CYBERSPACE INTEGRATION WITHIN THE AIR OPERATIONS CENTER

GRADUATE RESEARCH PROJECT

Bradley A. Rueter, Major, USAF

AFIT-ENG-GRP-13-J-02

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

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

AFIT-ENG-GRP-13-J-02

CYBERSPACE INTEGRATION WITHIN THE AIR OPERATIONS CENTER

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Warfare

Bradley A. Rueter

Major, USAF

May 2013

AFIT-ENG-GRP-13-J-02

CYBERSPACE INTEGRATION WITHIN THE AIR OPERATIONS CENTER

Bradley A. Rueter

Major, USAF

Approved:

Robert J Mills

Robert Mills, PhD (Chairman)

22 MAY 2013

Date

Jonathan Butts, PhD (Member)

22 May 2013

Date

AFIT-ENG-GRP-13-J-02

Abstract

The Air and Space Operations Center (AOC) is the United States Air Force's operational command and control (C2) platform for the planning and execution of Air, Space, and Cyber operations. Operational C2 of cyber forces is a significant challenge that impacts the planning and integration of cyber operations at the AOC. The Joint Staff's Transitional Cyberspace C2 Concept of Operations, released in March 2012, provides a cyber C2 framework at the Geographical and Functional Combatant Command level, but it is not clear yet how Air Force AOCs will work together to meet the requirements of the CONOPS or conduct cyber planning to support the needs of the Joint Force Air Component Commander. This paper summarizes the results of a mission analysis to identify the roles and responsibilities for cyber operations within the AOC, separating them from traditional J6/A6 responsibilities. Additionally, the Joint Staff CONOPS calls for significant "reach back" for planning, expertise, and potential execution of cyber capabilities; as such, the paper provides a discussion on how to facilitate globally linked, interoperable AOCs for cyber planning and execution.

Acknowledgments

Many individuals have greatly contributed to the development of this topic, and I sincerely appreciate their time and effort in reviewing the problem and offering their unique insights. My advisor, Dr. Mills, my former bosses, Col Lehman and Col Marker, as well as the 24AF/A3, 624OC Commander, and USAFCENT/DIRCYBERFOR all invested significant time and energy in discussing the various challenges and virtues of different organizations and organizational structures. My greatest thanks to each for their help.

Table of Contents

List of Figures

Figure Page

List of Tables

List of Acronyms

624OC	624th Operations Center
AFDD	Air Force Doctrine Document
AFFOR	Air Force Forces
AFI	Air Force Instruction
AFNet	Air Force Network
AFTTP	Air Force Tactics, Techniques and Procedures
AOC	Air Operations Center
AOR	Area of Responsibility
ATO	Air Tasking Order
C2	Command and Control
CCMD	Combatant Command
C-NAF	Component Numbered Air Force
COLE	Cyber Operations Liaison Element
COMAFFOR	Commander of Air Force Forces
CONOPS	Concept of Operations
CONPLAN	Concept of Operations Plan
COT	Cyber Operations Team
CSE	Cyber Support Element
DCO	Defensive Cyber Operations
DCO-TC	Defensive Cyber Operations - Tactical Coordinator
DIRCYBERFOR	Director of Cyber Forces
DIRMOBFOR	Director of Mobility Forces
DIRSPACEFOR	Director of Space Forces
DoD	Department of Defense
exCSE	Expeditionary Cyber Support Element
GIG	Global Information Grid
I-NOSC	Integrated Network Operations and Security Center
IO	Information Operations
IOT	Information Operations Team
ISRD	Intelligence, Surveillance, Reconnaissance Division
JCC	Joint Cyber Center
JFACC	Joint Forces Air Component Commander
JFC	Joint Force Commander
JIPTL	Joint Integrated Prioritized Target List
JPG	Joint Planning Group
NCC	Network Control Center
NDWG	Network Defense Working Group
NKOCC	Non-kinetic Operations Coordination Cell
NOSC	Network Operations and Security Center
OCO	Offensive Cyber Operations
OPLAN	Operations Plan

TTP	Tactics, Techniques and Procedures
USAF	United States Air Force
WIC	Weapons Instructor Course

Cyberspace Integration within the Air Operations Center

I. Introduction

The motivation for this research stemmed from personal experience as an operational level planner that struggled with how to integrate and synchronize cyber effects into a plan, and subsequently provide command and control during execution. This problem became more apparent and more concerning as the notion of network defense became a greater operational concern. This research endeavors to understand the full gamut of requirements levied on Component - Numbered Air Forces in terms of cyber, and provide recommendations to deal with those requirements. A methodical publication review was conducted to identify the Joint and Service requirements for cyber operations, as well as the latest organizational constructs prescribed at various levels.

This analysis provides the current command and control relationships and cyber integration constructs in the United States Air Force (USAF), presenting the relevant organizations within the Component Numbered Air Forces (C-NAF), the Combatant Commands, and USCYBERCOM. Following the situation is a section dedicated to exploring the requirements that have been levied on the C-NAF with regards to cyber. Additionally, the Air Operations Center's (AOC) internal processes are explored, to examine how cyber operations is integrated and synchronized with other effects, and ensure that critical AF-centric requirements are met. Finally, the last section provides a series of recommendations about how different organizations can be structured in order to meet the cyber-related requirements and build synergy amongst the AOCs. Specific recommendations for the C-NAF, AOC, and Cyber Operations Team are included, as well as recommendations to facilitate reach-back support to 24th Air Force.

This research is limited to the operational aspects of cyber, and does not address the infrastructure and engineering aspects of the domain. Additionally, it is assumed that the Joint Staff's Transitional Cyberspace Operations Command and Control Concept of Operations, or a very similar structure, will be upheld after the year-long trail and information gathering.

II. Situation

Since cyberspace was declared a unique and separate domain in March 2005 the Department of Defense (DoD) has continued to refine what cyber operations are, what effects they can generate, and how to synchronize those effects within the larger scheme of maneuver [1]. Much progress has been made thus far at the strategic and tactical levels of war, leaving organizations at the operational level struggling to define, deconflict, and institutionalize new roles and responsibilities. The Joint Staff, USSTRATCOM, and USCYBERCOM have spent significant time formalizing the presentation of cyber forces to include the necessarily complex global and regional command and control (C2) schemas required to have timely regional effects but also ensure global deconfliction [3]. Additionally, at the tactical level, cyber forces have made great strides in the development and fielding of various capabilities, the documentation and refinement of Tactics, Techniques and Procedures (TTP), and for the USAF, integration with air assets in exercises and the Weapons Instructor Course (WIC) [4].

2.1 Component – Numbered Air Forces

Despite these advances, operational organizations, such as the C-NAFs, are struggling with general roles and responsibilities, to include the planning, integration, deconfliction, and operational C2 of cyber effects. As articulated in the Joint Staff Transitional Cyberspace Operations Command and Control Concept of Operations, Combatant Commands (CCMD) are expected to have situational awareness of their networks, in order to coordinate network defense and coordinate offensive cyber operations [5]. To do this, CCMDs require information from their components, so that sensor data can be aggregated to produce Area of Responsibility (AOR) wide situational awareness. Additionally, most defensive cyber operations must be standardized and coordinated so that offensive operations are properly deconflicted with other units, agencies and departments. The Component staffs have a responsibility to the tactical level executors and provide the commander's intent, rules of engagement, special instructions, tactical tasks, and generally a feasible plan for the employment of their respective weapon systems. Tactical units expect that operational planners have already integrated cyber into the larger scheme of maneuver, synchronized effects, garnered appropriate authorities, and are prepared to provide operational C2 of cyber forces. With robust expectations from the strategic level (above) and from the tactical level (below), the C-NAFs must take significant steps to mitigate the current gaps.

A fundamental challenge for the C-NAF Commanders is that they typically wear multiple hats, as the Commander of Air Force Forces (COMAFFOR) and (usually) Joint Forces Air Component Commander (JFACC). As such, they have multiple staffs, and there are many competing equities and confused/unclear responsibilities related to cyber C2 and planning.

With the COMAFFOR hat, the commander is responsible for the sustainment of Air Force forces, generally thought of as "beds, beans, and bullets" which are critical to the successful accomplishment of operational missions. The COMAFFOR requires C2 nodes to assist in exercising command authorities, and when it comes to Service responsibilities (like sustainment) the AFFOR staff exercises operational and administrative control. The AFFOR staff's function is to support and assist the

COMAFFOR in preparing the Air Force component to carry out the functions and tasks assigned by the Joint Force Commander (JFC), and through which the COMAFFOR fulfills his/her operational and administrative responsibilities for assigned and attached forces, and is responsible for the long-range planning and theater engagement operations that occur outside the air tasking cycle (e.g., deliberate planning) [6]. Admittedly, all Directorates have equities in cyber, especially in the broader sense of information technology, computer networking, communications, etc. However, only a few Directorates are interested in cyber operations in terms of creating effects, and these are discussed below in order to distinguish them from the AOC functions and equities.

Within the AFFOR staff, the Intelligence Directorate (A2) has a responsibility to report on enemy actions in all domains, including cyberspace. The evolution of adversary tactics, techniques, and procedures is of particular interest to the commander and may have a direct impact on network defense. The assessment of likely enemy courses of action will also inform the development of active defense options and countermeasures available to network defense operators. The Operations Directorate (A3) is interested in anything effecting current operations, to include events in cyberspace that have a physical effect in another domain, or effects that occur solely in cyberspace. The A3 wants to have situational awareness on these types of cyber-effects but conversely is not concerned, for example, with the engineering and management of the network infrastructure. With regards to Cyber Operations, the A3 has inherent equities as these operations are trying to achieve an effect in some domain, and thus the A3 ensures they meet commander’s intent, are properly deconflicted, and properly synchronized with other efforts. The division of responsibilities between A3 and A6 for

Cyber Operations is not clearly articulated in any doctrine, and left to each organization. The Plans and Requirements Directorate (A5) has cyber equities primarily in the role of exercise participation and long range plan development. The A5 needs cyber planners to incorporate cyber effects into operational and conceptual plans as well as exercises to utilize all available AF capabilities and to exercise the C2 of these capabilities.

