

24 AF and AFCYBER



November 30, 2015

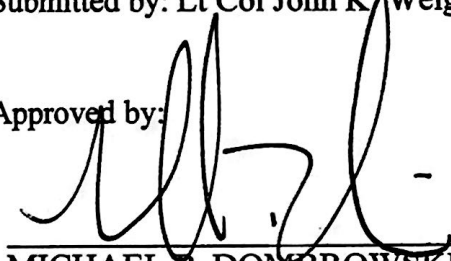
DEFENSIVE CYBERSPACE OPERATIONS CONCEPT OF EMPLOYMENT

THIS PAGE INTENTIONALLY LEFT BLANK

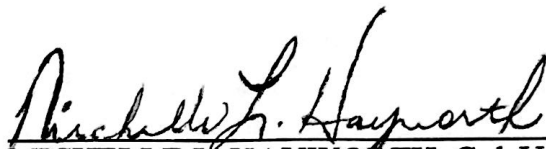
DEFENSIVE CYBERSPACE OPERATIONS CONCEPT OF EMPLOYMENT

Prepared by: Capt Jeremy L. Sparks, 24 AF/A3TW
Submitted by: Lt Col John K. Weigle, 24 AF/A3T

Approved by:



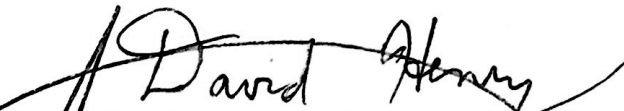
MICHAEL P. DOMBROWSKI, Col, USAF
Commander, 624th Operations Center



MICHELLE L. HAYWORTH, Col, USAF
Commander, 688th Cyberspace Wing



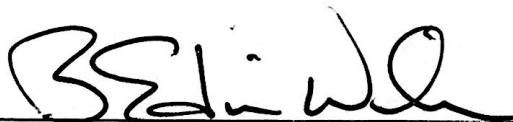
DAVID W. SNODDY, Col, USAF
Commander, 67th Cyberspace Wing



MARK D. HENRY, Col, USAF
Director of Plans and Requirements, 24th Air Force and Air Forces Cyber



DANIEL A. PEPPER, Col, USAF
Director of Operations, 24th Air Force and Air Forces Cyber



B. EDWIN WILSON, Maj Gen, USAF
Commander, 24th Air Force and Air Forces Cyber

Table of Contents

1.	Introduction.....	5
2.	Overview.....	5
2.1	Scope.....	5
2.1.1	Applicability.	5
2.1.2	Area of Operations.....	5
2.2	Purpose.....	5
2.3	Method.	6
2.4	End State.	6
3.	Authorities.....	6
4.	Operating Concepts.....	6
4.1	Command and Control (C2).....	6
4.2	Large Force Employment (LFE) Concepts.	7
4.2.1	When LFE is Advisable.	7
4.2.2	Force Packaging.....	8
4.2.3	Force Packaging Development and Execution.	8
4.2.4	Mission Commander.	8
4.2.6	Mission Planning Cell Chief (MPCC)	9
4.2.7	Mission Planning Cell Responsibilities and Composition.	9
4.2.8	Package Commander.....	9
4.2.9	Tactical Planning Framework.	9
4.3	Cyberspace C2 Documents.....	9
4.4	Current Cyberspace Mission Definitions.....	10
4.6	DCO Mission Types	13
5.	Tactical Mission Planning.....	18
6.	Force Presentation.....	18
7.	DCO Mission Thread.....	19
8.	Responsibilities.....	26
	APPENDIX A - Glossary of Terms.....	29
	APPENDIX B - Acronyms	31
	APPENDIX C - Strategy to Task.....	32
	APPENDIX D - Cyberspace LFE Foundations.....	34
	APPENDIX E - References	35
	APPENDIX F - Contributing Authors.....	36

1. Introduction

1.1 This Defensive Cyberspace Operations (DCO) Concept of Employment (CONEMP):

1.1.1 Guides 24th Air Force, Air Forces Cyber (AFCYBER) and, as authorized, designated mission partners for cyberspace operations, to secure, operate, and defend the critical mission elements of the Air Force Information Network (AFIN) or assigned Area of Operations (AO).

1.1.2 Serves as the foundational cornerstone to execute the AFCYBER mission to secure and defend the AFIN, or assigned AO, to ensure U.S. and allied freedom-of-action in cyberspace.

