For higher levels of conflict, the AFFOR will require augmentation to provide required services to supporting forces. The A6 also establishes an EI Cell to organize, administer, and control EI forces in the theater. In addition, the A6 exercises tactical control (TACON) over assigned and augmenting component C&I assets as delegated by the Commander, Air Force Forces (COMAFFOR).

Command & Control. The J6 is responsible for satisfying theater-level C&I requirements of the Joint Task Force (JTF) headquarters and all deployed forces. At the Combatant Command/JTF level, the J6 normally establishes a Joint Communications Control Center (JCCC) to manage combined or joint in-theater communications assets. Operational control (OPCON) of all in-theater military C&I systems and organizations resides with the J6 unless delegated to a lower level by the Joint Force Commander. The J6 delegates Tactical Control (TACON) to the lowest level of command necessary to accomplish the operational mission.

Engineering Installation (EI). Engineering and Installation units provide the capability to transition to permanent infrastructure and additional engineering expertise not resident in other deployable communications units. EI units can design, engineer, and install the full range of C&I equipment and components typically found at a fixed site and other specialty systems unique to expeditionary forces (Unmanned Aerial Vehicle (UAV) and Combined Aerospace Operations Center (CAOC) support, etc.). EI units typically follow “first-in” units and lead the effort to convert from tactical to fixed equipment. They provide specialized Air Traffic Control and Landing Systems (ATCALs) and weather system expertise and are knowledgeable in both tactical and fixed systems. Additionally, EI units may be tasked to “prepare the communications battlespace” by pre-wiring future operating locations with infrastructure to quickly accept forces and expeditionary communications equipment. They may also be tasked to repair and restore service for base communications systems damaged by enemy, friendly, or natural forces. EI units, when tasked and deployed, are AFFOR assets and work directly for the AFFOR/A6. They DO NOT provide day-to-day operations and maintenance support for engineered and installed systems.

Engineering and Installation units provide

- a. Specialized ATCALs/weather system support or commercialization
- b. Robusting base communications and conversion from tactical to fixed base infrastructure

- c. Follow-on long-term communications assessment, planning, engineering, and installation
- d. Preparation of the communications battle space by pre-wiring future operating locations with infrastructure to quickly accept forces and expeditionary communications equipment
- e. Repair and restore service for base communications systems damaged by enemy, friendly, or natural forces

Spectrum Management. The spectrum manager acts as the focal point for control of the frequency spectrum resource in the theater of operations. Essential spectrum management responsibilities include resource allocation (frequency assignments, Joint Communications-Electronics Operations Instructions (JCEOI) publication), prioritization, and spectrum resource guidance, including those required for ATC systems. Planners must provide the frequency manager with frequency requirements as soon as they are known. Each base will need a block of frequencies for Long Haul communications, Land Mobile Radios, Air to Ground radios, and landing rights for commercial satellite terminals that are established when the base location is known. The Combatant Commander, as far in advance as possible, should work host nation approval for all frequencies.

AIR NATIONAL GUARD AND RESERVE

ANG and Air Force Reserve Command (AFRC) Communications Flights. ANG and AFRC deployable communications units provide all levels of deployable C&I support. AFRC deployable units provide activation, robusting, sustaining, theater-level, and first-400-foot forces, as well as deployed NOSC, NCC, and AETF FM augmentation UTCs. The ANG provides air traffic control systems support.

ANG Air Traffic Control Squadrons. There are ANG Air Traffic Control (ATC) organizations exclusive to the ANG, located around the country, where they perform day-to-day air traffic control operations while also training on and maintaining wartime weapon systems. This includes the AN/MPN-14K (mobile radar system), the AN/TRN-26 (mobile TACAN), and the AN/MSN-7 (mobile control tower). These ATC Squadrons are capable of deploying a full scope of ATC capabilities to support any contingency.

ANG Combat Communications Units. Provide tactical engineering support, man-portable communications kits to support ADVON, initial reception of forces and reach forward deployment of key personnel. They are able to deployed base information infrastructure across the full spectrum of operations and provide connectivity for the base infrastructure to the theater information infrastructure. Additionally they provide power and environmental control and immediate commercial, national, and tactical imagery data support.

COMBAT COMMUNICATIONS UNITS

Combat Communications Units. Combat communicators are capable of immediate response (within 24 hours of tasking) in support of air and space operations. Combat communications units provide a broad range of communications capability (voice, data, video, network services, Deployable Air Traffic Control and Landing Systems (DATCALs) and weather services) and have more substantial combat training (air base ground defense and convoy training) than wing-level communications units. They are capable of providing initial communications packages and can build up services to a theater or strategic level. The focus on providing “first in” communications for combat communicators allows these units to practice the mission essential tasks required to perform this function in a semi-permissive environment. This flexibility allows

combat communications units to provide immediate support to expeditionary operations without disruption of in-garrison operations/missions. ANG Combat Communications Group Headquarters also provides a MAJCOM/NAF support element (6KMM9) that is tailored for each customer to support AFFOR/A6, Crisis Action Team (CAT), and other similar contingency support activities.

Combat Communications units are also capable of sustaining deployed air bases with voice, data, weather and air traffic control services. However, the priority for these units remains the "enabler" mission. Combat communications units are specifically designed, equipped and manned for the "first in" or initial response role. The use of these organizations to provide long periods of base sustainment may impact overall readiness and the units' ability to accomplish their primary mission. Their taskings must be managed carefully to balance experience in an operational environment with readiness to support short-notice contingency operations.

Combat communications units provide a well-trained force of C&I professionals capable of establishing and/or sustaining services in austere environments encountered in modern Joint expeditionary operations. These units can operate with minimal support and under permissive and semi-permissive conditions. Combat communications units are better equipped and trained for conducting air base ground defense, convoy operations, identifying unexploded ordnance, carrying out activities in black-out conditions while wearing nuclear, biological, chemical (NBC) protective gear, working in extremely austere and remote environments, and in some cases providing their own limited base operating support (BOS).

EMBEDDED COMMUNICATORS

Approximately 25% of postured communications AFSCs are embedded in non-communications UTCs. These forces must be included when considering the total expeditionary communications "foot print." Examples include:

- Air Control, AOC
- Wing Staff
- A/C Maintenance
- Intel
- Aviation UTCs
- AFFOR/JTF Support
- CRE, Aerial Port
- Ops Support
- RED HORSE
- Space support
- Medical
- Info Operations
- Public Affairs
- Security Forces

These forces provide services, such as:

- Initial site assessment (CRGs)
- Establishment of initial site communications for internal users (All)
- Support for C2 communications (All)
- Rapid deployment of tactical air control radar equipment (ACS)

- Air Operations Center support (ACOMS)
- Secure and non-secure voice and data services for internal users (All)
- Ground-to-air radio (All)
- Specialized support to Army ground units (ASOS)
- Direct support to Tactical Air Control Parties (TACPs) (ASOS)

Contingency Response Groups (CRGs). Contingency Response Groups provide a myriad of tailored, stand-alone airbase opening capability to the Joint Task Force or Combatant Commander. These include units such as CRGs in PACAF, USAFE, AMC, and the 820th Security Forces Group in ACC. Specific details of the CRG employment can be found in the Air Force Contingency Response Group Operational Concept. The core capability of the CRG as defined by the CRG Enabling Concept includes the airbase-opening capability and ensures consistency throughout the Air Force. Other deployable communications units (i.e., combat communications) can follow-on to replace or robust the inherent CRG deployable communications capabilities. Operational requirements may dictate the CRG receive augmentation forces and the CCGs need to be ready to provide that augmentation, as required.

Air Support Operations Squadrons (ASOS). ASOS provide direct support to Army units and Army ground commanders. ASOS missions range from that of an Air Support Operations Center (ASOC) to several variants of TACP units. ASOCs and TACPs are supported by ACC/A3YC and when deployed fall under the theater A3. Specifically, these units integrate joint airpower and advanced weather technology in support of Army close air support requirements. ASOS units assigned UTCs 7FVQA and 7FVQB deploy with tasked Air Support Operation Group (ASOG) staff to form the ASOC. As a subordinate element of the AOC, the ASOC is the principle command and control (C2) node in the close ground battle. It is the senior United States Air Force (USAF) liaison element to the Army or allied ground maneuver units. The ASOC, and its subordinate TACP UTCs with joint terminal attack controllers (JTACs), are the farthest extension of combined/joint force air component commander (C/JFACC) authority for executing air and space power on the battlefield. While the ASOS units have very good ground-to-air radio capability, they possess limited "first in" reach back capabilities in support of its wartime mission and specialty customers. These units are extremely adept in integrating and interoperating with Army communications systems.

The ASOS does not provide common user or expeditionary base deployable communications. TACP units possess ground-to-air communications capabilities in support of its wartime mission but do not provide common user or expeditionary base deployable communications.

Joint Communications Support Squadrons (JCSS). Two ANG communications units have been tasked, trained and equipped to provide support to the Joint Communications Support Element (JCSE). The mission of these two units is to provide communications support for a Joint Task Force (JTF) or a Joint Special Operations Task Force (JSOTF), provide the Chairman of the Joint Chiefs of Staff direct communications support of Unified Commands, Services, Defense Agencies and non-Defense Agencies as well as direct communications support to foreign governments.

Air Control Squadrons (ACS). Air Control Squadrons provide radar surveillance, control of sector air defenses, and collection and transmission of radar data to support development of the common air picture. Air Control Squadrons are supported by ACC/A3YG and when deployed fall under the theater A3. The ACS possesses substantial reach back capabilities via military

satellite communications terminals. ACS units also have inherent secure and non-secure voice and data capabilities; however, they do not support common user or expeditionary base deployable communications.

Air Communications Squadrons (ACOMS). Warfighting Headquarters (WFHQ) are the senior operational Air Force presence supporting a combatant commander. Each WFHQ consists of an in-place Commander, Air Force Forces (COMAFFOR) and an in-place AOC. Currently, ACOMS provide the AFFOR/A6 and staff, and AOC systems and communications support. The WFHQ also includes a Support Group to provide "inside-the-tent" services for the WFHQ. ACOMS capabilities embedded in the WFHQ Support Group include the ability to rapidly deploy one or more Air Component Coordination Elements (ACCE) to liaise with JTF-Headquarters active in the WFHQs AOR. Additionally, some ACOMS provide Network Operations and Security Center (NOSC) services for their AOR (if not already established) and reach back capability for ACCEs or other forces deployed to their AOR. Host communications unit will provide the "outside-the-tent" capabilities and services for WFHQ.

Air Mobility Operations Squadrons (AMOS). Provides dedicated EC&I support to the Air Mobility Director when not collocated with an AOC (e.g., mobility centric AOC).

WING COMMUNICATIONS SQUADRONS

Wing Communications Squadrons. In addition to operating and maintaining their home base garrison infrastructure, wing communications units primarily provide multimedia, administrative communications, and rotational sustainment forces. USAFE, PACAF, and some ACC units provide postal capabilities. Selected CAF and MAF wing communications squadrons may be TDC-equipped to provide EC&I activation or robbing forces to meet the Air Force's total AETF FM requirement.

Air Postal

Operates air post offices, aerial mail terminals, postal service centers, military locator facilities, and provides postal finance services overseas. Provides reciprocal support to Army, Navy, and Allied Forces as required and other U.S. government agencies.

Computer Systems Squadrons

Provides computer software and programming services as applicable.