The AFFOR Communications Directorate (A6) is the principal staff assistant to the COMAFFOR for communications, electronics and information capabilities. This includes establishing the theater communications and automated systems architecture to support operational and command requirements [6]. The AFFOR/A6 is generally responsible for the communications infrastructure, engineering, installation, and maintenance of computer networks, which could also include a Network Operations and Security Center (NOSC), and many other functions beyond the scope of this analysis. With the consolidation and centralization of most USAF NOSCs into Integrated NOSC (I-NOSCs) most C-NAFs will not have their own NOSC, but will rely on the assigned I-NOSC for day-to-day network operations and security [7]. In general, the AFFOR staff must develop a habitual working relationship with the AOC to fulfill the COMAFFOR's full range of responsibilities and to integrate staff efforts with the AOC battle rhythm, this holds particularly true for cyber as well [6].

The COMAFFOR normally uses some form of an AOC to exercise control of operations and to plan, direct, and assess the activities of assigned and attached forces [6]. The AOC provides operational-level C2 of air, space, and cyberspace operations, and is the focal point for planning, directing, and assessing air, space, and cyberspace operations to meet JFACC operational objectives and guidance [8]. With regards to cyber operations, the AOC is primarily focused on integrating and synchronizing offensive cyber effects with other effects to achieve military objectives. The AOC is uniquely suited to do this planning and integration, but a significant challenge is a lack of knowledgeable operational planners who understand how to plan and integrate cyber effects into the larger scheme of maneuver.

2.2 Strategic Guidance

Thus far, the discussed cyber equities have been largely Air Force specific, but the Joint Staff Transitional Cyberspace Operations Command and Control Concept of Operations (CONOPS) introduces several additional organizations that must be addressed. This CONOP mandated each CCMD establish a Joint Cyber Center (JCC) within their staff organization. Each JCC is the focal point for cyber command, planning, operations, intelligence, targeting, and readiness for each CCMD. The Joint Staff CONOPS also makes it clear that "providing all cyber support forward in CCMDs [AOR] is neither feasible nor desirable" and that many cyber capabilities would be provided solely through reach-back. Finally, some capabilities supporting synchronization must be forward deployed [5].

The CONOPS also introduces the Cyber Support Element (CSE) construct that is designed to be the USCYBERCOM liaisons to the CCMD. As required, the CSE would deploy to and be collocated with the JCC. The JCC would continue to represent the Geographic Combatant Commander, as the supported commander and the CSE would leverage their expertise and USCYBERCOM reach-back to support the Commander's objectives. This organization is shown in Figure 1 [5].

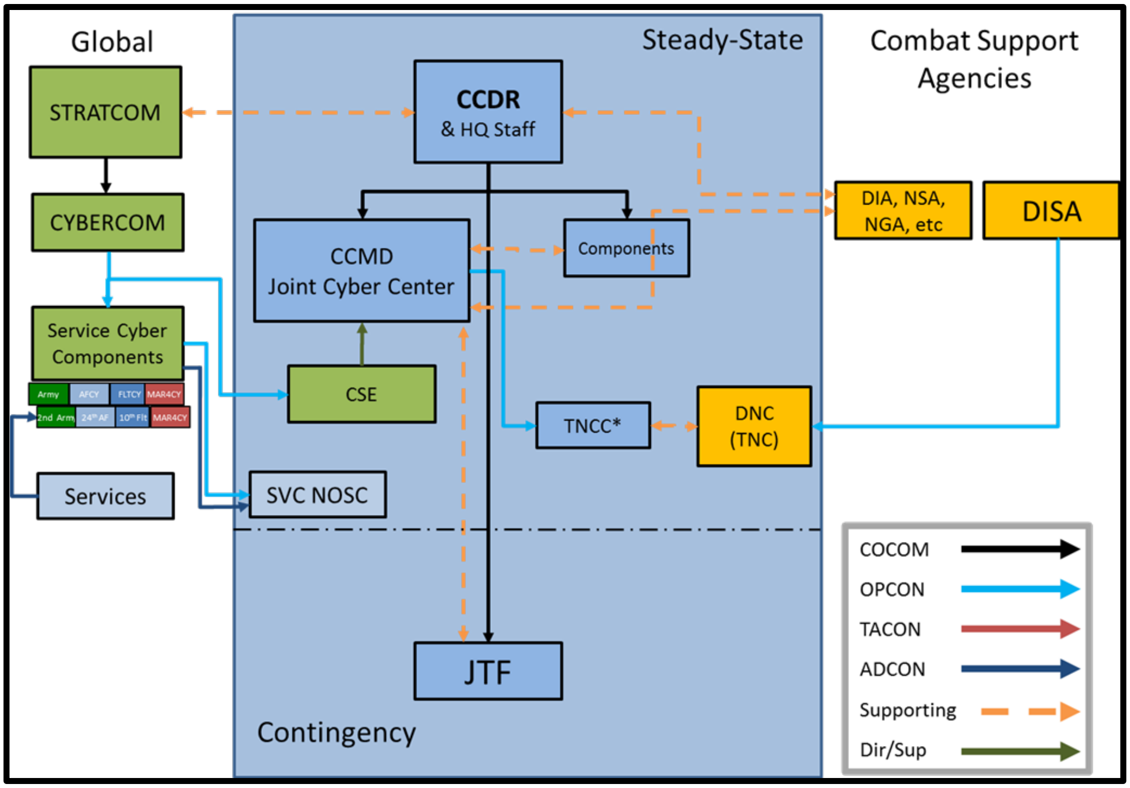


Figure 1: Strategic Cyber C2 [4]

Ostensibly, this arrangement would have no impact on the C-NAF, as the AFFOR and AOC cyber personnel would continue to work with the JCC as normal. However, each CCMD is different, and effects-integration and deconfliction may be delegated to a Component. USCYBERCOM has also developed a team called the Expeditionary Cyber Support Element (exCSE) which is meant to augment the CCMD Components at their respective C2 nodes or headquarters. The exCSE is subordinate to the CSE and is also comprised of USCYBERCOM personnel. This has particular impact for AOCs, because the JFACC is likely to be the lead effects integrator, or at the least has sufficient equities to warrant an exCSE. The AOC must understand what the exCSE is, what it can provide, what it is not, and must be prepared to share the same spaces with these liaisons.

It is important to note the difference between augmentees and liaisons in terms of AOC manpower. Augmentees are additional personnel that are assigned to the AOC, and ultimately work for the JFACC. They bring special knowledge or skills to the AOC team whenever needed. Liaisons are representatives of other component commanders and do not work for the JFACC [9]. Liaisons are an integral part of an AOC, but their marching orders ultimately come from someone other than AOC leadership. The CSE, to include the exCSE, are liaisons to the CCMD and its components respectively and thus should not be considered the primary cyber planners. The AOC should have organic cyber planners with whom the exCSE is liaising.

2.3 AFCYBER

Because cyberspace is global, all other C-NAFs must understand and work with AFCYBER/24AF, which is the USAF component to USCYBERCOM. AFCYBER is generally expected to prepare for “full-spectrum military cyberspace operations” which breaks down to three Lines of Operation: DOD-Global Information Grid (GIG) operations, defensive cyberspace operations (DCO) and offensive cyber operations (OCO). On the defensive side, AFCYBER is tasked to support the CCMD with reach-back support by directing and enabling operations and defense of the CCMD and subordinate DOD GIG networks, to recommend and enable local network access and defense actions, assist with local compliant measures, monitor CCMD and subordinate network events, and finally coordinate cyberspace defense among the CCMD, its components and external support elements [5].

One of AFCYBER's responsibilities is defending the USAF portion of the DOD's networks, which parallels the responsibilities of the AFFOR/A6 as discussed above. From a service perspective, the 24AF must also defend the AFNet, the Air Force provisioned portion of the GIG, which is the global connectivity and services that enable Air Force commanders to "achieve information and decision superiority" in pursuit of strategic, operational, and tactical objectives [10]. Of the three Lines of Operation detailed in the Joint Staff CONOPS, each requires specific information from the C-NAF to ensure the AFNet is providing and prioritizing the proper services (mission assurance), that the network's defense posture is responsive to the current threat, and that offensive operations meet the objectives of the Joint Force Commander and JFACC. While AFCYBER/24AF has these tasks, the regional C-NAF has a significant responsibility in providing the operational and regional context to AFCYBER/24AF, without which the AFCYBER/24AF forces are making the best decisions they can and generally without the context that the mission owner has.

The 24AF has an AOC C2 node, called the 624th Operations Center (624OC) which executes C2 for the subordinate wings and specifically the aforementioned I-NOSCs (Figure 2) [11]. The 624OC and the regional AOCs perform almost identical functions for their respective AORs. The 624OC follows the same ATO process as other AOCs and has the same organizational structure, which should facilitate cross communication. To enable communication, the regional AOCs can request a Cyber Operations Liaison Element (COLE), provided by AFCYBER/24AF, to work within the regional AOC to provide cyber planning and operations expertise and serve as the 24th AF Commander's and the 624OC's senior representatives in theater [11] [8]. It is unclear at this time whether the COLE is viable considering USCYBERCOM's exCSE construct which seems to create redundancy.