APPENDIX C: REFERENCES AND SUPPORTING INFORMATION

- Joint Pub 6-0, Doctrine for C4 Systems Support to Joint Operations, 30 May 1995
- Joint Pub 6-02, Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications and Computer Systems, 1 Oct 1996
- Air Force CONOP 2020
- Air Force Policy Directive 10-28, Functional Concept Development, 8 Jan 2002
- Air Force Doctrine Document 2-2 Organization and Employment of Aerospace Power, 17 Feb 2000
- Air Force Doctrine Document 2-4.1 Force Protection, 29 Oct 1999
- Air Force Instruction 21-116, Maintenance Management of Communications-Electronics, 19 Apr 2005
- Air Force Instruction 10-401, Air Force Operations Planning and Execution, 4 May 2005
- Air Force Policy Directive 10-28, Air Force Concept Development, 15 Sep 2003
- Theater Deployable Communications (TDC) Operational Requirements Document (ORD), 6 Jan 1995. Available at Communications & Information Functional Area Managers CoP (<https://rso.my.af.mil/afknprod/ASPs/CoP/EntryCoP.asp?Filter=OO-SC-CA-07>)
- Air Force Master Capabilities Library Version 5.5, 15 Nov 04. Available from AF/A5XC-INT.
- Air Force Agile Combat Support Concept of Operations, 15 Jul 05.
- Air Force Airbase Opening Enabling Concept of Operations, May 06.
- Communications and Information Prioritization and Sequencing Guidance, 25 May 2005
- Concept of Operations for Air Force Network Operations, Nov 2004
- HQ Air Force Special Operations Command Deployed Communications Functional Concept, 11 Sep 2001
- HQ Air Mobility Command Functional Concept for Deployed Communications, 11 Jul 2001
- HQ Air Combat Command, Concept of Operations for Theater Deployable Communications (TDC), 30 Oct 1996
- HQ Air Combat Command, Expeditionary Aerospace Force Communications and Information Deployment Construct, Draft, 14 Sep 1999
- HQ Air Combat Command, Expeditionary Aerospace Force Operations Construct, 9 Nov 1998
- HQ Air Combat Command, Expeditionary Aerospace Force Deployment Construct
- 282d Combat Communications Squadron Visitors Information Guide, Mar 2002
- 3d Combat Communications Group Concept of Operations, Apr 2002
- National Military Strategy of the United States of America, 2004
- Draft Program Guidance Letter, Organization of Air Force Expeditionary Communications And Deployable Air Traffic Control And Landing Systems (DATCALs) Force Structure, Dec 2005

APPENDIX D: GLOSSARY

A

ACC	Air Combat Command
ACOMS	Air Communications Squadrons
ADCON	Administrative Control
ADVON	Advanced Echelon
AEF	Aerospace Expeditionary Force
AEFC	AEF Center
AETF	Air and Space Expeditionary Task Force
AEW	Air Expeditionary Wing
AF	Air Force
AFETS	Air Force Engineering and Technical Services
AFFOR	Air Force Forces
AFNETOPS	Air Force Network Operations
AFRC	Air Force Reserve Command
AFSOC	Air Force Special Operations Command
AMC	Air Mobility Command
AMD	Air Mobility Division
AMOG	Air Mobility Operations Group
AMOS	Air Mobility Operations Squadron
ANG	Air National Guard
AOC	Air and Space Operations Center
AOR	Area of Responsibility
ARC	Air Reserve Component
ASR	Airport Surveillance Radar
ATC	Air Traffic Control
ATCALs	Air Traffic and Control Landing Systems
ATO	Air Tasking Order

AWACS	Airborne Warning and Control System
B	
BII	Base Information Infrastructure
BITS	Base Information Transfer System
BOS	Base Operating Support
C	
C&I	Communications and Information
C2	Command and Control
C3	Command, Control, and Communications
C4	Command, Control, Communications, Computers
CAF	Combat Air Forces
CAS	Close Air Support
CAT	Crisis Action Team
CE	Civil Engineering
COMAFFOR	Commander, AF Forces,
CONUS	Continental United States
COTS	Commercial off the Shelf
CSAR	Combat Search and Rescue
D	
DAMA	Demand Assigned Multiple Access
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMS	Defense Message System
DOC	Designed Operational Capability
DOD	Department of Defense
DSCS	Defense Satellite Communications System
DSN	Defense Switched Network
E	
EAJ	Expeditionary Aerospace Force
ECU	Environmental Control Unit
EI	Engineering Installation

G

GBS	Global Broadcast Service
GMT	Ground Multiband Terminal
GMTF	Global Mobility Task Force
GMTFCE	Global Mobility Task Force Communications Element
GMTFSS	Global Mobility Task Force Support Structure

H

HF	High Frequency
HMMWV	High Mobility Multipurpose Wheeled Vehicle

I

IA	Information Assurance
ICAP	Initial Communications Access Package
ICE	Initial Communications Element
IFR	Instrument Flight Rules
IM	Information Management
INMARSAT	International Maritime Satellite
IP	Internet Protocol

J

JCCC	Joint Communications Control Center
JCEOI	Joint Communications-Electronics Operations Instructions
JFACC	Joint Forces Air Component Commander
JSOAC	Joint Special Operations
JSTARS	Joint Surveillance Target Attack Radar System
JTF	Joint Task Force
JWICS	Joint Worldwide Intelligence Communications System

L

LDR	Low Data Rate
LMR	Land Mobile Radio
LMST	Lightweight Multiband Satellite Terminal
LPI/LPD	Low Probability of Intercept and Detect
LRU	Line Replaceable Units

M

MACS	Mobile Air Traffic Control System
MAF	Mobility Air Forces
MAJCOM	Major Command
MDR	Medium Data Rate
MICK	Mobile Initial Communications Kits
MMLS	Mobile Microwave Landing System
MOB	Main Operating Base
MRSP	Mission Readiness Spares Packages
MSS	Mobile Subscriber Systems
MTW	Major Theater War

N

NCC	Network Control Center
NCC-D	Network Control Center-Deployed
NIPRNET	Non-Secure Internet Protocol Router Network
NOSC	Network Operations and Security Center

O

OEF	Operation Enduring Freedom
OOTW	Operations Other Than War
OPCON	Operational Control
OPLAN	Operations Plan
OPS	Operations Subsystem
ORE	Operational Readiness Exercise
ORI	Operational Readiness Inspection

P

PAR	Precision Approach Radar
-----	--------------------------

R

RSP	Readiness Spares Packages
-----	---------------------------

S

SATCOM	Satellite Communications
SDB	SATCOM Data Base

SDI	Special Duty Identifier
SHF	Super High Frequency
SIPRNET	SECRET Internet Protocol Router Network
SOF	Special Operations Forces
SOG	Special Operations Group
SOLE	Special Operations Liaison Element
SORTS	Status of Resource and Training System
SOW	Special Operations Wing
SPINS	Special Instructions
STE	Secure Terminal Equipment
STEM	Systems Telecommunications Engineering Manager
STEP	Standardized Tactical Entry Points
STU	Secure Telephone Unit
T	
TACANs	Tactical Air Navigation Aids
TACON	Tactical Control
TALCE	Tanker Air Lift Control Element
TBMCS	Theater Battle Management Core System
TCNO	Time Compliance Network Orders
TDC	Theater Deployable Communications
TERPS	Terminal Instrument Procedures
TIG	Theater Information Grid
TII	Theater Information Infrastructure
TMSS	Transportable Mission Support Systems
TRI-TAC	Tri-Service Tactical
TTPs	Tactics, Techniques, and Procedures
U	
UHF	Ultra High Frequency
UTC	Unit Type Code
V	
VFR	Visual Flight Rules

VI	Visual Information
VISC	Visual Information Support Center
VTC	Video Teleconferencing
W	
WAN	Wide Area Network
WGM	Workgroup Manager
WMP	War and Mobilization Plan

XXV. Appendix 5, Cyberspace Professional Roadmap

Appendix 5, *Cyberspace Professional Roadmap*, provides clear direction for the development of cyberspace forces. It is derived from the Air Force Roadmap for the Development of Air Force Cyberspace Professionals, which establishes a way ahead for the next 10 years. The roadmap provides specific guidance essential to successfully develop new Cyberspace Airmen. It also allows for flexibility, as we develop and better understand the operations and capabilities required to establish, control, and leverage the cyberspace domain. This roadmap considers the challenges presented by the cyberspace domain and charts the developmental path required to produce the Air Force's Cyberspace Professionals. It formalizes the bridge between strategy and reality, establishing the appropriate sequencing of events and timelines to achieve success.

**The Air Force Roadmap
for the
Development of
Cyberspace Professionals
2008 - 2018**



U.S. AIR FORCE

15 APR 2008

OPR: AF/A30-CF

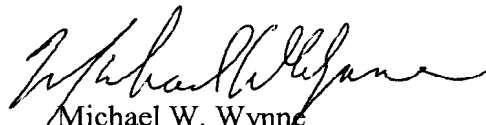
This Page Intentionally Left Blank

Executive Summary

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. With the recognition of cyberspace as a new domain comes the pressing need to develop cyberspace capabilities that extend the Air Force’s global vigilance, reach, and power into the domain of the electromagnetic spectrum and networked electronics. For the Air Force, cyberspace is now a warfighting domain on par with air, space, land, and sea. The cyberspace domain, like the air and space domains, demands a professional cadre of Cyberspace Airmen and the means to purposefully develop these Airmen as the warriors, leaders, advocates, and visionaries of tomorrow. This roadmap will guide our efforts toward this end and establish key milestones that we must reach in an expeditious fashion.

Successful cyberspace operations will ensure cross-domain freedom of action for our friends and allies, and deny that same freedom to our adversaries. Since our potential adversaries have declared their intent to challenge us in the cyberspace domain, the Air Force must ensure it can establish and maintain cyberspace superiority anywhere the nation requires the use of military force. Effective development of cyberspace capabilities encompass much more than the technology required to connect entities across the battlespace. We must aggressively dedicate appropriate resources to further develop the intellectual and technical prowess that is a hallmark of today’s Airmen. We must implement a force development approach that will give the Air Force a distinct advantage over any potential adversary in the cyberspace domain, just as it has in air and space. Harnessing this prowess dictates we retool our education and training programs to encompass cyberspace fundamentals. These fundamentals are identified in this roadmap and are essential to developing our new officer and enlisted cyberspace career fields.

In the past century, we have encountered and mastered new challenges in air and space. Cyberspace will be no different. The imperative is clear – we must establish, control and leverage the cyberspace domain. This roadmap will unambiguously establish the path required to develop Cyberspace Professionals – officers, enlisted, and civilians – and allow for flexibility as our understanding of the new cyberspace domain continues to mature. The roadmap establishes end states and charts a well-defined course to ensure our efforts remain focused on the force development required to address the cyberspace imperative. This roadmap is the keystone document that will shape how we develop our new breed of Airmen to “fly and fight” in cyberspace.



Michael W. Wynn
Secretary of the Air Force

Table of Contents

1.0 Introduction..... 1
 1.1 Purpose..... 1
 1.2 Background..... 2
2.0 Air Force Cyberspace Operations..... 2
 2.1 Cyberspace Operations 3
 2.2 Cyberspace Cross-domain Operations..... 3
 2.3 Cyberspace Combat Sustainment Operations..... 4
 2.4 Intelligence, Surveillance, and Reconnaissance Operations (ISR)..... 4
3.0 Air Force Cyberspace Forces..... 4
 3.1 Air Force Cyberspace Forces: Core Competencies 5
 3.2 Air Force Cyberspace Enabling Competencies 6
4.0 Air Force Cyberspace Career Fields: Force Development Foundations 7
 4.1 Roles 8
 4.2 Force Development – Cyberspace Operators and Specialists..... 9
5.0 Air Force Cyberspace Career Fields: Training and Education Concept..... 14
6.0 Air Force Cyberspace Career Fields: Challenges 15
 6.1 Cultural 15
 6.2 Organizational..... 16
 6.3 Fiscal..... 16
7.0 Air Force Cyberspace Career Fields: Milestones and Implementation 16
8.0 Summary 19
Appendix A: References..... 21
Appendix B: Enlisted Cyberspace AFSC Construct..... 22
Appendix C: Officer Cyberspace AFSC Construct 26
Appendix D: Cyberspace Training and Education Construct..... 29

Figures

Figure 1: Enlisted Cyberspace Force Development Construct..... 11
Figure 2: Officer Cyberspace Force Development Construct..... 12
Figure 3: Cyberspace Force Education & Training 13
Figure 4: Major Cyberspace Professional Roadmap Milestones..... 19

1.0 Introduction

The idea of freedom of cyberspace may, in time, be the same kind of principle as freedom of the seas and freedom of the skies. This means that cyberspace is a domain in which many rely, and in which warfighting can and by some definitions already takes place.

My duty as the Secretary of the Air Force is to put the nation's most technologically capable force on a path to do our share of the task of presenting to our Combatant Commanders, and so to the President and the Nation, the trained and ready forces they may need to ensure the same security and Freedom of Cyberspace that Americans and indeed many in the world already enjoy in the Oceans, in the Air, and also in Space.

Good stewardship means attending to the systematic training, organizing, and equipping that is our job. This includes especially attending to the career progression of the Airmen involved in Cyberspace, including our guard, reserve, and civilian professionals.

*Michael W. Wynne
Secretary of the Air Force
Remarks to C4ISR Integration Conference, 2 Nov 06*

1.1 Purpose

Developing Air Force cyberspace capabilities is a strategic imperative for protecting and preserving the sovereignty of the United States. The development of the United States Airman's ability to establish, control and leverage the cyberspace domain is the bedrock which supports the presentation of cyberspace capabilities in support of our national interests. This roadmap considers the challenges presented by the cyberspace domain and serves to chart the developmental path required to produce our Cyberspace Professionals. It also formalizes the bridge between strategy and reality, establishing the appropriate sequencing of events and timelines to achieve success.

The Air Force Roadmap for the Development of Air Force Cyberspace Professionals provides a clear vector for the development of cyberspace forces for the next 10 years and will drive the development of a corresponding Implementation Plan. The roadmap provides specific guidance essential to successfully develop new Cyberspace Airmen. It also allows for flexibility, as we develop and better understand the operations and capabilities required to establish, control and leverage the cyberspace domain.

1.2 Background

1.2.1 A Historical Perspective

During the past one hundred years, numerous technological advancements have re-shaped our warfare concepts. Our predecessors recognized the air domain's unique attributes necessitating a nationally focused effort to secure and dominate the environment. The 1950's advent of space as a new domain required the fielding of space-based capabilities to support national objectives. Each domain requires a professional corps skilled in the art and science required to secure it. Given the rapid pace of technological evolution, we cannot afford to develop our Cyberspace Airmen twenty years after we've recognized the national capabilities afforded to us via cyberspace – we must develop the Cyberspace Professional now.

1.2.2 A National Perspective

The 2006 *Quadrennial Defense Review* highlighted the increasingly critical and inseparable aspect of cyberspace from our national power and interests. Additionally, the United States' *National Strategy to Secure Cyberspace* lists three strategic objectives:

- 1) Prevent cyberspace attacks against America's critical infrastructures;
- 2) Reduce national vulnerability to cyberspace attacks; and
- 3) Minimize damage and recovery time from cyberspace attacks that do occur.

The 2006 *National Military Strategy for Cyberspace Operations (NMS-CO)*¹ further identifies the achievement of strategic military superiority in cyberspace as the Department of Defense's strategic goal. The national strategy document characterized the cyberspace domain as a warfighting domain which favors the offense. For the purposes of this roadmap, we've adopted the following NMS-CO definition of the domain of cyberspace:

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.

2.0 Air Force Cyberspace Operations

In order to create effects in and through cyberspace, the Air Force must first enable combatant commanders to gain and maintain cyberspace superiority. In line with the national and military objectives, Air Force Cyberspace Command (Provisional) has identified the following objectives:

- Deter and prevent cyberspace attacks against vital US interests
- Prevent and rapidly respond to attacks and reconstitute cyberspace operations
- Integrate cyberspace power into the full range of global and theater effects
- Defeat adversaries operating through cyberspace

¹ *National Military Strategy for Cyberspace Operations, referenced document is classified SECRET/NOFORN*

- Freedom of action in cyberspace for US and Allied commanders
- Persistent cyberspace situational awareness

Drawing from a common language used throughout the Air Force we can characterize these operations as cyberspace operations (both offensive and defensive cyberspace operations), Cross Domain cyberspace operations and Cyberspace Combat Support Operations.

2.1 Cyberspace Operations

Counter cyber involves those operations conducted to ensure friendly freedom of action in cyberspace while denying it to adversaries when required. The main objectives of counter cyber operations are to allow friendly forces to exploit cyberspace, while negating the enemy's ability to do the same. They can be conducted by air, space, land, sea, cyberspace or special operations units. Counter cyber consists of offensive and defensive operations.

2.1.1 Offensive Cyberspace Operations

Offensive cyberspace operations (OCO) deny, degrade, disrupt, destroy, or deceive an adversary's cyberspace capability. Adversary cyberspace capabilities employ electronics, networks, and other systems that span the electromagnetic spectrum (EMS). OCO targets include adversary terrestrial, airborne, and space networks; electronic attack (EA), network attack (NetA), and directed energy attack systems; and, command, control, communication, computers, and intelligence (C4I) links and nodes.

2.1.2 Defensive Cyberspace Operations

The objective of defensive counter cyber (DCO) is to protect friendly forces and vital interests from adversary cyberspace attack. DCO consists of active and passive operations, including all defensive measures, designed to destroy attacking adversary forces or reduce their effectiveness. DCO includes measures to preserve, protect, recover, and reconstitute friendly cyberspace capabilities before, during, and after an adversary attack. DCO extend beyond electronic protection (EP) and network defense (NetD); DCO provides end-to-end *secured* service for both wired and wireless and both Internet Protocol (IP) and non IP-based connectivity, which includes terrestrial, airborne, and space-borne links/nets.

2.2 Cyberspace Cross-domain Operations

Cyberspace capabilities will be used to achieve effects in and across other domains. Cyberspace forces can disrupt communications, deny effective C2, or disable other lines of communication that rely on the use of cyberspace. This includes attacking adversary terrestrial, airborne, and space based communications, networks, and systems. Specifically, cyberspace forces can directly contribute to the achievement of air superiority by disrupting or destroying adversary integrated defenses or even networked air-to-air operations. Cyberspace capabilities can be used to achieve counterland objectives by interdicting adversary C2 links or by conducting close support with friendly ground or air forces to defeat ground attacks. Cyberspace forces will also support counterspace functions and help to achieve some degree of space control

by denying adversaries access to their satellite systems as well as ensuring continued access for coalition forces.

2.3 Cyberspace Combat Sustainment Operations

In order to conduct effective cyberspace combat operations, the Air Force must develop robust provisioning and sustainment operations. The near-term and emerging challenges will be developing the cyberspace infrastructure, systems, and forces to meet the current and evolving operational environment. The cyberspace infrastructure encompasses the entire range of capabilities that operate within or enable access to cyberspace. It includes communications networks, data management systems, software, hardware, facilities, ranges, tools, weapons, and sensors. In line with this vision of cyberspace warfare, the infrastructure will include secure and survivable capabilities that are adaptive to the rapidly changing and dynamic cyberspace environment. Like air and space power, cyberspace superiority enables speed, global reach, persistence, flexibility, and the ability to achieve tailored effects. Cyberspace warfare systems and databases must routinely update cyberspace weapon systems, mission planning systems, visualization modeling and simulation systems, and air and space operations center (AOC) planning and execution systems. Like DCO, cyberspace combat sustainment operations provides end-to-end assured service for both wired and wireless, which includes terrestrial, airborne, and space-borne links/nets.

2.4 Intelligence, Surveillance, and Reconnaissance Operations (ISR)

The cyberspace environment is highly dynamic and operations can easily render unexpected collateral effects. Timely collection, processing, analysis, production, and dissemination of reliable and accurate intelligence are critical to successful cyberspace operations. ISR professionals must develop an extensive understanding of the cyberspace domain and leverage the combined analysis of all ISR disciplines, in and across all domains.

3.0 Air Force Cyberspace Forces

The Air Force has redefined its mission by extending the Air Force's global vigilance, reach, and power into the cyberspace domain. The foundation of all Air Force combat capability resides with Airmen. To achieve Air Force objectives, we must develop an organized, trained, and equipped force of Cyberspace Professionals capable of integrating, synchronizing, and executing sustained cyberspace operations across the full spectrum of conflict. Cyberspace Professionals will employ cyberspace warfare capabilities through operations designed to achieve strategic, operational, and tactical objectives. Our Air Force recognizes control of the air domain affords us freedom of action to operate in and through the air. We will leverage Air Force's capabilities – to include command and control, electronic warfare operations, network warfare operations, surveillance and reconnaissance, and intelligence – to conduct operations in the cyberspace domain while supported by, and in support of operations in the air and space domains. The concept of creating a variety of tailored effects over, around, and through fielded forces to strike at an adversary's center of gravity is essential to our Air Force missions. The unique aspects of the cyberspace domain allow integrated operations to occur instantaneously with the potential to deliver a full spectrum of global kinetic and non-kinetic effects. To

accomplish this mission, the Cyberspace Professional must be trained and educated to establish, control, and utilize the cyberspace domain.

3.1 Air Force Cyberspace Forces: Core Competencies

3.1.1 Establish the Cyberspace Domain

One significant characteristic of cyberspace is the requirement to first establish the domain. Cyberspace capabilities exist when electronics are networked together within a physical infrastructure that employs the electromagnetic spectrum to store, modify and exchange data. Possessing the ability to establish and operate portions of the domain, whether on land, through air, at sea or in space, becomes the foundational capability provided by our cyberspace forces. Provision and sustainment of information mobility capabilities is a precursor to utilization, control, or exploitation of cyberspace. Our Airmen must provide mission assurance and must have an intimate understanding of operations supported by their sustainment operations in order to effectively provide, control, and defend the cyberspace enterprise.

3.1.2 Control the Domain

It will not be sufficient for the Air Force to simply establish the cyberspace domain, for without effective control, operations in all other domains are placed at risk. Control of the domain demands robust situational awareness, the ability to prepare the battlespace ahead of time, strong defensive capabilities, and mechanisms to ensure positive command and control of our cyberspace warfare capabilities.

Control of the domain begins with effective situational awareness. Robust situational awareness means more than just monitoring network utilization, available bandwidth, and on-going perimeter attacks. We must be able to maintain real-time awareness of users, processes, communications, configuration changes, and use of resources for the network under their charge, while being able to discern between authorized and unauthorized, friendly and unfriendly activities across the electromagnetic spectrum. Situational awareness also means maintaining currency on threats to the enterprise, understanding the range of effects such threats can achieve, and being able to immediately assess impacts to both the cyberspace enterprise and the supported mission. Preparation of the battlespace enhances our ability to ensure control at the time and place of our choosing. Cyberspace Professionals provide the ability to prepare the cyberspace battle environment by employing technical skills and fielded capabilities, and/or through the coordination with others that do so. Timely, pervasive situational awareness and thorough preparation of the battlespace enables Cyberspace Professionals to properly defend friendly areas of cyberspace, whether in preparation for, in response to, or recovery from external and internal threats. Finally, control of cyberspace relies on our ability to effectively command and control the capabilities under our charge consistent with the strategic and operational objectives and rules of engagement as determined by the supported operational commander. This includes:

- establishing cyberspace defense plans that outline strategies and rules of engagement
- managing the use of cyberspace resources
- de-conflicting cyberspace operations

- coordinating with organizations outside their area of responsibility, and
- directing defensive or offensive actions based on a commander's chosen course of action

A Cyberspace Professional's awareness and understanding of cross-domain dependencies facilitates their ability to direct synchronized and integrated combat operations across the air, space, land, and sea domains. At the tactical level, this may mean directing changes to a network configuration or ordering the use of an electronic attack weapon. At the operational level, it means developing, integrating and executing a fully integrated cyberpower strategy within the AOC and in support of theater or global objectives.

3.1.3 Leverage the Domain

The ability to establish and control portions of cyberspace enables engagement across the domain at the time and location of our choice to achieve operational objectives. Effective control enables surveillance and reconnaissance activities or the projection of power in and through cyberspace from land-, air-, sea- or space-based platforms. Surveillance and reconnaissance operations within cyberspace produce data and information that feed a wide-variety of operations in air, space, and cyberspace. Such operations require special oversight and are typically conducted under authorities outlined in U.S.C. Title 50, except in immediate preparation for U.S.C. Title 10 operations. Cyberspace forces project power in and through cyberspace in order to ensure use of the domain while denying the same advantage to the adversary. Offensive operations in cyberspace directly affect the data resident in the domain, or the software and hardware components of the domain itself. Such operations can have a broad span of effects and include, but are not limited to, sensor disruption, data manipulation, decision support degradation, command and control disruption, weapons system degradation, and communications disruption. Offensive operations may be conducted to achieve stand-alone effects (e.g., deny adversary use of critical data on a server) or in support of other operations (e.g., disrupt adversary IADS capabilities in support of airborne ingress/egress operations). Offensive operations in cyberspace are conducted under authorities outlined in U.S.C. Title 10.

3.2 Air Force Cyberspace Enabling Competencies

3.2.1 Intelligence Competencies in Cyberspace

The ability to tightly integrate our capabilities to task, collect, process, exploit, and disseminate accurate and timely intelligence information is crucial today and will only increase as our technological dependency increases. It is imperative we provide the commander the situational and battlespace awareness necessary to successfully plan and conduct cyberspace operations in tandem with air and space operations. Commanders use the intelligence information derived from ISR assets to maximize their own forces' effectiveness by optimizing friendly force strengths, exploiting adversary weaknesses, and countering adversary strengths. Our mobilization into the cyberspace arena requires us to better define the intelligence requirements associated with this mission set. Integrated with other domain requirements, these requirements will help drive the development of intelligence professionals across air, space and cyberspace domains.

3.2.2 Engineering and Acquisition Competencies in Cyberspace

Rapid commercial technology refresh cycles and Air Force reliance on commercial infrastructure to deliver operational capabilities place a significant challenge on developing and acquiring cyberspace weapon systems and tools. Existing processes such as those used in the Secretary of the Air Force Rapid Capabilities Office can be used to develop standardized, yet agile, procedures for maintaining and acquiring combat cyberspace systems. However, the rapid pace of technological advancements necessitates a large reliance on commercial technologies. Acquiring commercial technology that supports the cyberspace warfighting mission presents a paradigm shift from current acquisition strategies. The Air Force will need to adapt current research and development and acquisition processes to rapidly deliver meaningful operational capabilities to the warfighter and posture the Air Force to counter peer competitors and technology savvy adversaries.