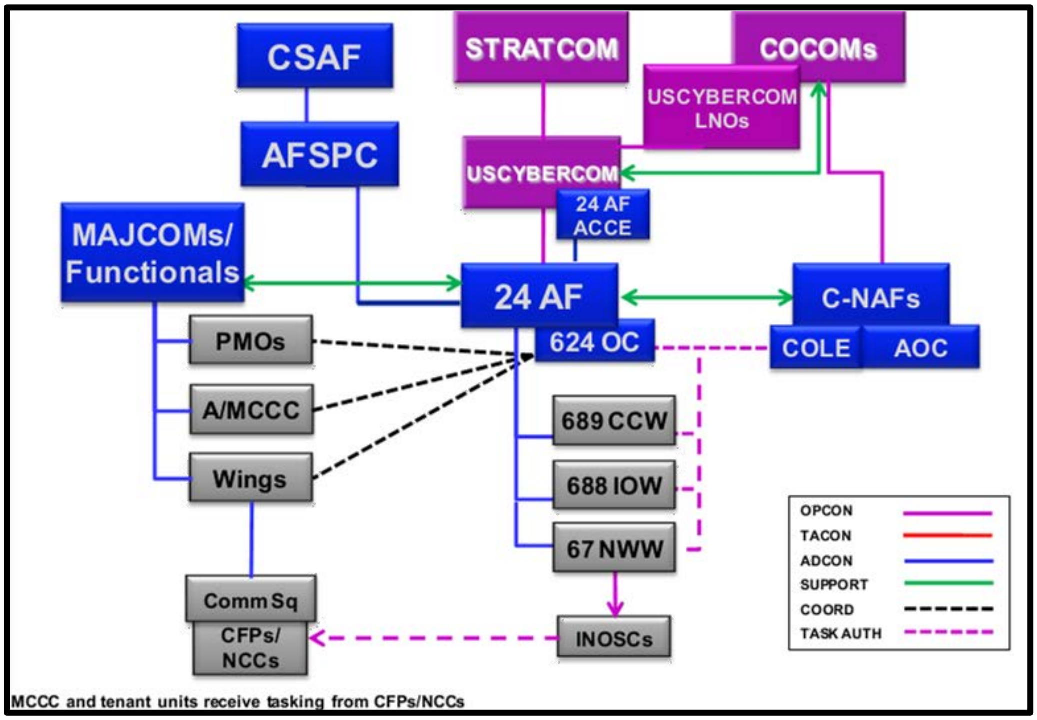


Figure 2: 24AF Command and Control [10]

In summary, there are many different organizations with substantive cyber equities that must be included in order for the AOC to meet the JFACC's objectives. At the operational level, the AOC must work with its associated AFFOR staff, the 624OC and 24AF planners. At the strategic level, the Combatant Commander's JCC will provide guidance and required inputs. When necessary, USCYBERCOM will deploy their CSE to collocate with the JCC, but may also send an exCSE to work at the AOC. With so many stakeholders, roles and responsibilities must be clearly defined; the requirements for cyber stakeholders will be analyzed next, in hopes of identifying natural seams around which roles and responsibilities can be developed.

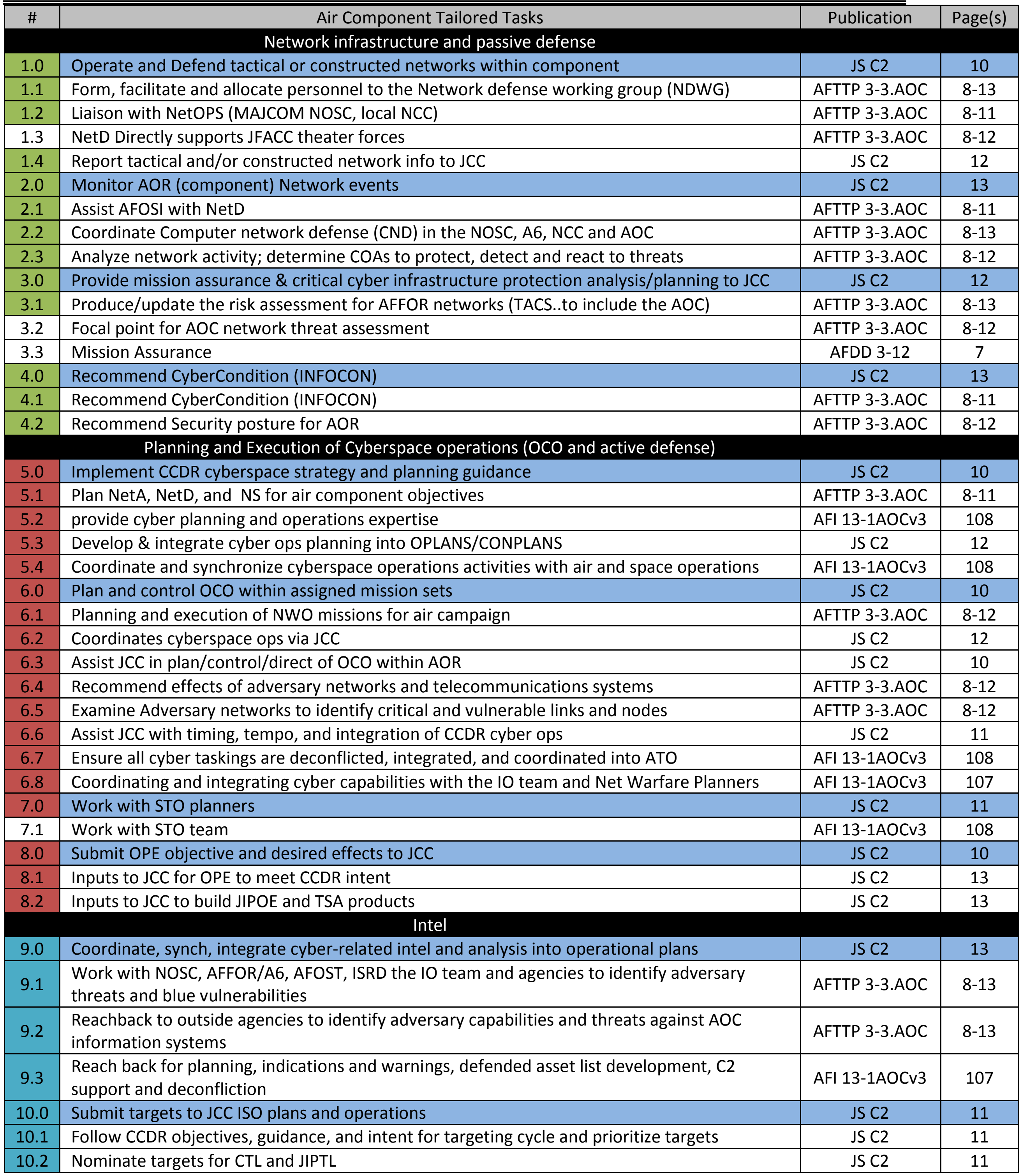
III. Requirements

There are many sources for requirements when it comes to offensive and defensive cyber operations, but in order to maintain focus on the AOC and its role in cyber operations, this study focused on requirements pertinent to the planning and execution of cyber operations. This means that there are many other requirements and regulations that govern the engineering, installation, and maintenance of network infrastructure that are not included herein. In a C-NAF, these infrastructure related tasks fall to the A6, and since this analysis does not include those infrastructure tasks, it may appear that the AFFOR is undertasked, which would be an unfair assessment [6]. The goal is to identify the operational tasks that must be accomplished by the C-NAF and which organizations have equities in those tasks; ultimately identifying roles and responsibilities within the C-NAF.

3.1 Document Review

To accomplish this mission analysis, a document review was conducted on Joint guidance, Air Force Doctrine, Air Force Instructions, Air Force Policy Documents, and Air Force Tactics, Techniques, and Procedures. These tasks are aggregated and distilled into distinct mission areas, and are provided in Table 1. The Joint Staff Transitional Cyberspace Operations C2 CONOPS specifies tasks for USSTRATCOM, USCYBERCOM and its Components, Geographical and Functional CCMDs and their respective Joint Cyber Center.