3.2.3 Research Competencies in Support of Cyberspace Operations

A significant component of the Air Force's development of cyberspace capabilities will require technological capabilities that do not currently exist today. The Air Force must support the research efforts that can satisfy both short term/quick reaction requirements and long term acquisitions. This research will take place both inside and outside the Air Force, but must be guided in directions that support prioritized cyberspace operational requirements with emphasis on solutions that are on a timely technical transition path to provide useful solutions to the warfighter.

3.2.4 Space Operations in Cyberspace

There are some space mission areas that achieve effects in the cyberspace domain. Counter communications is a primary mission that operates in cyberspace. As cyberspace develops, there may be space mission areas that may make sense, to include as a part of cyberspace to include as a part of cyberspace operations. 13Ss and 1C6s will continue their roles in space and will likely have job opportunities in cyberspace. For those roles in space mission areas that achieve effects in cyberspace, it is yet to be determined as to what roles will be accomplished by space operators (13Ss and 1C6s), or cyberspace operators (17Ds and 1BXs).

4.0 Air Force Cyberspace Career Fields: Force Development Foundations

The Air Force will produce professional Airmen with the ability to establish, control and leverage the cyberspace domain. They will operate across a broad range of critical infrastructures, warfighting systems, and technologies and employ capabilities from airborne platforms and through space systems, from in-garrison units and from forward deployed units. They will comprise combat ready forces able to execute missions as part of air, space, special ops, and cyberspace combat missions. As a matter of necessity, these will be cross-domain professionals since it is they who will establish, control, and achieve effects within a domain upon which all forces rely.

4.1 Roles

Success in all domains, air, space, and cyberspace, is and will be increasingly dependent upon the success we achieve developing core cyberspace competencies in our Cyberspace Professionals. Based on concepts identified in Sections 2 and 3 of this Roadmap, we can identify core roles fulfilled by these Airmen: Operators, Specialists, Analysts and Developers. In order to establish, control and project power in and through this domain, we require professionals who have the technical prowess, ingenuity, and ability to adapt and overcome the challenges faced within it. It is a holistic effort and one that cannot be accomplished by any singular skill set. This cadre must exemplify a Total Force Integration construct, combining strengths of active duty, Air National Guard, Air Force Reserve, civilian, and contractor personnel.

4.1.1 Cyberspace Operators

Cyberspace Operators plan, direct, and execute defensive and offensive actions in and through cyberspace in support of assigned missions. Fundamentally, they maintain an in-depth understanding of the technologies and characteristics that comprise cyberspace (e.g. the EMS, networking fundamentals) and a general knowledge of common functional networks found within the domain. 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 achieve a range of effects (e.g., deny, disrupt, collect, defend, etc.). At the operational and strategic levels they are well versed in a broad range of cyberspace capabilities which permits them to become planners who can effectively integrate these assets with other national and military capabilities and advocates who can sharply champion future requirements. While every cyberspace operator possesses fundamental competencies in a broad range of technologies, ideally each specializes in a select few. In addition, those assigned to airborne platforms or space-based missions require additional skill sets in order to operate effectively in those domains. Career field constructs for cyberspace operators, including AFSC, training, and education concepts, and career paths, are outlined later in this document.

4.1.2 Cyberspace Specialists

Cyberspace Specialists provision, sustain and protect friendly portions of cyberspace. From the installation and configuration of an airborne router to “touch maintenance” of a base local area network (LAN), Specialists work on portions of cyberspace used by all Air Force personnel in support of a wide variety of missions. Their efforts are conducted under the auspices of defensive operations and in coordination with cyberspace operators in order to ensure their activities are executed in accordance with the defensive strategies of the entire enterprise. Competencies for cyberspace Specialists range from system administration to network engineering to Radio Frequency fundamentals. They are able to build, install, and manage system hardware, operating systems and applications. For specialists supporting airborne or space-based assets, they must also comprehend the integration and interdependencies between their responsible portions of cyberspace and the applicable major weapon system platforms. Career field constructs for cyberspace specialists, including AFSC, training and education concepts, and career paths, are outlined later in this document.

4.1.3 Cyberspace Analysts

Analysts supporting cyberspace operations examine all-source intelligence information, analyze industrial, technological, geographical, and sociological factors; prepare intelligence assessments; and apply processed intelligence information in support of assigned missions in cyberspace. Like all intelligence analysts, cyberspace analysts maintain the basic qualifications required in the intelligence career field. However, the nature of cyberspace warfare requires that these analysts possess additional skills in networking, operating systems, internet protocols, system architectures, and aspects of the EMS. More in-depth knowledge of select technologies is dependent upon the supported cyberspace warfare missions. While a cyberspace analyst will be trained in certain technologies, their expertise and experience should be focused more on functional application of networks. Such competency not only creates a cadre of experts capable of analysis and targeting for offensive operations, but provides the technical foundation with which to recognize adversary trends, technologies, and TTP in support of defensive operations. Career field constructs for cyberspace analysts will be outlined within the subsequent Cyberspace Force Development Implementation Plan. However, it is expected that they will not comprise a separate AFSC, but be identified within existing Intelligence AFSCs.

4.1.4 Cyberspace Developers

Cyberspace Developers design, develop, and document solutions that can be tactically employed by cyberspace forces to meet combatant commander requirements. They apply current technologies, sound engineering techniques, and proven TTP in their work. These professionals, in collaboration with operations, test, and range units, work long- and short-term solutions to create or modify tools, weapon systems, and TTP that meet current and emerging operational needs. Developers for long-term projects should have experience as cyberspace operators.

Developers require very specific and extensive educational preparation. Many will have advanced academic degrees (Master's or higher) in a particular computer science or engineering specialty. Minimally, they have in-depth expertise with the software or hardware technologies to which they are assigned (usually specializing in one or more network classes), appropriate computer programming experience and expertise, and sound problem solving skills. Career field constructs for cyberspace developers will be outlined within the subsequent Cyberspace Force Development Implementation Plan. However, it is expected that they will not comprise a separate AFSC but be identified within existing engineering and acquisition AFSCs.

4.2 Force Development – Cyberspace Operators and Specialists

As an initial first step, these cyberspace forces will be developed under the split Functional Authorities of AF/A3/5 and SAF/XC. This construct will allow the Air Force to immediately apply the accumulated functional, operational and technical expertise to the challenges of forging an integrated cyberspace force development plan. Functional Management of rated Cyberspace Airmen will be performed by AF/A3O, while Functional Management of all non-rated Cyberspace Airmen and the civilian cyber work force will be SAF/XCT. To ensure the integrated and operationally-focused development of these forces, a Cyberspace General Officer Steering Group (GOSG) will be established to ensure the aggressive implementation of this

roadmap meets the long-term needs of the Air Force and our Nation. This Cyberspace GOSG will be co-chaired by AF/A3O, SAF/XCT, AF/A1P and AFCYBER(P)/CC (pre-MAJCOM activation) / AFCYBER/CV (post-MAJCOM activation). In the future, as Air Force Cyberspace Command becomes operational, as cyberspace operating concepts mature, and as we press towards a more complete integration of our cyberspace forces, the Functional Authority will rest with the AF/A3/5.

These cyberspace operators and specialists comprise an accessions-to-retirement force and their careers will traverse air, space, and cyberspace organizations executing and supporting a wide array of Air Force missions. They will achieve a high degree of technical competency early, followed by a high degree of management and leadership proficiencies later in career development. As Senior NCOs and Field Grade Officers, our force will have developed a great degree of understanding regarding the integration and employment of cyberspace capabilities with Air, Space, and Cyberspace operations.

A cornerstone of the cyberspace force development construct recognizes the integrated and inseparable ties between provision/sustainment operations and C2/warfighting operations of cyberspace. Our construct builds on the tight coupling of these mission/skill sets and will allow the Air Force to field forces with the technical depth and breadth required to secure and dominate cyberspace while supporting all aspects of cyberspace operations.

A second foundational aspect of cyberspace force development is the cross-domain nature in which forces are employed. The force development focus is on fielding combat ready cyberspace forces to execute missions as a part of space, special ops, air mobility, air combat, and cyberspace combat organizations. If the mission requirement includes provisioning, sustaining, defending or conducting offensive operations in the AF cyberspace enterprise, these requirements will be met by purposely-developed cyberspace forces.

4.2.1 Enlisted Cyberspace Force Development Concept

Ingenious and innovative enlisted leaders must be developed and professionalized to ensure the cyberspace capabilities are successfully employed. The enlisted cyberspace force must be built to establish, secure, control, and operate across a broad range of critical infrastructures, warfighting systems, and technologies.

The enlisted force will provide the technical depth to execute both the cyberspace functions and tactical missions required for cyberspace dominance. These missions may be executed from a deployed-in-place cyberspace or space ops unit, an airborne cyberspace attack platform, or a forward deployed team supporting Combatant Commander requirements. These Airmen will be developed and managed as a new, integrated series of Air Force Specialties in the 1B career field. The 1B career field is depicted in Figure 1 and detailed in Appendix B.

The 1B AFS series will require the transformation of the 2E (Communications-Electronics Systems), 3A (Information Management) and 3C (Communication-Computer Systems). The foundation to consolidate these different AFSCs has been in place since 2001 and is driven by a convergence in technical advances and efficiencies gained in streamlining current operations. Additionally, the ground based technical support, configuration, maintenance and repair of

aircraft special mission platforms currently performed by a variety of AF specialties will be incorporated into the cyberspace workforce. The migration of the backend maintenance function to the cyberspace workforce provides seamless ground/air networks that are built, secured, maintained, and operated by cyberspace professionals. As indicated in paragraph 7.1.4, a review of the 1A3 (Airborne Mission Systems) series of AFSCs will identify mission skills that may or should require cyberspace training or which may migrate to cyberspace AFSCs. This force development approach capitalizes on these efforts and enables us to build new enlisted specialties that ensure qualified/certified professionals provision, sustain, protect and defend these critical airborne/space assets as nodes in a larger AF cyberspace enterprise.

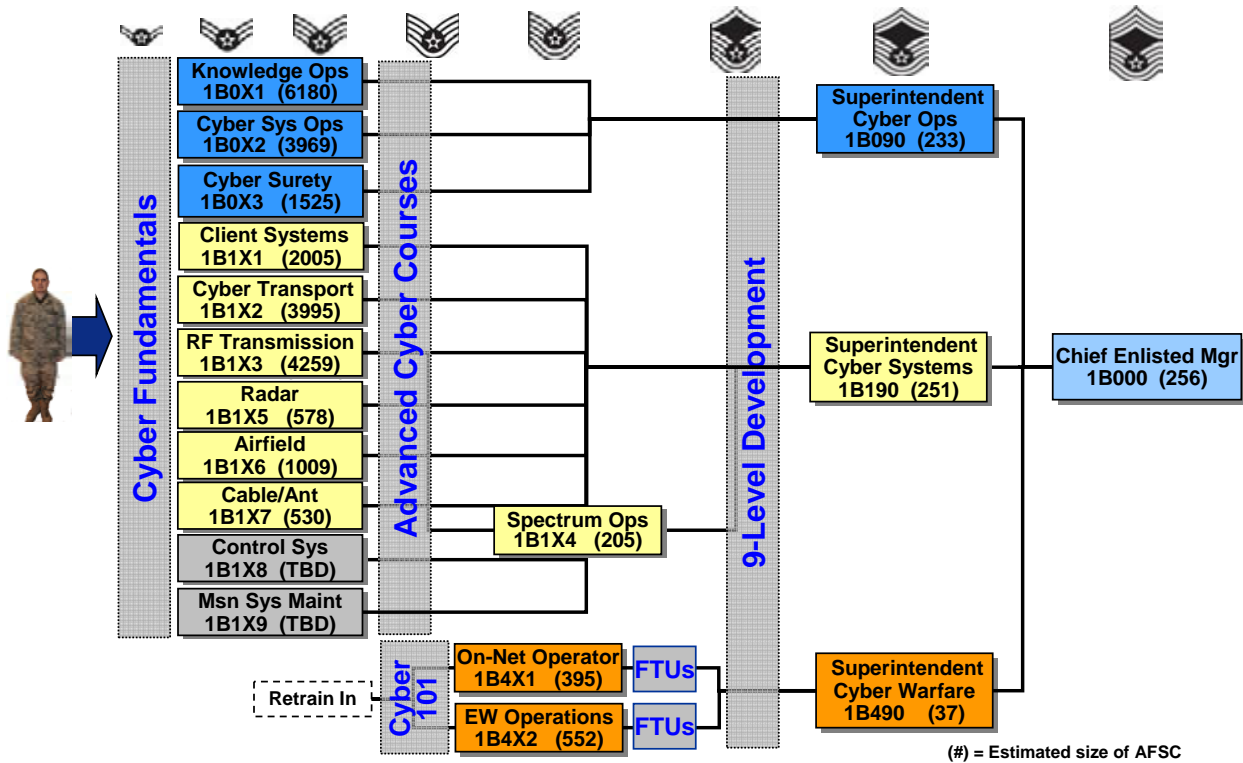


Figure 1: Enlisted Cyberspace Force Development Construct

4.2.2 Officer Cyberspace Force Development Concept

The Cyberspace Warfare Officer (CWO) force development construct will produce professional airmen able to establish, control and leverage an operational cyberspace domain. While technical degrees, including in some cases graduate technical degrees, and other technical proficiencies will be required, a breadth of knowledge and experience within cyberspace and across other domains is the desired end-state. These officers will be developed to generate the leadership, vision, and advocacy for the future of Air Force cyberspace operations. All CWOs will be developed in an integrated fashion under the oversight of the Cyberspace GOSG and in coordination with other Functional Authorities to promote cross-functional and cross-domain career broadening opportunities. There will be several

variants of the CWO, but they will all be ‘cut from the same bolt of cloth.’ While some CWOs will require a Navigator rating to get them into the fight, others will not. Initially, this construct will require separate Functional Authorities, Functional Managers and Career Field Managers for the rated and non-rated CWOs, but with efforts synchronized and unified under a single Cyberspace GOSG.

The foundation for consolidation of these different AFS series lies in the rapid convergence of electronic warfare (EW) and network warfare (NW) targets and capabilities. Both EW and NW can, and are conducted from airborne platforms and their convergence increases with each technological advance. As we further develop our dependence upon the systems and applications that traverse the cyberspace domain, we find our own capabilities vulnerable to attacks from potential adversaries. These vulnerabilities exist in our airborne platforms/systems, our terrestrial data and communication systems, and in our space-based capabilities.

CWOs initially will be comprised of both 17D (non-rated) and 12W (rated) Air Force Specialties and developed in an integrated approach under the oversight of the Cyberspace GOSG. Implementation of the 17D series construct will require the phase-out of the 33S Air Force Specialty, while implementation of the 12W construct will require the transformation of the 12X Electronic Warfare Specialties. The 17D and 12W CWO specialties are depicted in figure 2 and detailed in Appendix C.

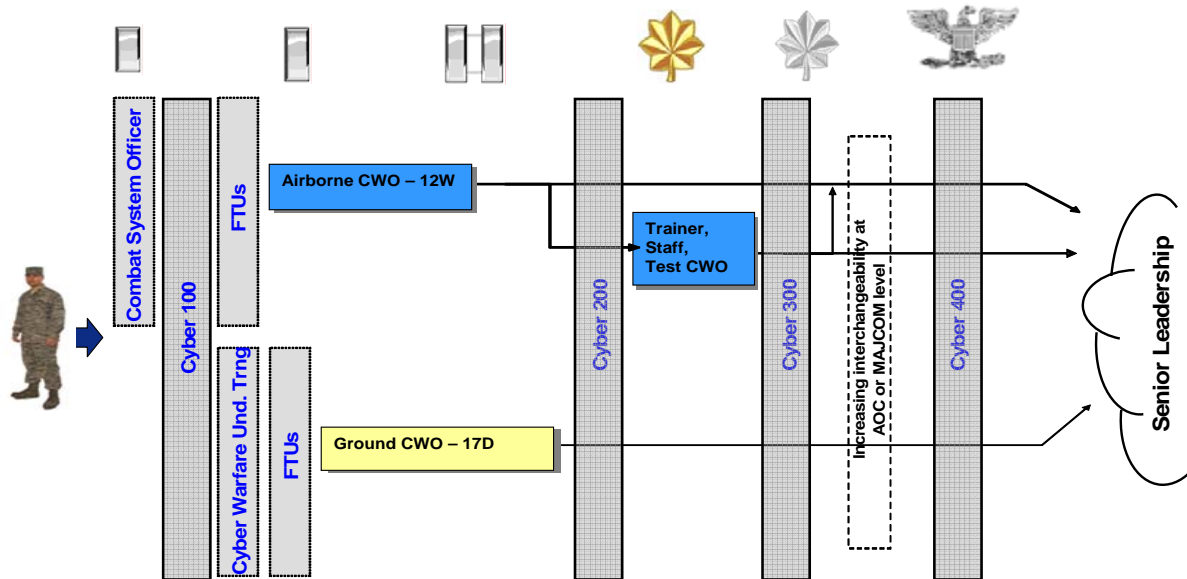


Figure 2: Officer Cyberspace Force Development Construct

All CWOs will be trained early in technical skills and prepared for a wide variety of jobs in cyberspace operations. Those CWOs who do not require an aeronautical rating will fulfill jobs in cyberspace, air (as X-prefixed coded 17D positions) and space organizations. The rated CWO (12W) must be developed beyond today’s current Electronic Warfare Officer and better prepared to fulfill increased duties in the cyberspace domain. Those CSO students who are assigned upon

graduation to aircrew positions that are designated as cyberwarfare will be sent to the Cyberspace Fundamentals course which will award their specific 12W AFSC (see figure 3). These officers will be developed for technical depth in their major weapon system platform, consistent with public law and Air Force policies, evaluated for appropriate non-flying, cyber-broadening assignments at key time frames in their careers. While all EW AFSCs are to be considered for inclusion as 12Ws, a separate study will refine recommendations on the EW AFSCs which will convert to 12Ws (see paragraph 7.1.4).

This force development construct provides continuing education through a progression of Cyberspace 100/200/300/400 courses over the span of an officer’s career. These courses will systematically integrate the rated and non-rated CWOs to synergize warfighting experiences and increasingly converge the two sub-sets of CWOs as officers advance in rank. The long term plan will be to fully integrate these cyberspace forces within a single family of cyberspace Air Force Specialties by 2018. As field grade officers, CWOs will be uniquely qualified to work at the MAJCOM Staff level or as a planner in the Air Operations Center (AOC), and then prepared for key leadership roles.

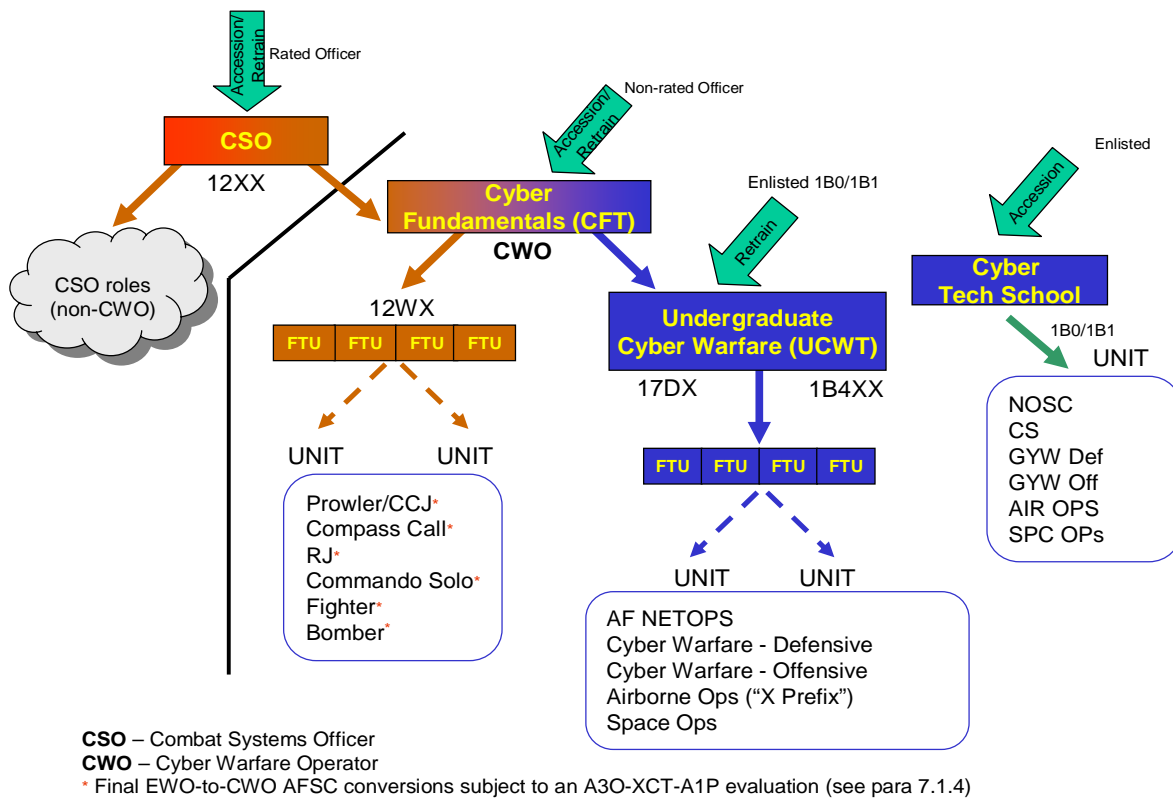


Figure 3: Cyberspace Force Education & Training

4.2.3 Civilian Work Force Development Concept

The civilian force development construct will develop civilian professionals integral to the establishment, control and leverage of cyberspace to achieve AF and national objectives. While

increased technical proficiencies will be required, a breadth of knowledge across all cyberspace operations is the desired end-state. These civilians will help provide leadership, vision, and advocacy for operations today and for future cyberspace operations. The civilian cyberspace workforce will be developed alongside their enlisted and officer counterparts using constructs conducive to taking full advantage of and implementation of the National Security Personnel System (NSPS) and other applicable personnel systems, policies and procedures. Using a two track process, the civilian leader will be developed using both a Leadership and a Technical track to provide maximum career development opportunity based on the individual's personal talents and career aspirations while also meeting the needs of the Air Force. The Cyberspace Functional Authority will coordinate with other Functional Authorities to promote cross-functional and cross-domain career broadening opportunities, promote leadership development, and develop common Air Force visions for shared occupational series.

5.0 Air Force Cyberspace Career Fields: Training and Education Concept

Technical prowess, ingenuity, and an ability to adapt and overcome are hallmark of the United States Airman. The ultimate source of combat capability resides in our people. The value of strategy, technology, and organization is diminished without professional airmen to leverage their attributes. Our total force of active, Guard, Reserve, civilian, and contractor personnel is our largest investment and most critical asset. Realistic training, high standards for technical competence, strong analytical skills, and personal reliability are key elements that shape the force. Our Airmen will be presented with no greater technical challenge than the demands that warfighting and integration in cyberspace bring to bear, and these challenges, along with the rapid pace of change in cyberspace will drive significant investments in our training and force development programs.

Every Cyberspace Airman will be required to know and understand a core set of cyberspace fundamentals. These fundamentals will differ some between the officer and enlisted force, but will serve to define the professional force which will allow the Air Force to 'fly and fight' in cyberspace. It is on this foundation that we will implement specific Cyberspace AFSC training, built on core technical competencies which define each AFSC. These forces will be fielded and integrated into air, space, and cyberspace organizations to ensure success in all Air Force mission areas. Operational roles will require AETC training at the accession level and at follow on training courses (Cyber 100/200, 5-level, 7-level, 1B4 schools, and Formal Training Units as they are developed). Training will require rigorous unit-level training using the Initial Qualification Training (IQT) and Mission Qualification Training (MQT) construct.

Our Total Force partners in the Air Reserve Component (Air National Guard and Air Force Reserves) are a key component in allowing the Air Force to maintain the technical and professional skills required. Because these Cyberspace Airmen will often be employed within the industries that produce the means to establish, control, and operate within the cyberspace domain, the Air Force can leverage their technical skills and train them in unique ways. Technically experienced personnel can be a source of expertise for training our active duty personnel through syllabus validation or acting as subject matter expert instructors. Due to the unique background and availability of Air National Guard and Air Force Reserve personnel, consideration may need to be given to reducing time spent in lengthy, in-residence schools in

order to free them up for operations and targeted education. This concept may require a new mind-set along the lines of the DoD's Continuity of Service initiative.

Directly contributing to our cyberspace force development approach will be the establishment of an Air Force designated and funded Cyberspace Technical Center of Excellence (AF CyTCoE) at the Air Force Institute of Technology. This center will be a catalyst, informational center point and advocate to serve as a bridge between the operational cyberspace forces and the various cyberspace research, education, and training communities within the USAF, DoD, various federal agencies, and civilian academic and commercial research organizations. The AF CyTCoE will require the leadership and close integration between the Air Force academic and research institutions, and outreach to the Department of Defense (DoD) and national organizations to further define and develop our mission capabilities in cyberspace. To advance Air Force's capabilities in cyberspace, it is paramount the Air Force focus cyberspace education, training, and research efforts to optimize return on investment.