Table 1: C-NAF Cyber Tasks



#	Air Component Tailored Tasks	Publication	Page(s)
Network infrastructure and passive defense			
1.0	Operate and Defend tactical or constructed networks within component	JS C2	10
1.1	Form, facilitate and allocate personnel to the Network defense working group (NDWG)	AFTTP 3-3.AOC	8-13
1.2	Liaison with NetOPS (MAJCOM NOSC, local NCC)	AFTTP 3-3.AOC	8-11
1.3	NetD Directly supports JFACC theater forces	AFTTP 3-3.AOC	8-12
1.4	Report tactical and/or constructed network info to JCC	JS C2	12
2.0	Monitor AOR (component) Network events	JS C2	13
2.1	Assist AFOSI with NetD	AFTTP 3-3.AOC	8-11
2.2	Coordinate Computer network defense (CND) in the NOSC, A6, NCC and AOC	AFTTP 3-3.AOC	8-13
2.3	Analyze network activity; determine COAs to protect, detect and react to threats	AFTTP 3-3.AOC	8-12
3.0	Provide mission assurance & critical cyber infrastructure protection analysis/planning to JCC	JS C2	12
3.1	Produce/update the risk assessment for AFFOR networks (TACS..to include the AOC)	AFTTP 3-3.AOC	8-13
3.2	Focal point for AOC network threat assessment	AFTTP 3-3.AOC	8-12
3.3	Mission Assurance	AFDD 3-12	7
4.0	Recommend CyberCondition (INFOCON)	JS C2	13
4.1	Recommend CyberCondition (INFOCON)	AFTTP 3-3.AOC	8-11
4.2	Recommend Security posture for AOR	AFTTP 3-3.AOC	8-12
Planning and Execution of Cyberspace operations (OCO and active defense)			
5.0	Implement CCDR cyberspace strategy and planning guidance	JS C2	10
5.1	Plan NetA, NetD, and NS for air component objectives	AFTTP 3-3.AOC	8-11
5.2	provide cyber planning and operations expertise	AFI 13-1AOCv3	108
5.3	Develop & integrate cyber ops planning into OPLANS/CONPLANS	JS C2	12
5.4	Coordinate and synchronize cyberspace operations activities with air and space operations	AFI 13-1AOCv3	108
6.0	Plan and control OCO within assigned mission sets	JS C2	10
6.1	Planning and execution of NWO missions for air campaign	AFTTP 3-3.AOC	8-12
6.2	Coordinates cyberspace ops via JCC	JS C2	12
6.3	Assist JCC in plan/control/direct of OCO within AOR	JS C2	10
6.4	Recommend effects of adversary networks and telecommunications systems	AFTTP 3-3.AOC	8-12
6.5	Examine Adversary networks to identify critical and vulnerable links and nodes	AFTTP 3-3.AOC	8-12
6.6	Assist JCC with timing, tempo, and integration of CCDR cyber ops	JS C2	11
6.7	Ensure all cyber taskings are deconflicted, integrated, and coordinated into ATO	AFI 13-1AOCv3	108
6.8	Coordinating and integrating cyber capabilities with the IO team and Net Warfare Planners	AFI 13-1AOCv3	107
7.0	Work with STO planners	JS C2	11
7.1	Work with STO team	AFI 13-1AOCv3	108
8.0	Submit OPE objective and desired effects to JCC	JS C2	10
8.1	Inputs to JCC for OPE to meet CCDR intent	JS C2	13
8.2	Inputs to JCC to build JIPOE and TSA products	JS C2	13
Intel			
9.0	Coordinate, synch, integrate cyber-related intel and analysis into operational plans	JS C2	13
9.1	Work with NOSC, AFFOR/A6, AFOST, ISRD the IO team and agencies to identify adversary threats and blue vulnerabilities	AFTTP 3-3.AOC	8-13
9.2	Reachback to outside agencies to identify adversary capabilities and threats against AOC information systems	AFTTP 3-3.AOC	8-13
9.3	Reach back for planning, indications and warnings, defended asset list development, C2 support and deconfliction	AFI 13-1AOCv3	107
10.0	Submit targets to JCC ISO plans and operations	JS C2	11
10.1	Follow CCDR objectives, guidance, and intent for targeting cycle and prioritize targets	JS C2	11
10.2	Nominate targets for CTL and JIPTL	JS C2	11

The Air Force's overarching doctrine for cyberspace operations is encapsulated in AF Doctrine Document (AFDD) 3-12, which highlights that cyberspace operations are "not synonymous with information operations (IO)" but that cyberspace can directly support IO; this is a key consideration in defining roles and responsibilities inside a C-NAF. As previously described, the Joint Staff C2 CONOPS and AF Policy Directive 13-3 tasks AFCYBER/24AF with mission assurance responsibilities for the AFNet, but AFCYBER/24AF cannot provide mission assurance alone. The mission owner (the AOC, AFFOR Directorate, weapon system, etc.) must prioritize essential functions, map these missions and their dependencies against cyberspace, and thereby identify the associated vulnerabilities and potential mitigation strategies [12].

Finally, per AFI 13-1AOC volume 3, the AOC is required to provide cyber planning and operations expertise in order to coordinate and synchronize cyberspace operations activities with other domains, to include the IO Team. The regional AOC is tasked to reach-back to 624OC for planning, indications and warnings, defended asset list development and C2 support and deconfliction. Additionally, the AOC is charged with communicating Joint Force Commander's requirements to 24AF and the 624OC. Finally, the AOC shall ensure all cyber tasking are deconflicted, integrated and coordinated into the Air Tasking Order (ATO).

These tasks are numbered according to the functional area where 1.0, 1.1, 1.2, etc., are all similar tasks from different sources, by grouping these tasks in this manner, the number of minimum essential tasks that the C-NAF must handle becomes more manageable. The network infrastructure and passive defense section includes requirements to operate and defend tactical and constructed networks. The planning and execution of cyberspace operations includes active defense, Concept of Operations Plan (CONPLAN)/ Operation Plan (OPLAN) integration, and Operational Preparation of the Environment development. The intelligence section includes tasks that assess threats and enemy capabilities, and process cyber-related targets.

3.2 Operational Task Views

These tasks are then mapped on a communication flow diagram (Figure 3) to describe which organizations the C-NAF must work with, and what tasks/data must be provided. The tasks inside the AF Component box, which includes the AOC and AFFOR Staff, are processes and products that remain internal to the C-NAF, although the specific roles and responsibilities within the C-NAF are not yet defined. Also, within the AF Component block are the liaisons, to include the exCSE, which are noteworthy because they will likely assist in many of these reporting functions.

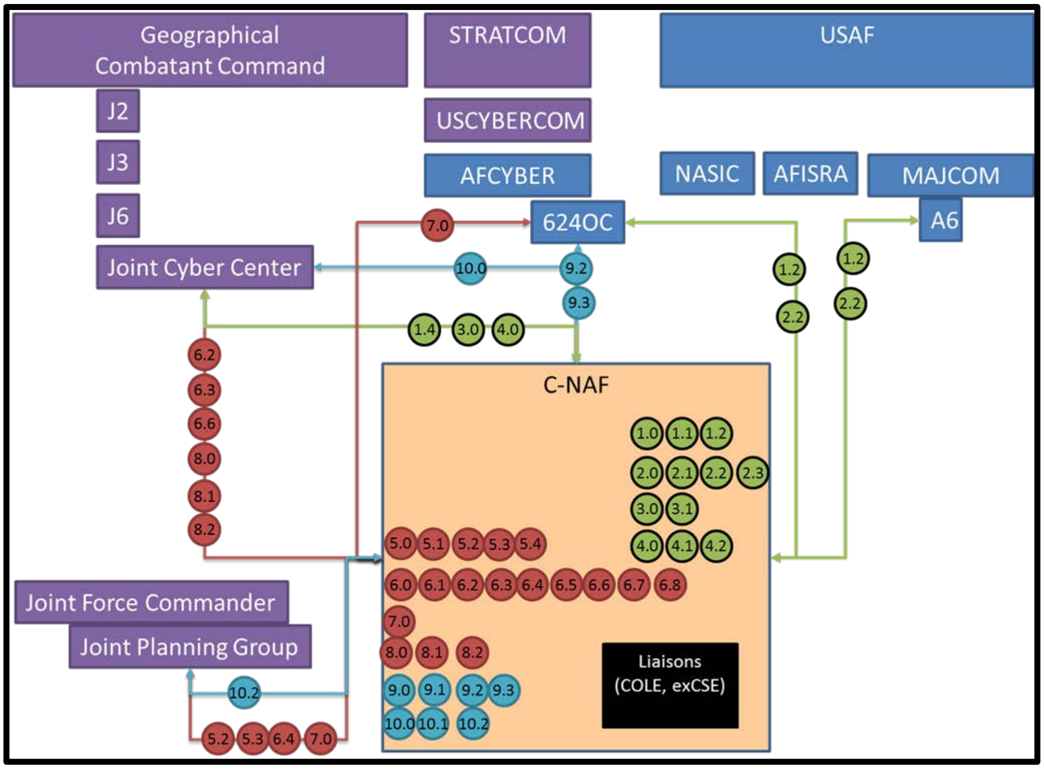


Figure 3: Operational Task view (top)

The next level in the operational task view is focused on the roles and responsibilities within the AF Component (Figure 4). Here, the tasks are divided between the AFFOR and the AOC based on the task itself and the organization that is explicitly tasked or best suited to handle it. As was previously noted, this depiction shows significantly fewer tasks for the AFFOR than the AOC, but is missing the plethora of tasks required for infrastructure engineering and support. The intersection of the AOC and AFFOR circles is an area of particular interest, because it succinctly depicts the challenges that the C-NAF must overcome in order to handle all aspects of the cyber mission-set.

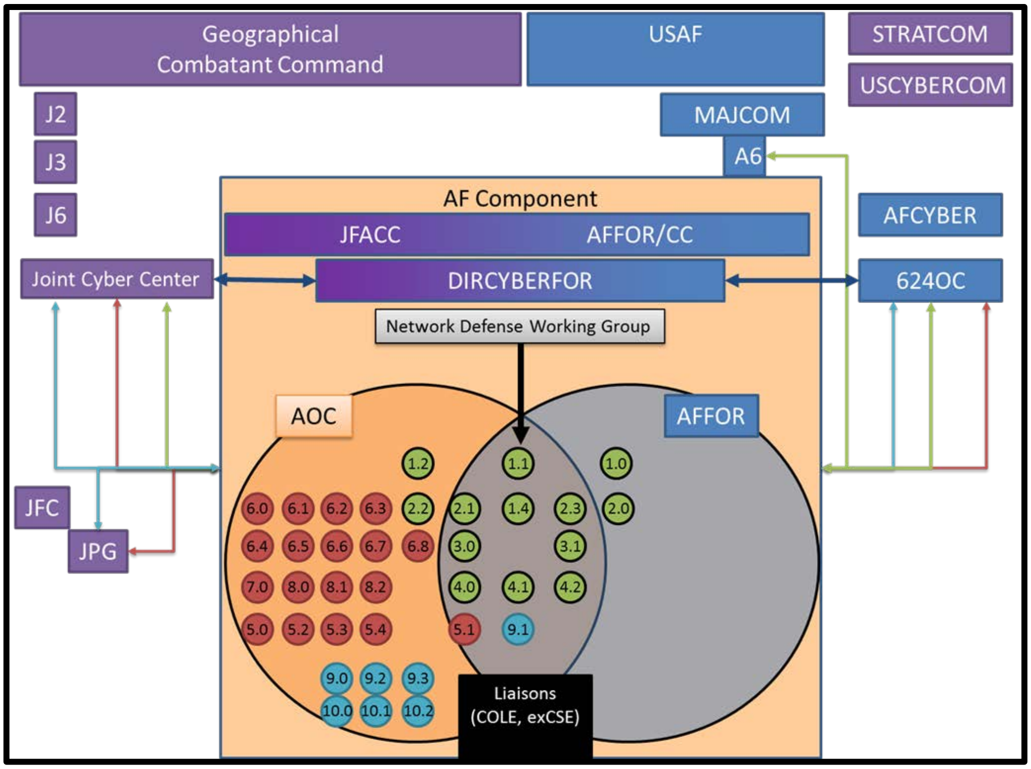


Figure 4: Operational Task View (intermediate)

AFTTP 3-3.AOC recommends the formation of a Network Defense Working Group (NDWG) as a cross-organizational body that can coordinate network defense across all stakeholders. The NDWG includes representatives of the AOC, NOSC, AFFOR/A6, Network Control Center (NCC) and others as required [9]. For the Network Infrastructure and passive defense tasks (green) in the intersection, no single organization has sufficient situational awareness, authority, or capability to identify the system vulnerabilities, assess enemy capabilities, determine mitigation strategies, assess mission risks, prioritize the mitigations based on mission impact, and implement a chosen course of action. A cross-organization entity like the NDWG, that includes Service and CCMD equities and authorities, is required to address these network defense gaps for the C-NAF.

3.3 ATO Synchronization

Of the many tasks remaining on the AOC side of the diagram, 6.7 is imminently important: “ensure all cyber taskings are deconflicted, integrated, and coordinated in the ATO,” [8] although synchronization should be included as well. This singular task also represents the main purpose of the AOC, all of the internal process, working groups and boards ultimately lead to the approval, publishing, and execution of the ATO. The ATO is the core document that ensures effects are integrated and synchronized. Not only airborne based effects are on the ATO; any effects that impact the air domain are included as well. In order to holistically evaluate the cyber-related requirements for the AOC, it is necessary to also evaluate the internal AOC process, at a minimum where cyber equities are anticipated.

For a complete review of the ATO process, reference AFI 13-1AOC volume 3 and AFTTP 3-3.AOC, but the most critical times for cyber are summarized here. A cyber planner, who understands the capabilities and limitations of cyber, must participate in the beginning Strategy discussion in order to ensure timely reach-back requests for support and the formulation of intelligence collection requirements. During ATO production, only an experienced cyber planner can match potential cyber effects against cyber delivery platforms, and express the capabilities and limitations to the other weapon-system planners. If the intelligence preparation is not sufficient, then the cyber planner may be forced to remove certain cyber weapons or platforms from the available list. While the previous steps are underway, the Intelligence, Surveillance, and Reconnaissance Division (ISRD), in coordination with the CCMD, USCYBERCOM and other agencies, will be conducting intelligence preparation of the operational environment, enemy analysis, developing a collection plan, and target development, which is currently the greatest challenge to integrating cyber into the ATO [8] [13]. Finally, execution presents challenges as offensive cyber capabilities are not usually deployed to the AOR and may not belong to the USAF. However, controlling operational timing and tempo are key elements to synchronizing effects for air-centric offensive and defensive operations. Furthermore, unlike the Integrated Air & Missile Defense forces, the JFACC does not necessarily have Operational or Tactical control over all the entities necessary to mount an effective cyber defense. A habitual relationship and practice with the 624OC and the JCC is essential to ensuring timely coordination and responsive reachback.

This exact problem arose during several USAF exercises in the recent past, and one mitigation proposal is a Defensive Cyber Operations-Tactical Coordinator (DCO-TC), which is fundamentally a liaison from the 624OC that has sufficient authority, from 24AF, to directly task Service organizations, like the I-NOSC, AF Computer Emergency Response Team, or base-level network control center to coordinate cyber defense. This method puts the necessary Service authorities at the disposal of the Joint Force without losing the operational context or confusing the chains of command [14].

In summary, there are many cyber-related requirements and expectations levied on the C-NAF from a variety of sources. When aggregated and analyzed, these requirements can be grouped and organized into a manageable set of minimum essential tasks. The singularly most important task for the Air Component is the integration and synchronization of cyber into the ATO, which is a very involved process and requires cyber-savvy planners at many different levels in the AOC to ensure success. The cyber challenges peak in the execution phase because of the disparate organizations across the AOR (or globe) that have vital data and no easy mechanism to share it and thereby enhance the AOC's situational awareness. Clearly defining roles and responsibilities, and developing a suitable organizational structure are the first challenges that the operational level must overcome. Suggestions for doing this are provided in the next chapter.

IV. Recommendations

As described above, there are many organizations and many requirements that a C-NAF must deal with to effectively utilize, defend, and operate in cyberspace. In order to effectively address the challenges for the AOC, the problems must also be addressed from the higher C-NAF level, and the 624OC. The following recommendations will be discussed in-turn:

- Establish a Cyber Center at the C-NAF Level
- Establish AOC Cyber Operations Team
- Manage Expectation for/with Liaisons
- Establish a Regional Structure within the 624OC
- Implement Globally linked, Interoperable AOCs

4.1 Establish a Cyber Center at the C-NAF Level.

The first recommendation, and the basis for the subsequent ones, is that the USAF should seek to parallel the organization outlined in the Joint Staff Transitional Cyberspace Operations C2 CONOPS. Just as the CCMD has a Joint Cyber Center, the AF Component should establish a parallel entity, one that stretches across the AFFOR Staff and AOC boundaries. This office is the lead for cyber in the AF component, and it provides a single focal point for the JCC to work with. The JCC has liaisons from USCYBERCOM (the CSE); likewise the C-NAF Cyber Center has continual liaisons from AFCYBER/24AF in the form of 624OC/I-NOSC representatives, and when necessary can still request a COLE from AFCYBER/24AF. During an exercise or contingency, the CSE embeds with the JCC and reaches back to USCYBERCOM, similarly, USCYBERCOM will likely provide an exCSE to the Air Component, or the COMAFFOR can request a COLE. By paralleling the design at the strategic level, lines of communication and roles begin to take shape. The JCC concept is fundamentally about bridging the equities that each directorate has and providing a common framework for addressing cyber issues. The AF component can garner the same benefits by adopting a Cyber Center setup that bridges the equities of A2, A3, A5, A6, and the AOC. The C-NAF Cyber Center will also serve to remove redundancy between cyber liaisons, clarify the lines of communication and streamline tasking and integration within the Air Component. The challenge is in aligning and synchronizing actions across the many staff elements. C-NAF staffs work extensively across the directorates on a routine basis for a variety of functions, but not usually cyber. Each C-NAF needs to build a Cyber Center construct and divide the roles and responsibilities according to their specific needs. Furthermore, communications with the CCMD will become easier and normalize when there is a single C-NAF Cyber Center, regardless of how its personnel are matrixed across the staff.

The AFFOR A2, A3, A5 will continue to work CONPLAN development as they normally would, but by identifying the cyber planners for each directorate and binding them under the C-NAF Cyber Center, the cyber aspects of the CONPLAN will improve drastically. Also, a more robust intelligence reporting and A6 response for cyber is critical to developing an integrated network defense posture. In many C-NAFs, these functions are primarily handled by 24AF entities (I-NOSC, 624OC, etc.) but as mentioned above, these organizations generally lack the context which is important to the C-NAF commander. The C-NAF Cyber Center is poised to tackle this with tighter meshing of A2, A3 and A6 but also including 24AF representation. Finally, the A3 and A6 responsibilities overlap in the area of Network Defense rules of engagement, the development of flexible response options, and the codification of these policies for the tactical units.

At the nexus of the AFFOR staff's overlapping responsibilities is the Director of Cyber Forces (DIRCYBERFOR). The DIRCYBERFOR is a fundamental position in the C-NAF Cyber Center, he/she provides unity of command and a single voice to the CCMD, and COMAFFOR on cyber planning, integration, and execution. The inherent challenge for the DIRCYBERFOR will be to bridge the communications and operations tribes and provide a unity of purpose. A potential good match of the DIRCYBERFOR is the deputy A6 and deputy A3 positions that can unite the tribes. The DIRCYBERFOR position, if adopted should also be afforded formal training similar to what the Director of Mobility Forces receives from Air Mobility Command. The lead command for identifying training requirements for the DIRCYBERFOR should be 24AF, as the DIRCYBERFOR will play a significant role in coordinating reach-back support for the C-NAF.

Additionally, the DIRCYBERFOR will play an integral role in the AOC, where the current director positions, Director of Mobility Forces (DIRMOBFOR) and the Director of Space Forces (DIRSPACEFOR), advise the JFACC/COMAFFOR on issues in their unique enclaves. The directorships were meant to provide augmenting advice for a JFACC that may not be well versed in Mobility or Space capabilities and limitations. From this precedent, a DIRCYBERFOR position certainly has merits of its own, and USAFCENT has already instituted at DIRCYBERFOR for the 609th AOC in Southwest Asia.

4.2 Establish AOC Cyber Operations Teams.

Every C-NAF will approach this Cyber Center differently, based on manpower, expertise and roles, but the AOC is an integral part of the C-NAF Cyber Center, and must be prepared to perform a bulk of the tasks during exercises and contingencies, when the AFFOR staff is focused on "beans, bullets, and beds." Furthermore, each C-NAF has missions and focuses that are unique to their AOR, which inevitably means that each C-NAF will have different manning requirements which will need to be addressed. Thus, the next level that requires organizational analysis is the AOC itself, the robust cyber requirements, as outline above, cannot be adequately met by a network warfare cell buried inside of the information operations team (IOT) as currently outlined in the regulations [8]. As seen in Figure 4, the AOC has many tasks centered on coordinating defense, planning and executing offense, and the intelligence actions to support both. These general tasks take many man-hours of planning to be ready for execution, coupled with the mandate of robust ATO integration, the loose collection of cyber planners that an AOC may currently have must be solidified into an organization that best suites the AOC and the emerging requirements of cyber.