6.0 Air Force Cyberspace Career Fields: Challenges

The United States of America is significantly dependent on the use of cyberspace to maintain its way of life and to employ the instruments of national power – and our dependence is increasing daily. The rapid development and use of networks, telecommunication systems, transmission systems and other technologies that use electronics and the electromagnetic spectrum (EMS) have led to the recognition of cyberspace as a domain. Several potential adversaries already recognize America's dependence on cyberspace as a national center of gravity. They actively seek ways to exploit this reliance while using the domain to further their own agendas. Therefore, developing Air Force cyberspace capabilities is a strategic imperative for protecting and preserving the sovereignty of the United States. Our current understanding of cyberspace and operations in this domain will mature over the next few years and as such, we can expect that our force development initiatives will undergo to a corresponding evolution in understanding and approach. This document will guide the development of our forces into the future and the implementation plan for this Roadmap will be subject to recurring review and vector checks. Cultural, organizational and fiscal realities pose significant challenges to our immediate and pressing need to develop Air Force Cyberspace Airmen.

6.1 Cultural

Complete development of the Cyberspace Professional includes a dramatic cultural transformation. The growth of the cyberspace profession must take us from a culture traditionally characterized as 'supporting' or 'enabling,' to one exemplified as 'warfighting' and 'operational.' Cyberspace capabilities provided by today's electronic warfare mission set bring a well-developed warfighting culture to the table that must be leveraged in the command, control, and operations of the AF's cyberspace enterprise, as well as in the global provisioning, protection, and sustainment of cyberspace capabilities. Additionally, cultural differences that distinguish cyberspace operations performed by today's rated force and cyberspace operations performed by a predominately non-rated force will pose challenges to integrating and unifying goals. Creative and forward-thinking vision will be required to ensure the Air Force cyberspace

force development efforts continue to move forward and achieve parity with mature Air and Space force development efforts.

The nature of cyberspace operations demands an increased technical capability in the enlisted force. The Air Force has always depended on the technical competence of the enlisted force and roles in cyberspace will push technically savvy, well-trained airmen to the forefront of our warfighting operations. The core competencies, knowledge-skills-abilities, and technical foundations required through all aspects of cyberspace tightly couple the traditional roles of the sustainer and the operator.

6.2 Organizational

Changes should and must occur across multiple organization levels within the Air Force to support the Air Force's cyberspace objectives (see paragraph 2.0). The Air Force has already established a new, provisional major command, AFCYBER (P) and has identified a robust organizational construct to be in place upon activation of AFCYBER. Additionally, further initiatives will identify and develop Reserve and Air National Guard organizations which can contribute to cyberspace operations. However, the development and sustainment of the AF Cyberspace Airman should be largely independent of organizational constructs and should be well-grounded in a capabilities-based development approach.

6.3 Fiscal

The cyberspace challenge is significant and resources are bounded. It is imperative the Air Force foster strong partnerships with other Services, government agencies, industry, and academic institutions to share intelligence and intellectual capital. From a programmatic and requirements perspective, the Air Force currently supports multiple operational activities within the cyberspace mission area. The requirements derivation, planning and programming of these activities are spread across numerous program elements managed throughout the Air Staff directorates and impacts multiple Air Force Corporate Panels. Developing new cyberspace career fields will require additional funding beyond the current FY08/09 POM allocations. In large part this is due to the formalization of new AF Specialties trained to execute network warfare missions. Today, there is little-to-no mission specific training for such operations, and no AFSC awarding courses for the airmen expected to provide this critical capability. While some force development efforts can be executed in FY08 and FY09, significant change cannot occur without successful identification, prioritization and FY10 funding of cyberspace education and training requirements.

7.0 Air Force Cyberspace Career Fields: Milestones and Implementation

In order for the Air Force to field forces in an expeditious fashion and meet the operational challenges of warfare in the cyberspace domain, several closely-integrated tasks must be executed in parallel. Major milestones are identified in Figure 4. An AF Cyberspace Force Development Implementation Plan will be developed, with a target approval date of 30 Apr 08. It will provide the detailed courses of action necessary over the next ten years to make this Roadmap a reality. Development of this implementation plan will be the responsibility of the

UNCLASSIFIED – FOR OFFICIAL USE ONLY

AF/A3O-C under the guidance and oversight of the Cyberspace GOSG chaired by AF/A3O, SAF/XCT, AF/A1P and AFCYBER(P)/CC. The Cyberspace GOSG will convene to review the progress and status of the Implementation Plan at least twice annually to assess progress. In addition to the milestones generalized in Figure 4, the following are essential tasks that are considered the most crucial. These tasks will be included in greater detail in the Implementation Plan. This tasking list is not all inclusive or comprehensive. As our efforts mature, other essential tasks may manifest themselves.

These tasks will be included with greater detail in the Implementation Plan:

7.1 Formalize and implement AFSCs and career paths for the Cyberspace Professional as detailed in this Roadmap, NLT 1 Oct 09.

7.1.1. The Air Force Warfighting Integration (XC) Community will develop an AF/A3O SAF/XC coordinated cyber force development plan for cyberwarfare operators and specialists in order to field an operationally adequate depth of expertise to execute cyberspace operations.

7.1.2. The Air Force Intelligence (A2) Community will detail a force development plan that will produce an operationally adequate depth of expertise in our cyberspace analysts necessary to conduct cyberspace operations.

7.1.3. The Functional Authority for Scientists & Engineers (SAF/AQ) will detail a requirements-based force development plan for engineers that include cyberspace domain experience.

7.1.4. AF/A3O will establish an A3O/XCT/A1P evaluation team to review existing electronic warfare operations and, by 01 December 2008, make recommendations to the Cyberspace GOSG on the following:

- recommend changes to targeted EW AFSCs (see Appendix C) which will be converted to rated cyberspace (12W) AFSCs
- recommend EW billets which may be considered for conversion to X-prefix 17D billets
- recommend changes which should be considered to Cyber 100 training for all CWOs (rated and non-rated)
- recommend 1A3 AFSC missions which require cyberspace training, or which should migrate to new cyberspace AFSCs

7.2. Establish and mature AETC training pipelines for all Cyberspace Professionals. In the short-term, expanding the curricula of existing schools in order to quickly field our initial cadre is expected. In the long-term, novel approaches to training should be institutionalized and further consideration given to geographical co-locating cyberspace schoolhouses to leverage our leading-edge organizations in this arena (e.g., AFIT, AFRL, or San Antonio), where and when appropriate.

7.3. Develop and implement education and training programs to transition current forces into implemented cyberspace AFSCs in FY10. The C&I and EWO communities will form the

UNCLASSIFIED – FOR OFFICIAL USE ONLY

UNCLASSIFIED – FOR OFFICIAL USE ONLY

preponderance of our cyberspace forces. As such, they will make for a relatively easy transition to the new career fields. Additionally, a significant number of individuals representing a wide-variety of AFSs outside the C&I and EWO communities possess skills and experience critical to cyberspace. These transition efforts will require collaboration between multiple functional communities in order to ensure a strong initial cadre of cyberspace forces.

7.4. Evaluate and implement appropriate civilian force development constructs, and ensure such constructs are integrated with officer and enlisted force development plans. Our civilian workforce will fulfill many cyber-related roles, to include some of those identified above. Current civilian force development constructs will be evaluated and modified as appropriate.

7.5. Establish training standards and evaluation mechanisms analogous to those of airborne and space operations. It is imperative that development must include a change in culture from one of “support” to one of “operations”. AFCYBER will lead the development of training and evaluation standards for cyberwarfare operations units. Formal qualification training, weapon and mission readiness standards, and recurring evaluations should be part of every Cyberspace Professional’s development and is essential to increase operational effectiveness.

7.6. Establish professional development education programs to ensure Cyberspace Professionals maintain exposure to activities and changes across the breadth of this mission area. The Air Force cyberspace force development construct provides continuing education through a progression of cyberspace 100/200/300/400 courses over the span of an individual’s career. These courses will systematically integrate Cyberspace Professionals to educate and synergize warfighting experiences.

7.7. Develop recruiting, accession, and retention strategies. Proper screening and the implementation of focused pre-accession programs can reduce the time, money and AETC training burden to field qualified personnel. Expansion of the ASVAB and AFOQT, or the development of new tests should be considered to identify individuals with a strong aptitude and desire for this mission area. Summer programs for our cadets and more specialized degree programs will also help prepare incoming Cyberspace Professionals. Well planned retention strategies must be developed to help retain these skilled professionals.

7.8. Develop and ensure that necessary resources are allocated within the FY10–15 POM. This should include, but are not limited to, the establishment of new and the re-tooling of existing AETC schools, as outlined in this Roadmap (1BXXX, Cyberspace 100/200/300/400, UCWT, Field Training Units, continuing education, transition/grandfathering training, etc.).

7.9. Immediately establish an Air Force Cyberspace Technical Center of Excellence (AF CyTCoE) in FY08. This AF CyTCoE will serve as a bridge between operational cyberspace forces and the various cyberspace research, education, and training communities within the Air Force, our sister services in DoD, the various federal agencies, and civilian academic and commercial research organizations. It will serve as the Air Force catalyst, clearinghouse, and advocate for cyberspace education, training, research and development across globe.

7.10. Expand PME for all Airmen to incorporate theory and application for warfighting in Cyberspace. Just as air and space power theory are inculcated throughout our enlisted and

officer PME, so must cyberspace power theory and application. PME curricula will be expanded to ensure our Airmen understand the application of warfare in this domain.

7.11. Establish continual training to ensure all Airmen are knowledgeable of the dynamics, and ever present and changing threats in the cyberspace environment. All levels of education and training from accession through senior level courses should enhance awareness of the threats and skills required to defend against threats, both internal and external.

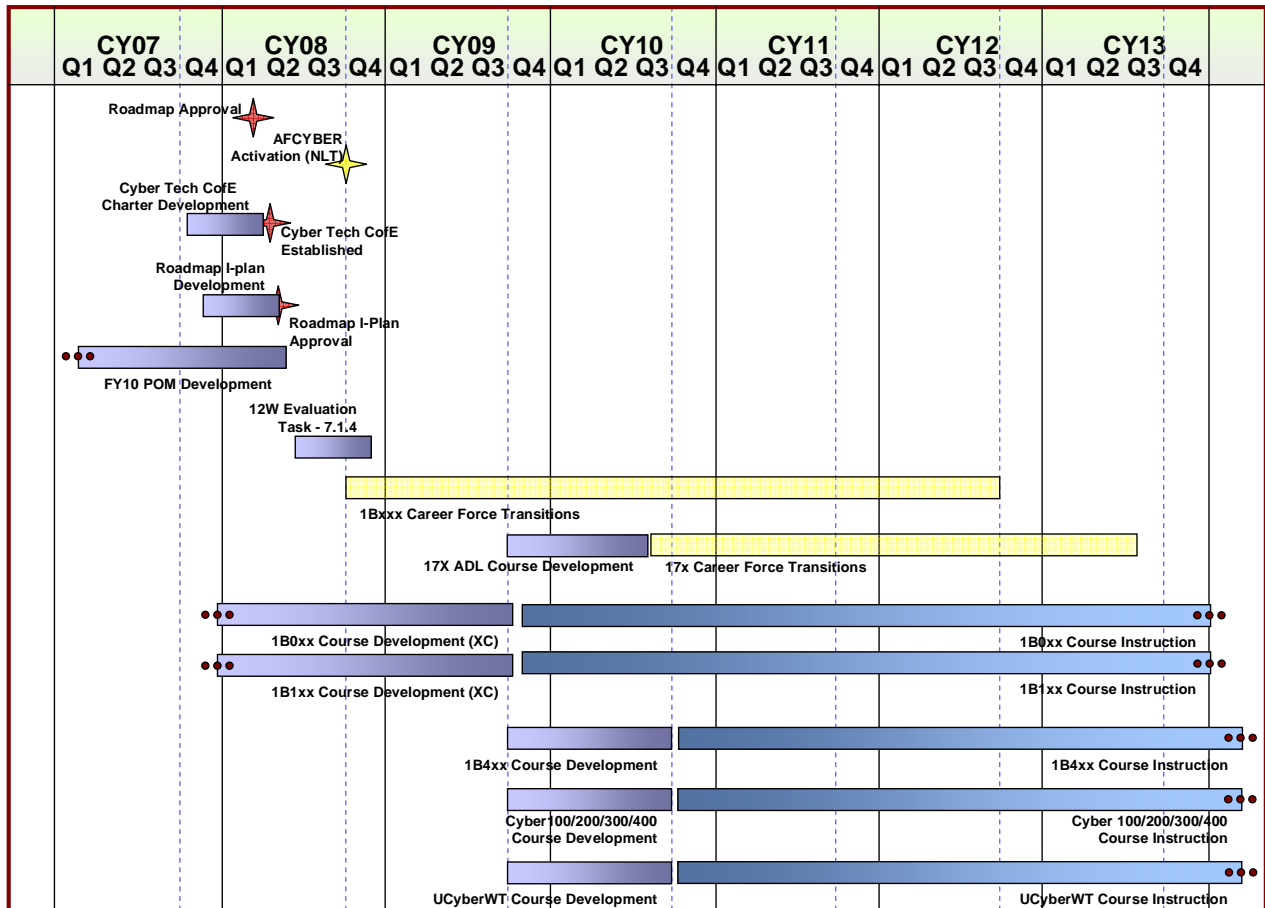


Figure 4: Major Cyberspace Professional Roadmap Milestones

8.0 Summary

The characteristics of cyberspace allow operations to occur literally at the speed of light and potentially deliver a wide range of effects almost anywhere in the world. Our cyberspace combat forces, integrated with other combat forces, can deliver effects in all domains in support of national and theater objectives. It is important to recognize the development of these new cyberspace forces as the foundation for presenting and executing cross-domain cyberspace capabilities. The cyberspace forces we charge to ensure freedom of maneuver in the Cyberspace

domain must be developed on a par with professionals similarly charged in the Air and Space domains.