There are three primary archetypal organizations within the AOC, a division, a director's staff, and a team. Extensive analysis was conducted on how cyber personnel could be organized under each of these archetypes. The resulting organizational structures were then graded on their relative merits in the areas of manpower use, cross-division integration, and autonomy to focus on cyber issues.

4.2.1 A new AOC division for cyber. As depicted in Figure 5, this consolidates all cyber planners under a single division chief who reports to the AOC commander. The cyber division is further divided into teams focused on defense, offense, and intelligence support. The Air Mobility Division (AMD) currently resembles this proposal, and the AMD functions much like a self-contained mini-AOC, with strategy, plans, execution, tactics, and intelligence teams. The AMD requires this autonomy because they generally execute missions outside of the current operational scheme of maneuver, the logistics requirements levied by the Combatant Command does not necessarily require significant integration with combat forces, instead deconfliction is more important. AMD's sorties are all loaded on the ATO, but the Combat Operations Division does not execute AMD missions per se. The autonomy that AMD enjoys based on its mission-sets may be a detriment to a cyber-division. Cyber is still very much an enabling capability and is the most useful when it creates effects that are synchronized with the rest of the force. In short, cyber needs to integrate and be synchronous with the fight, not asynchronous. Additionally, running an entire AOC division is resource intensive, and the USAF cyber force structure would be stressed to support it. While a division does nicely aggregate all the cyber responsibilities into a single organization, a division may be counterproductive to fully enmeshing cyber with the other weapon systems.

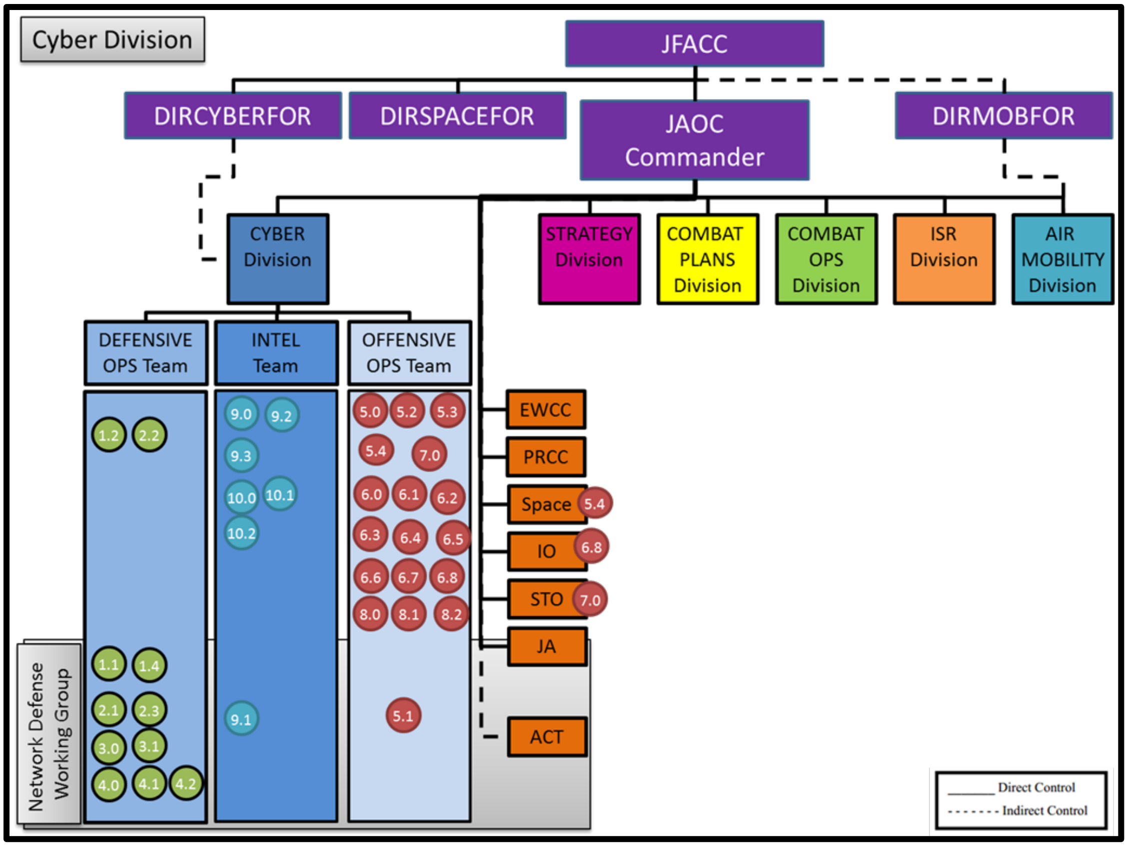


Figure 5: Cyber Division

4.2.2 Director Staff for Cyber A second option is that of a director's staff. There are generally two directors within an AOC, the Director of Mobility Forces (DIRMOBFOR), and the Director of Space Forces (DIRSPACEFOR). The DIRMOBFOR works issues specifically related to the airlift and tanker operations, while the AMD chief handles day-to-day operations, the DIRMOBFOR advises the JFACC on mobility issues, but should not be involved in the day-to-day operations. Conversely, the DIRSPACEFOR has no single division that they are concerned with, much like cyber planners, space planners are scattered throughout the AOC, specifically in the strategy, combat plans, and combat operations divisions. The DIRSPACEFOR usually has their own small staff, but the space planners work for their respective division chiefs, not the DIRSPACEFOR. With this setup, the DIRSPACEFOR advises the JFACC on space related issues, and leverages reach-back with Air Force Space Command and USSTRATCOM as required. As the senior space officer in an AOC, the DIRSPACEFOR helps to coordinate the efforts of the other space personnel, and provide guidance when necessary. Figure 6 illustrates a set of cyber working groups that directly report to the DIRCYBERFOR the offensive and defensive workgroups include personnel from all of the traditional AOC divisions, but only the workgroup leads work directly for the DIRCYBERFOR. In this manner, the cyber planners work for their respective division chiefs, but coordinate across the divisions with the help of the DIRCYBERFOR's staff.

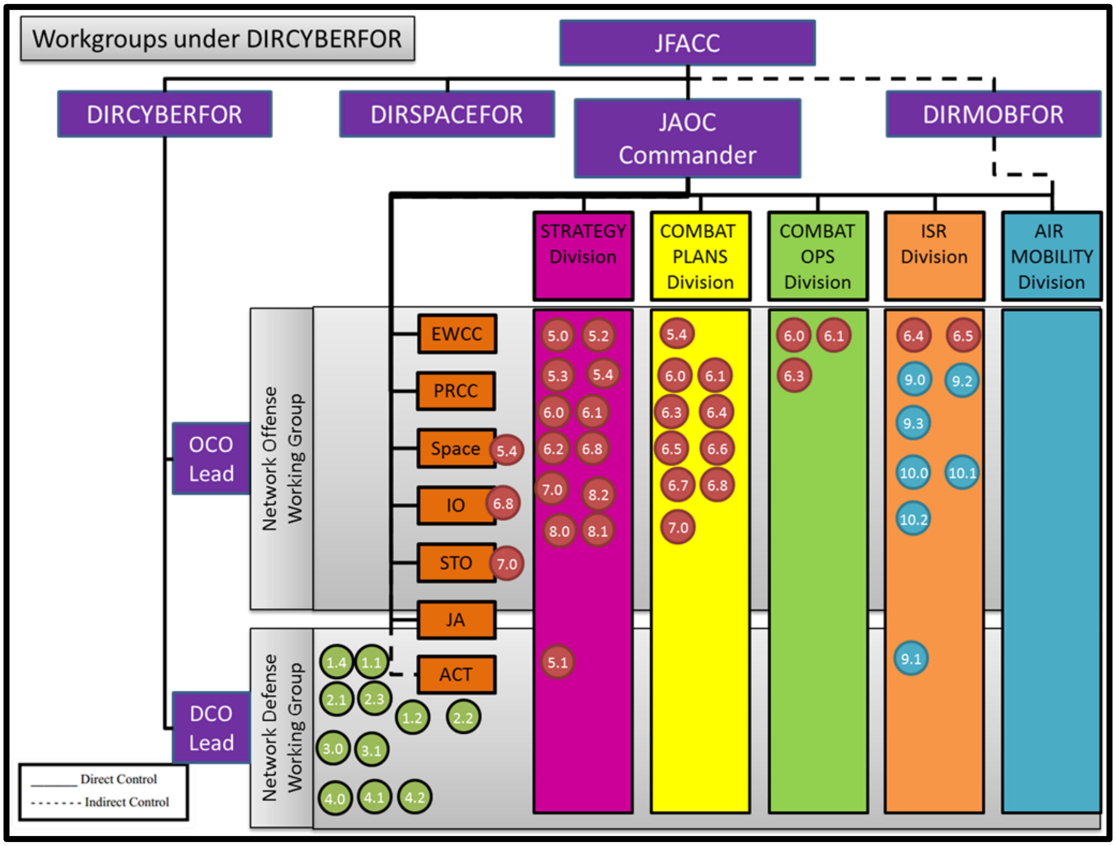


Figure 6: Workgroups under DIRCYBERFOR

4.2.3 Cyber Operations Team The final "traditional" organization in the AOC is a team, which generally reports directly to the AOC Commander, but may be administratively under a division chief. Examples of teams in the AOC include the Electronic Warfare Coordination Cell, the Information Operations Team, Special Technical Operations, and Personnel Recovery Coordination Cell. These teams work across the various division to plan, integrate, and ensure their equities are accounted for. In much the same way, as depicted in Figure 7, the Cyber Operations Team would be on the same level as the other teams, but also have additional guidance from the DIRCYBERFOR. The cyber operations teams includes all of the cyber planners in the AOC and work for a team leader who ensures proper representation in strategy meetings, ATO production meetings, as well as ensure sufficient representation on the "floor" to coordinate execution of offensive and defensive cyber effects. Of the three organizational types, the team makes the best use of manpower while being able to focus almost exclusively on cyber issues. The team structure also addresses cross-division integration quite well, as long the team stays engaged with the ATO cycle.

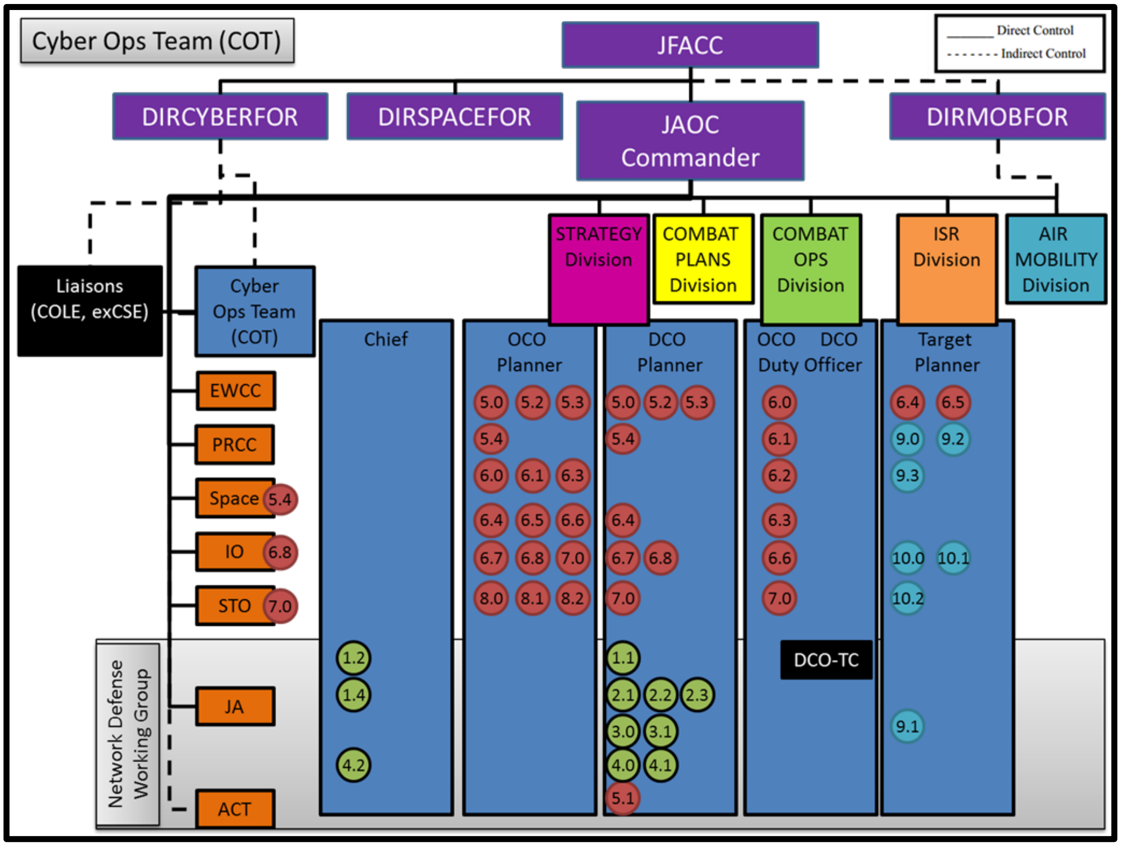


Figure 7: Cyber Operations Team

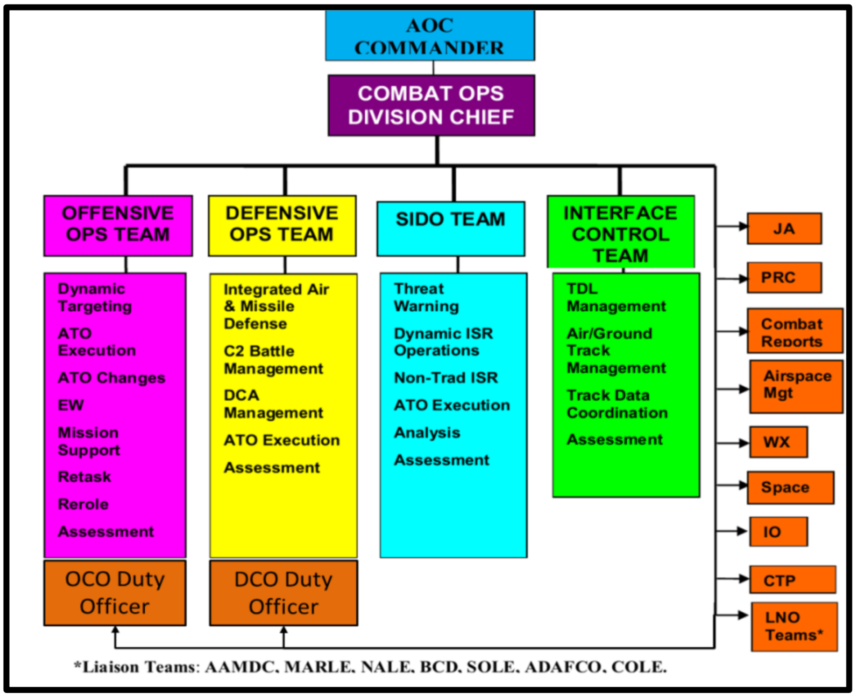
4.2.4 Implementation To summarize the organizational analysis, a division requires administrative overhead and manpower that the other organizational structures do not, and could serve to further stove-pipe cyber instead of integrating it across the AOC. The director's staff framework will face the same challenges as the Director of Space Forces does now, with each cyber planner working for their respective Division Chief, and the DIRCYBERFOR will be challenged to exercise significant influence over cyber planning processes, and will find it difficult to synchronize efforts throughout the ATO cycle. Finally, AOC specialty teams work across the various division to plan, integrate, and ensure their equities are accounted for. Comparing the relative merits of these three organizational paradigms, and while each AOC will have unique needs in this regard, the Cyber Operations Team best balances impact with personnel.

Given the relative merits of the Cyber Operations Team (COT) over the other paradigms, the exact organization of the team still requires attention, especially when reminded of all the tasks that fall to the AOC. The COT is led by a team chief that reports directly to the AOC Commander. The team chief has the unenviable task of ensuring that cyber is integrated and planned from the first strategy meeting through the execution phase. It is natural to divide the work between offense, OCO, and defense, DCO. As shown in Figure 7, the COT must have planners dedicated to OCO and DCO; these planners will begin planning with the Strategy Division but also carry forward to the Combat Plans Division for targeting effects, and master attack planning. The AF-wide lack of cyber experts is an unavoidable issue with this construct; putting greater responsibility upon a relative few number of AOC planners emphasizes the need for a thoughtful, deliberate assignment process. In order for this to work, the manpower functional managers and the AOC leadership should be concerned with getting the right individual to shoulder these responsibilities, else this construct will be counterproductive to cyber integration writ large. Also, the number of planners needed for this will depend greatly on the operations tempo of the region, but the emphasis for the foreseeable future should be on defense.

The DCO planner will also be the lead of the Network Defense Working Group (NDWG). The NDWG should be the primary reoccurring briefing that the DIRCYBERFOR receives; it provides the needed focus on bridging A2, A3, and A6 planners with the AOC. Additionally, the AOC Communications Team (ACT), which is usually a sub-unit of the AFFOR/A6, should attend in order to discuss hardening and defending the AOC systems themselves. The DIRCYBERFOR may decide to chair the NDWG for several months in order to provide it the proper vector and get firsthand accounts of the challenges for each of the staff elements. The NDWG is also the primary entry point for 24AF support, initially in the form of the servicing I-NOSC and later with select parts of the 624OC, which will be discussed later. The DIRCYBERFOR will likely find that the NDWG will raise issues that will require significant O-6 level discussions between directors within and without the C-NAF.

If done correctly, by "baking-in" cyber during the initial strategy meetings, the local ISRD and 624OC/ISRD will have sufficient lead time to gather sufficient intelligence to build target folders. This is the primary role of the Target Planner, a trained intelligence airman with sufficient cyber background to manage the cyber targets, identify intelligence shortfalls, and prioritize requests based on the OCO and DCO planner's needs. As discussed above, the targeting process for cyber is still rather immature and depending on the CCMD requirements may be the single largest hurdle for the COT to tackle.

Finally, the execution portion of the ATO cycle must be adequately addressed for the addition of cyber capabilities. The Combat Operations Division is basically divided into offensive operations, defensive operations, and intelligence teams, with a variety of specialty teams providing inputs as required (Figure 8). The COT should be staffed with an OCO and a DCO duty officer and have a continuous presence on the floor sitting near or with their respective counterparts. The DCO duty officer is also the perfect location for DCO-TC, as described above, to provide AF Service level defensive capabilities without delay and in full coordination with theater forces controlled by the DCO Duty Officer. The DCO-TC is a liaison, however, and should not be expected to C2 forces assigned to the Combatant Commander.



*Liaison Teams: AAMDC, MARLE, NALE, BCD, SOLE, ADAFCO, COLE.

Figure 8: Combat Operations Division

4.3 Manage Expectations for/with Liaisons

With regards to cyber liaisons from USCYBERCOM or 24AF, the COT provides a seamless organization for them to liaison with. The exCSE or COLE Chief would be the natural counterpart to the Cyber Operations Team Chief, and they would jointly decide where and when each of the liaison-team-members should work. The COT should be prepared to double in size when an exCSE arrives and should already understand what an exCSE can offer in terms of reach-back support. Additionally, the DIRCYBERFOR should have recurring communications with the USCYBERCOM CSE lead and discuss roles, responsibilities, and expectations of the exCSE before they arrive at the AOC.