The work done to scope out a solution for the development of our cyberspace forces is significant, but it is only the beginning. The core cyberspace operations and competencies identified in this roadmap form the foundation for understanding operational cyberspace roles and force development. The *Roadmap to Develop Cyberspace Forces* establishes a new officer and enlisted force structure and the Air Force will move forward aggressively to develop and field forces who can ‘fly and fight’ in cyberspace.

Appendix A: References

National Military Strategy for Cyberspace Operations

National Military Strategic Plan on Cyber Ops

JP 3-13, Information Operations

Air Force Strategic Plan, 2006 - 2008

Air Force Roadmap 2006 - 2025

AFDD 1, Air Force Basic Doctrine

AFDD 2-1, Air Warfare

AFDD 2.5 Information Operations

AFDD 2-5.1 Electronic Warfare

Concept for Employment for Cyberspace (8AF)

Appendix B: Enlisted Cyberspace AFSC Construct

[Knowledge Operations \(1B0X1\)](#)
[Cyber Systems Operations \(1B0X2\)](#)
[Cyber Surety \(1B0X3\)](#)
[Client Systems Specialist \(1B1X1\)](#)
[Cyber Transport Systems Specialist \(1B1X2\)](#)
[RF Transmission Systems Specialist \(1B1X3\)](#)
[Cyber Spectrum Specialist \(1B1X4\)](#)
[RADAR Systems Specialist \(1B1X5\)](#)
[Airfield Systems Specialist \(1B1X6\)](#)
[Cable/Antenna Systems Specialist \(1B1X7\)](#)
[Control Systems Specialist \(1B1X8\)](#)
[Mission Systems Maintenance \(1B1X9\)](#)
[On-Net Operations \(1B4X1\)](#)
[Electronic Warfare Operations \(1B4X2\)](#)

Knowledge Operations (1B0X1)

Knowledge operations will focus on ensuring information is available, accurate, relevant, secure, timely, and usable. They will plan, collect, control, process, manage, protect, and share organizational data and information assets. Knowledge operators will possess application and presentation networking skills necessary for content management, retrieval, and presentation. They will leverage people, processes, training, and technology to acquire, share, process, and manage information and experiences to create ubiquitous access to coalesced tacit and explicit knowledge. Skills required to fuse and present data, information, and knowledge will be required to facilitate the delivery of decision quality information to commanders, aiding commander's in obtaining situational awareness and understanding of the battlespace to make timely and effective decisions faster than the adversary. They will possess skills to identify, recon, and exploit information vulnerabilities within network environment to achieve desired affects. They will deploy in small teams to manage, integrate, and deliver data, information, and knowledge services enabling decision superiority.

Cyber Systems Operations (1B0X2)

Systems operators will focus on servers, data storage and the software applications and possess a solid understanding of information systems technologies, protocols, standards, and applications required to integrate cyberspace systems and applications. Their core competencies are servers, core services, distributed applications, security, enterprise storage, database administration, messaging, application monitoring, and client interfaces. They will possess the skills required to support the identification, reconnaissance and exploit vulnerabilities within cyberspace environments to achieve desired affects. They will deploy in small teams to provide, sustain, and enhance core services, plus administer warfighter networks.

Cyber Surety (1B0X3)

Cyber Surety operators use fixed and deployed Information Technology (IT) resources to monitor and evaluate policy and procedures to protect clients, networks, data/voice systems and databases from unauthorized activity. They identify potential threats and manage resolution of security violations. They enforce national, DoD and Air Force security policies and directives to enhance cyberspace security by installing, monitoring and directing proactive and reactive information protection and defensive measures to ensure Confidentiality, Integrity, Availability, Authentication and Non-Repudiation of IT resources. They administer and manage the Information Assurance (IA) program to include Communications Security (COMSEC), Emissions Security (EMSEC) and Computer Security (COMPUSEC) programs. They will deploy in small teams to secure and defend the Air Force enterprise.

Client Systems Specialist (1B1X1)

The Client Systems specialists will possess a solid understanding of information systems technologies, protocols, and standards required to integrate and sustain common client-level voice, data, and video devices. Although their focus will primarily be on end user devices, they will possess the networking skills necessary to ensure these systems can reliably interface with base infrastructure. They will deploy in teams to integrate, manage, and sustain client information services equipment and devices.

Cyber Transport Systems Specialist (1B1X2)

Transport Systems specialists will possess a solid understanding of network technologies, protocols, and standards required to integrate and sustain airborne and terrestrial information transport systems. They will focus on sustainment of the network and telecommunication infrastructure, distribution media, cryptographic equipment, and associated devices. They will possess the skills required to identify, recon, and exploit vulnerabilities within a network environment to achieve desired affects. They will deploy in teams to provide and sustain the networked infrastructure accessing the global information grid.

RF Transmissions Systems Specialists (1B1X3)

RF Transmissions Systems specialists will possess solid understanding of space, radio, and satellite systems technologies and configurations required to integrate and sustain airborne and terrestrial multi-mode, multi-band radio frequency systems. They will focus on wireless voice, data, and video infrastructure, distribution media, cryptographic equipment, and associated devices to interface with the global information grid. They will possess the skills required to identify, recon, and exploit vulnerabilities within network environment to achieve desired affects. They will deploy in teams to integrate, manage, and sustain a variety of radio frequency systems that support dispersed forces and aggregated connectivity from control centers to reach-back facilities.

Cyber Spectrum Specialist (1B1X4)

Spectrum specialists engineer, nominate, and assign frequencies to support communications and operational requirements. They coordinate frequency needs with federal, military, and civil spectrum management offices and secure operating authority, while promoting interference-free radio frequency operations. They review spectrum interference reports, and establish/analyze baseline signatures across the cyberspace domain. They identify interference and coordinate countermeasures to neutralize effects as well as analyze spectrum requirements to determine compatibility, system specifications, antenna data, emission characteristics, and propagation modes. They will deploy in small teams to provide electronic attack, jamming, deception, and theater level spectrum management.

RADAR Systems Specialist (1B1X5)

Radar Systems specialists will possess a solid understanding of radar technology to support airfield, weather, and early warning radar system missions. They will ensure airfield radar systems meet all national airspace system certification requirements and will be capable of performing search, intercept, identification, and location of sources radiating electromagnetic energy for purposes of immediate threat recognition. Although focused on radar systems, they possess skills to integrate with the global information grid. They deploy in teams to integrate, manage, and sustain airfield, theater air control, and early warning radar systems.

Airfield Systems Specialist (1B1X6)

Airfield Systems specialists will possess a solid understanding of meteorological, navigational, and air traffic control radio, console, and recorder technologies. They will ensure airfield systems meet all national airspace system certification requirements. Although their focus will be airfield systems, they will possess the information transport and networking skills necessary to integrate these systems into the global information grid. They will deploy in teams to integrate, manage, and sustain air traffic operations.

Cable/Antenna Systems Specialist (1B1X7)

Cable/Antenna Systems specialists will possess a solid understanding of information systems technologies, protocols, and standards required to link the base campus voice, data, and video networks. Although their focus will primarily be on external communications cables and radio frequency antenna systems, they will also possess the installation and assembly skills for premise wiring and protected distribution systems. They will deploy in teams to integrate, manage, and sustain client information services equipment and devices.

Control Systems Specialist (1B1X8)

Control Systems specialists will possess a solid understanding of industrial monitoring and control systems. They will ensure emergency management systems, distribution management systems, and supervisory control and data acquisition systems meet all national standards and are secured, protected, and updated. Although their focus will be systems controls, they will possess

the information transport and networking skills necessary to integrate these systems into closed networks or the global information grid. They will deploy in teams to integrate, manage, sustain, secure, and defend industrial control systems.

Mission Systems Maintenance (1B1X9)

The Mission Systems Maintainer will perform maintenance on airborne platforms. Primarily, they will maintain, repair, and test aircraft communications, sensor, computer, and electronic systems. They will also test, troubleshoot, isolate malfunctions, and repair aircraft mission systems including radio, audio distribution, switching, data, cryptologic, broadcasting, imaging, computer, radar and network equipment. They will also configure and operate aircraft cryptographic devices and verify configuration of equipment and software while on the ground.

On-Net Operations (1B4X1)

Network Warfare operators or On-Net Operators, provide network attack, defense and exploit capabilities. Honed computer network attack skills, allow them to deliver effects to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. They will exploit systems and will counter hostile attempts to manipulate, degrade or exploit our networks and systems. They will capitalize on human, social software and hardware vulnerabilities to achieve tactical, operational, and strategic objectives. They will deploy in small teams to provide electronic attack, electronic protect, jamming, deception, and theater level spectrum management.

Electronic Warfare Operations (1B4X2)

Cyberwarfare operators will possess a solid understanding of systems and technologies required to integrate and sustain operations across the unbound electromagnetic spectrum. They will possess the skills required to identify, recon, and exploit vulnerabilities to achieve desired affects. They will perform search, intercept, identification, and location of sources radiating electromagnetic energy for purposes of immediate threat recognition and implement electronic protect and electronic attack measures. Although focused on operational spectrum, they will provide guidance on acquisition of radiating and receiving equipment. They will deploy in small teams to provide electronic protect, electronic attack, jamming, deception, and theater level spectrum management.

Appendix C: Officer Cyberspace AFSC Construct

Cyberspace Warfare Officer (17D)

Airborne Cyberspace Warfare Officer (ACWO)

Bomber CWO (12B)

Fighter CWO (12F)

Reconnaissance/Surveillance/Electronic Combat CWO (12R)

Special Operations CWO (12S)

Experimental Test CWO (12E)

Generalist ACWO (12G)

Trainer CWO (12K)

Cyberspace Operator (17D)

Cyberspace Operators provide a broad range of expertise key to successful warfighting operations in the air, space, and cyberspace domains. Key competencies include: network systems operations, including information assurance, computer network defense electronic protection and computer network exploitation and attack; 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. Cyberspace operators plan, design, build, maintain, and operate electronic systems necessary for warfighting operations in and through cyberspace; plan and organize communications acquisition management activities; and perform communications engineering functions. When producing effects within the battlespace environment, these Airmen operate as Cyberspace Warfare Officers.

Airborne Cyberspace Warfare Officer (ACWO)

An officer who is a graduate of today's Specialized Undergraduate Navigator Training (SUNT) who has also completed a follow-on Electronic Warfare Officer (EWO) course is referred to as an Airborne CWO. As the Air Force implements Combat Systems Officer (CSO) training to replace today's SUNT, all CSOs will receive training in basic EW fundamentals. As CWOs, Following SUNT or CSO training, these Airmen will receive advanced cyberspace fundamentals training to expand skills beyond electronic warfare and into full-spectrum cyberspace operations. These officers perform different duties as aircrew members on a variety of aircraft but their specialty centers around the understanding and use of the electromagnetic spectrum (EMS). CWOs are trained to be experts in electronic warfare, but must also be aware of how their missions interact with other cyberspace capabilities. They must possess the ability to not only understand the friendly use of the EMS but also the enemy's. There are many missions that CWOs perform across the full range of military operations to include collecting ELINT/SIGINT/MASINT, countering integrated air defense systems (IADS), suppression of an enemy's air defenses (SEAD), disrupting military command & control (C2) nodes and platform "end-game" self-protection measures. All these functions are required in order to find, fix, track, target, engage and assess (F2T2EA) "anti-access" systems across the entire sequence of the "kill

chain.” While implementation of the 12W construct will require the transformation of some 12X Electronic Warfare Specialties for inclusion as 12Ws (see list below), a separate study will refine recommendations on specific EW AFSCs, by positions, which will convert 12Ws (see paragraph 7.1.4).