4.4 Establish a Regional Structure within the 624OC

As the CCMDs begin to solidify their JCC and associated processes, it is likely that more will be expected from the components in terms of cyber planning, reporting, and situational awareness. As the pressure increases on the geographic C-NAFs, AFCYBER/24AF will see increased requests for reach-back support, to augment the situational awareness and capabilities that the geographic C-NAFs do not have access to or do not have the expertise to handle. One crucial part of the C-NAF Cyber Center will be to coordinate with their 24AF counterparts to ensure a unified message from the AF components to their respective CCMDs. This should hold true for the AOC functions as well, and the 624OC must be postured and organized to facilitate the necessary reach-back support.

A fundamental aspect of reach-back support that will frustrate the supported and supporting AOCs alike is an inevitable lack of context outside of the AOR. In order for the 624OC to make the "right" decisions and provide the "right" support, they must have context on what is going on in theater. This is achieved in two ways: First, the 624OC personnel must develop a concept of "normal" for that particular region. "Normal" network traffic looks a certain way; attacks usually occur from a particular vector and seem to be targeting certain things. Without a concept of "normal", the 624OC will not be able to provide the indications and warnings that their counterparts need. The

624OC/ISRD is divided up regionally. They have specific people concentrating on specific regions of the world, and they provide intelligence analysis and can provide context to leadership when it deviates from normal. The rest of the 624OC divisions are not organized regionally, and thus have no baseline for “normal” in the AORs. The 624OC should consider implementing Mission Area Teams, in which each team includes members from every division for each Geographical Combatant Command. The ISRD should provide recurring intelligence briefs to all members of the Mission Area Team and as the team members build context and make contact with their regional AOC counterparts, other divisions can brief pertinent details that aid in developing context.

4.5 Implement Globally Linked, Interoperable AOCs

The second recommendation that will help the 624OC gain and maintain regional context, is to build habitual relationships with their AOC counterparts. Meetings between the COTs and Mission Area Teams should occur at a bi-weekly basis via secure teleconference. The team leaders will have to decide what topics are appropriate to share between supported and supporting AOCs, but mutually increasing situational awareness and providing context is worth the additional effort. The COTs within each regional AOC then need to communicate the “cyber tribe’s” understanding of the threats to the rest of the AOC planning team. Creating a closed door, “cyber only” process should be aggressively avoided. This habitual relationship will make reach-back during contingencies and exercises feasible, ensuring that both organizations understand the battlerythm, capabilities and limitations of the other beforehand. This relationship will also make sourcing a COLE or exCSE easier, as some 624OC personnel are already familiar with the AOR and its respective challenges.

The maturing of globally linked interoperable AOCs may be more compelling for 24AF leadership than simple the fostering of context and situational awareness, the 24AF needs help with one of their primary tasks, Mission Assurance. Addressing mission assurance for the USAF cannot be accomplished without the mission owners, but the mission owners do not necessarily understand the term, what it means to them, or why they have such a critical role. Fostering communications between AFFOR staffs and AOCs will greatly help the 24AF in beginning to tackle the mission assurance problem. Mapping the AOC missions to required infrastructure may be a feasible first step in understand the larger mission assurance problem-set, and habitual working relationship between AOCs is a necessary first step.

4.6 Summary In summary, the C-NAFs need to adopt an organizational structure that provides unity to the CCMD and sister services in terms of cyber. The C-NAF Cyber Center mirrors what the CCMDs are adopting, and thus makes for an easy transition. The C-NAF Cyber Center must bridge the AFFOR Directorates and the AOC, and this is most likely achieved through a Director of Cyber Forces. The AOC is a vital part of the C-NAF Cyber Center, and should reorganize its cyber personnel into a Cyber Operations Team, with the autonomy to plan offensive and defensive cyber operations while the DIRCYBERFOR ensures all the of C-NAF's cyber equities are included. The Network Defense Working Group is critical to breaking down organizational stove-pipes and solving the tough problems of defending the AFNet and other constructed networks. The 624OC should consider forming teams for each Geographic Combatant Command that spans each of the 624OC divisions. The Mission Area Teams should build their situational awareness on normal network operations and begin habitual working relationships with their regional AOC counterparts. Finally, these relationships can help 24AF begin to understand the mission assurance problem space.

V. Conclusions

5.1 Conclusion Through this analysis, the current situation was presented with regards to cyber players in a C-NAF, the CCMD, and USCYBERCOM to include the CSE, exCSE, and AFCYBER. Additionally, the plethora of operational cyber-related tasks and requirements were discussed and aggregated, further defining the requirements the C-NAF must meet, with particular emphasis on cyber integration with other assets, manifested in the ATO. Finally, a series of organizational recommendations were offered in order for the C-NAF, the AOC, and ultimately the Cyber Operations Team to meet all of the expectations for the C-NAF. Additional recommendations for the 624OC were offered in order to facilitate globally linked, interoperable AOCs.

5.2 Recommendations for Future Research

Training and Education for Cyber Planners: The 505CCW at Hurlburt AFB, conducts all of the pre-deployment and pre-assignment training for personnel assigned to an AOC. These courses include AOC processes and organizations, the assumption being that planners are already well educated, or experts, in their respective weapon systems. The AOC courses build on the knowledge of operations that most students already have. When it comes to cyber planners, there is lack of operational experience, specifically in the areas of OCO and DCO. The training and education requirements for cyber planners in the AOC, and AFFOR staff, need to be examined, to baseline OCO and DCO and provide the operational context those planners need before they go to the AOC courses.

Training and Education for the DIRCYBERFOR: The 505CCW also offers the DIRMOBFOR course, to educate, train, and eventually certify students as a

DIRMOBFOR. This type of course is also necessary for DIRCYBERFORs if the position is to expand beyond USAFCENT, and be effective in the role as outlined above.

Technical Solutions to link AOCs. Currently, cyber taskings between AOCs is done manually. For instance, if the 603AOC wanted to send a set of cyber-related tasks to the 624OC, the cyber specific tasks would be cut from the 603d's ATO, and emailed to the 624OC, which is then aggregated into the 624's tasking order for processing. More details about targets and intent has to be passed as well, because the ATO format does not contain all the required elements needed by many cyber capabilities. Future research should look at technical solutions to pass taskings, including all necessary fields, as well as target folders, cyber situational awareness, etc between the 624OC and the other AOCs worldwide.

Bibliography

[1] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," 2011.

[2] Secretary of Defense, *Memorandum for Commanders of the Combatant Commands,* 2012.

[3] K. Lustig, "Weapons school integrates cyber warfare," 16 06 2012. [Online]. Available: http://www.af.mil/news/story.asp?id=123304225. [Accessed 10 01 2013].

[4] Joint Staff, *Joint Staf Transitional Cyberspace Operations Command and Control Concept of Operations*, 2012.

[5] LeMay Center/DDS, *Air Force Doctrine Document 1,* 2011.

[6] Air Intelligence Agency Public Affairs, "Air Force stands up first network warfare wing," 05 07 2006. [Online]. Available: http://www.af.mil/news/story.asp?id=123022799. [Accessed 07 02 2013].

[7] *Air Force Instruction 13-1 AOC, Volume 3, change 1,* 2012.

[8] *AFTTP 3-3.AOC,* 2007.

[9] HQ USAF/A3/5, *Air Force Policy Directive 13-3,* 2008.

[10] 624 OC, *Concept for the 624th Operations Center (OC),* 2010.

[11] LeMay Center/DDS, *Air Force Doctrine Document 3-12, Change 1,* 2011.

[12] S. J. Smart, "Joint Targeting in Cyberspace," *Air and Space Power Journal,* pp. 65-75, 2011.

[13] 561st Joint Tactics Squadron, *Flash Bulletin 12-12: Defensive Cyber Operations - Tactical Coordinator Planning and execution,* 2012.

[14] 8AF, *Concept of Cyber Warfare*, 2007.

[15] 561st Joint Tactics Squadron, *Tactics Bulletin 2011-02: Non-Kinetic Operations Coordination Cell,* 2011.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to an penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 13-June-2013	**2. REPORT TYPE** Graduate Research Project	**3. DATES COVERED** *(From – To)* 15 June 2012 – 14 June 2013

4. TITLE AND SUBTITLE CYBERSPACE INTEGRATION WITHIN THE AIR OPERATIONS CENTER	**5a. CONTRACT NUMBER** N/A **5b. GRANT NUMBER** N/A **5c. PROGRAM ELEMENT NUMBER** N/A
6. AUTHOR(S) Rueter, Bradley A. MAJ, USAF	**5d. PROJECT NUMBER** N/A **5e. TASK NUMBER** N/A **5f. WORK UNIT NUMBER** N/A
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology 2950 Hobson Way, Building 640 WPAFB OH 45433-7765	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT-ENG-GRP-13-J-02
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Intentionally Left Blank	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

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

14. ABSTRACT
The Air and Space Operations Center (AOC) is the United States Air Force's operational command and control (C2) platform for the planning and execution of Air, Space, and Cyber operations. Operational C2 of cyber forces is a significant challenge that impacts the planning and integration of cyber operations at the AOC. The Joint Staff's Transitional Cyberspace C2 Concept of Operations, released in March 2012, provides a cyber C2 framework at the Geographical and Functional Combatant Command level, but it is not clear yet how Air Force AOCs will work together to meet the requirements of the CONOPS or conduct cyber planning to support the needs of the Joint Force Air Component Commander. This paper summarizes the results of a mission analysis to identify the roles and responsibilities for cyber operations within the AOC, separating them from traditional J6/A6 responsibilities. Additionally, the Joint Staff CONOPS calls for significant "reach back" for planning, expertise, and potential execution of cyber capabilities; as such, the paper provides a discussion on how to facilitate globally linked, interoperable AOCs for cyber planning and execution.

15. SUBJECT TERMS
Cyberspace, Operations, AOC, Operations Center, Integration

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Robert F. Mills, PhD (ENG)
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
U	U	U	UU	51	(937) 255-6565x4527; robert.mills@afit.edu

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