Bomber CWO (12B)

A Bomber CWO is any officer who is assigned to either the B-52 or B-1 to perform duties as a CWO or Weapons Systems Officer (WSO) to accomplish combat, training and other assigned missions. The Bomber CWO accomplishes mission planning by analyzing mission tasking, intelligence data and weather information to create a plan to avoid or defeat enemy threats. In flight, the CWO is responsible for monitoring the aircraft’s EW and navigation equipment to maintain situational awareness of enemy threats. If threats are detected, the CWO will direct evasive maneuvers and employ countermeasures to defeat the threat.

Fighter CWO (12F)

A Fighter CWO is any CWO officer assigned to EA-6B and F-15E aircraft to perform duties as either an Electronic Countermeasures Officer (ECMO) or Weapons Systems Officer (WSO) to accomplish combat, training and other assigned missions. The F-15E CWO accomplishes mission planning by analyzing mission tasking, intelligence data and weather information to create a plan to avoid and/or defeat enemy threats in order to deliver kinetic effects. In flight, they are responsible for monitoring the aircraft’s EW and navigation equipment to maintain situational awareness of enemy threats. If threats are detected, they will direct evasive maneuvers and employ countermeasures to defeat the threat. The EA-6B ECMO plans, briefs, and leads complex lethal/non-lethal network attack and defense suppression combat missions in order to garner optimum kinetic/non-kinetic effects. They employ electronic attack/information ops capabilities in both cyberspace and air domains to generate effects primarily against communications and radar systems.

Reconnaissance/Surveillance/Electronic Combat CWO (12R)

An officer who is assigned to RC-135 and EC-130H/J aircraft to perform duties as an CWO to accomplish reconnaissance, surveillance, electronic combat, training and other assigned missions. The RC-135 CWO is responsible for combat EW support to SEAD and jamming aircraft platforms. The CWO acts as a key member of the electronic attack package providing real-time, direct targeting information. They also execute signals and signature collection and mission reporting for strategic and operational forces. An EC-130H CWO is responsible for planning, coordinating and executing counter-information and electronic attack missions. They employ electronic attack/information ops capabilities in both cyberspace and air domains to deny enemy communications and radar systems. The EC-130J CWO is responsible for coordination and employment of the aircraft’s special mission equipment for the offensive use of the electromagnetic spectrum. They are also charged with aircraft defense through proper mission planning and use of on and off board systems.

Special Operations CWO (12S)

An officer who is assigned to AC-130H/U and MC-130E/H aircraft to perform duties as an CWO to accomplish special operations, training and other assigned missions. The Special Operations CWO accomplishes mission planning by analyzing mission tasking, intelligence data and weather information to create a plan to avoid and/or defeat enemy threats. In flight, the CWO is responsible for monitoring the aircraft's EW and navigation equipment to maintain situational awareness of enemy threats. If threats are detected, the CWO will direct evasive maneuvers and employ countermeasures to defeat the threat.

Experimental Test CWO (12E)

A cyber-trained graduate of Air Force Test Pilot School, Experimental Test Navigator Course or US Navy or foreign test navigator course whose primary job is conducting flight tests. Systematically plans, directs and reports on the design development and modification of aircraft, aerospace vehicles, flight simulators and related systems. They also identify design and operational deficiencies and manage research, test and evaluation projects.

Generalist ACWO (12G)

Initially qualified in another airborne CWO AFSC, this officer performs staff functions for EW and Cyberwarfare programs and issues. Duties include developing plans and policies, monitoring and evaluating operations and coordinating staff activities. Also develops requirements for equipment and training, prepares and coordinates budgets and analyzes manpower requirements and formulates personnel policies.

Trainer CWO (12K)

Initially qualified in another airborne CWO AFSC, this officer conducts and supervises training of students in EW and navigation. Trainers ensure optimum training opportunities by reviewing syllabus requirements and student progress. They also develop plans and policies, monitor operations and advise commanders on training activities.

Appendix D: Cyberspace Training and Education Construct

1B0XX and 1B1XX AFSC-Awarding (Pipeline) Courses

The 1B0 and 1B1 AFSs will take advantage of the current C&I Transformation construct of migrating the 2EX, 3AX, and 3CX AFSs to a new AF career field. Current skill sets will be repurposed to align with core cyberspace competencies. Most will be accession-level AFSCs, while a few may be retrain-in only. Utilization & Training Workshops (U&TWs) will be conducted in FY08/09 to refine each new AFSC and identify training tasks required to produce a cyberspace workforce. AETC will produce Course Resource Estimates (CREs) based on U&TW results. Where possible, resources (instructors, student man-years, equipment, facilities, and O&M) currently supporting the 2E, 3A, and 3C AFSC-awarding and supplemental courses will be used as offsets to bring the new courses online. Additional resources (especially course developers, instructors, and student man-years) will be needed. Some of the current 2E, 3A, and 3C pipeline student flow may need to be reduced or terminated for a period of time while equipment is moved and new courses developed. Timelines will be established to stand down the current pipelines and bring the new pipelines online in the most cost effective manner.

1B4XX AFSC-Awarding (Pipeline) Courses

The 1B4X1 On-Net Operator and 1B4X2 Electronic Warfare Operator are new AFSCs supporting bound/wired and unbound/wireless cyberspace warfare capabilities. Knowledge critical to these AFSCs will be used to protect and defend our networks, as well as attack enemy cyberspace capabilities. Airmen will be screened around the 3-5 year time frame for aptitude and proficiencies and if accepted, will be targeted for retraining as a 1B4. These are retrain-in only AFSCs and will be drawn from strong cyberspace foundations developed in specific 1B0 and 1B1 Specialties. Initial knowledge, skills, and abilities (KSAs) to support these two AFSCs were identified to create a Rough Order Magnitude (ROM) of costs to develop, conduct and sustain these pipeline courses through the FYDP. The ROM costs will be included in the AETC FY10 POM submission. U&TWs will be conducted in FY08/09 to refine the required training tasks for each new AFSC. AETC will produce CREs based on U&TW results to fine tune the FY10 POM submission. Timelines will be established to bring these new pipelines online in the most cost effective manner.

1B4XX Transition Courses

While new accessions into the cyberspace warfare career field will receive their IQT in AFSC awarding courses, many of the individuals transitioning from an existing AFSC to a new AFSC will need some amount of retraining. Core cyberspace fundamentals differ enough from existing training that some form of distributed learning, targeted Career Development Courses or mobile education teams may be necessary to prepare the existing force to operate in tomorrow's domain.

Cyberspace 100/200/300/400 Courses

Cyber 100 is an introductory Cyberspace Fundamentals course common to both the 17D and rated 12W AFSC-awarding course paths. While Cyberspace 100 completes AFSC-awarding training for the rated CWO, it is also the foundational training for the 17D CWO. Initial training task requirements for all were identified to create a ROM of costs to develop, conduct and sustain the course through the FYDP. The ROM costs will be included in an AETC FY10 POM submission. Cyberspace 200, 300 and 400 courses are advanced officer courses. Current 33SX advanced and supplemental course resources will be used as offsets to bring these three courses online. U&TWs will be conducted in FY08/09 to refine required training tasks. AETC will produce CREs based on U&TW results to fine tune the FY10 POM submission. Timelines will be established to bring these new courses online in the most cost effective manner. These courses may also form the baseline of requirements necessary to ensure other AFSCs (14N, 13S, 62E, etc.) are qualified for roles in cyberspace organizations or missions.

17D Undergraduate Cyberspace Warfare Training (UCWT)

The UCWT course is the AFSC-awarding course for the 17D Cyberspace Warfare Officer and will follow the Cyberspace 100/Fundamentals course. Initial training task requirements for this course were identified to create a ROM of costs to develop, conduct and sustain the course through the FYDP. The ROM costs will be included in AETC's FY10 POM submission. The current 33SX Basic Computer Officer Training course resources will be used as offsets to bring the Basic Cyberspace Warfare Officer course online. U&TWs will be conducted in FY08/09 to firm up total force numbers and required training tasks. AETC will produce a CRE based on U&TW results to fine tune the FY10 POM submission. Timelines will be established to bring this new course online in the most cost effective manner.

17D and 12W Transition Courses

While new accessions into the cyberspace warfare career field will receive their IQT in AFSC awarding courses, many of the individuals transitioning from an existing AFSC to a new AFSC will need some amount of retraining. Much of this retraining may take place through FTUs as individuals move into assignments in cyberspace warfare units; however, some core cyberspace fundamentals differ enough from existing training that some form of distributed learning or cyberspace education teams may be necessary to prepare the existing force to operate in tomorrow's domain.

Formal Training Units (FTUs)

FTUs, as required, will provide the final initial training needed by the cyberspace career field to achieve initial qualification training status. They will provide both initial skill training to new accessions to a career field, as well as retraining for individuals transitioning from one cyberspace warfare arena to another as they move between assignments. While the final force structure and employment plan will drive the creation of specific FTUs in addition to the already established aircrew FTUs, examples include:

UNCLASSIFIED – FOR OFFICIAL USE ONLY

- Garrison Communications FTU – this FTU will provide the training needed by officers destined for fixed base communications organizations
- Network Attack FTU – this FTU will provide the training needed by individuals destined for cyberspace attack organizations
- Network Defense FTU – this FTU will provide the training needed by individuals destined for cyberspace defense organizations

Cyber Weapons School

The mission of the United States Air Force Weapons School under the USAF Warfare Center is to teach graduate-level instructor courses, which provide the world's most advanced training in weapons and tactics employment to Air Force officers. Cyberspace warfare officers (CWO) will require advanced Weapons Instructor Courses (WICs) to provide a core AF expertise that advances tactics employment of cyberspace systems/capabilities and integration with their counterpart expertise in air and space systems. Airborne cyberspace warfare officers already have WICs (e.g. Compass Call, Rivet Joint and Bomber EWOs). A WIC for non-airborne cyberspace warfare officers (e.g. those trained on network warfare systems) will require development and implementation. IAW AFI 11-415, the USAFWC, AFIOC, and 67 NWW (in concert with ACC/A3T) must plan, develop and implement a WIC for CWOs conducting network warfare operations, and leverage/synchronize with existing airborne CWO WICs to provide an integrated cyberspace focus to the Weapons School and Combat Air Forces no later than FY11.

Continuing Education and Training

Training and education require a strong commitment from leaders at all levels. Cyberspace is inherently a technological domain, whose “terrain” changes constantly as new technologies evolve and networks evolve. The speed at which technology advances imposes an operational shelf-life for most technology skills. Keeping the cyberspace sword sharp requires recurring training programs, periodic certifications (or recertification) in the newest technologies and realistic exercises. In this new era of cyberspace warfare, life-long learning is paramount.

Education provides the foundation for conducting effective cyberspace operations. Education is necessary to move Cyberspace Professionals beyond the tactical and technical focus of their day-to-day jobs and to assure the requisite level of skills and abilities necessary to sustain the cyberspace mission. Cyberspace education goes beyond individual service requirements and encompasses all organizations within the national security cyberspace environment.

The Air Force intends to redefine airpower, which requires changing the Air Force culture. This will necessitate an extensive review of our current education programs covering air and space power. Simply inserting new material on cyberspace power will not suffice, nor will replacing “air and space” with “air, space, and cyber”. Cyberspace should not be viewed as a detractor from kinetic capabilities, but as an enabler and provider of new capabilities. Cyberspace supports air, and vice versa.

UNCLASSIFIED – FOR OFFICIAL USE ONLY

Not everyone needs a comprehensive grounding in cyberspace operations, but every Airman should have a general understanding of Air Force capabilities in this domain. Every Airman should understand that cyberspace is a domain in which we have peer competitors (nation states and trans-national actors) who are continually probing and attacking US systems, and that every Airman has a role in defending our cyberspace capabilities.

Our developmental education (DE) programs must evolve to help us grow leaders who understand how cyberspace operations integrate with conventional kinetic operations. Future leaders must understand how cyberspace and kinetic effects can be integrated at the joint and operational levels, how to plan and execute cyberspace operations within our Air Operations Center construct, and how to assess the effectiveness of these operations.

An initial list of cyberspace competencies have been developed through extensive collaboration with cyberspace subject matter experts in the operational, academic, and doctrine communities. The topical areas are nature and characteristics of the domain; cyberspace capabilities and functions; integration of cyberspace with kinetic effects; employment of cyberspace capabilities; and law, policy, and ethics.

The proposed cyberspace competencies can be used by curriculum developers at all levels of DE to assess their programs and begin modifying their curricula as necessary. However, we recognize that current programs are “full” and adding/revising content to address cyberspace operations is difficult without guidance and prioritization.

The Air Force Basic Doctrine (AFDD 1-1), Institutional Competencies List is the guiding document to drive DE curricula. AF/A1D, utilizing the ICL, will provide guidance on how best to prioritize and integrate cyberspace material into the existing DE programs.