1.1.3 Leverages the full range of capabilities, capacity, and authorities of AFCYBER forces and mission partners.

1.1.4 Clarifies command and control (C2) relationships and established authorities, as well as outlines DCO mission types and processes necessary for timely execution of cyberspace operations.

1.2 This DCO CONEMP is the culmination of lessons learned (LL) from 2011-2015: Operation PHANTOM BLITZ, Operation MONGOOSE WEDGE, Operation LINOLEUM NEEDLE, Operation FLYING MONKEY, Operation SAVAGE KNIGHT, Operation PHANTOM FORTRESS, Operation COBALT CASTLE, Operation HEARTBLEED, Operation COBALT SIRIUS, Operation CRAFTY EAGLE, Operation CRAFTY SCORPION, Operation CRAFTY HORNET, Operation CRAFTY WASP and the implementation of the concepts defined in Operation COBALT NEEDLE. For more information regarding the genesis of AFCYBER's DCO LFE foundations, including the specific lessons learned from the aforementioned operations, see appendix G.

2. Overview

2.1 Scope.

2.1.1 Applicability. This DCO CONEMP is specific to Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM) and applies to assigned and attached AFCYBER forces. AFCYBER forces in this document include service reallocated Cyberspace Protection Teams (CPT) and Air Force DCO forces.

2.1.2 Area of Operations (AO). The AO includes the AFIN as defined by Air Force Instruction (AFI) 10-1701, *Command and Control for Cyberspace Operations* and AOs tasked by the 624th Operations Center (OC), including AOs outside the AFIN.

2.2 Purpose. The purpose of this document is to provide a concept for executing DCO missions through presented and apportioned forces which are capable of producing deny, degrade, destroy, disrupt, and manipulate (D4M) effects in and through cyberspace.

2.3 Method. Consolidate various AF and joint documents and lessons learned from past operations into a single authoritative source for planning and employment considerations at operational and tactical levels.

2.4 End State. A repeatable construct for presenting, tasking, apportioning and employing AFCYBER forces. The 624 OC tasks AFCYBER forces in support of single missions or large force employment (LFE) operations to accomplish prioritized objectives within available capacity. Mission Planning Cell Chiefs (MPCC) and Mission Commanders (MC) plan and orchestrate tactical timing and tempo of effects within the vulnerability (vul) window specified in the Cyberspace Tasking Order (CTO). Enterprise DCO forces and CPT forces collaborate to plan, brief, execute and debrief missions when integrating their capabilities. For more information regarding the MC and MPCC roles and responsibilities, see *Air Force Tactics, Techniques and Procedures (AFTTP) 3-1.General Planning (GP)*.

3. Authorities

3.1 In accordance with (IAW) AFD 10-17, *Cyberspace Operations*, the Commander, Air Force Space Command (AFSPC/CC) is responsible for the command and control, security and defense of the AFIN, the Air Force-provisioned portion of the Department of Defense Information Network (DoDIN).

3.2 24 AF is the Service Cyber Component to United States Cyber Command (USCYBERCOM). 24 AF/CC, when acting as Commander, AFCYBER (CDR AFCYBER), or when executing authorities delegated by AFSPC/CC, will issue orders for the operation, defense, maintenance and control of the AFIN to the major commands (MAJCOM), wings, network operations security center (NOSC), and communication focal points (CFP). CDR AFCYBER is delegated authority of service reallocated CPTs from Commander, US Strategic Command (USSTRATCOM) per the Global Force Management Implementation Guidance Fiscal Year 2014-2015.

3.3 IAW AFI 10-1701, *Cyberspace Operations*, 24 AF/CDR AFCYBER is responsible for issuing the cyberspace orders ISO DCO. Applicable cyberspace orders are distributed by the 624 OC to MAJCOMs, field operating agencies (FOA), direct reporting units (DRU), MAJCOM communications coordination centers (MCCC), AF component commands and associated air operations centers (AOC), and air force forces (AFFOR) communications control centers (ACCC) for actions affecting assets (e.g., personnel, information systems, etc.,) not under the direct control or authority of 24 AF.

4. Operating Concepts

4.1 Command and Control (C2)

4.1.1 Centralized Control and Decentralized Execution. Centralized control and decentralized execution is the foundational tenet for the employment of air, space, and cyberspace power. Within the AF, the centralized control for cyberspace operations is conducted by 624 OC and the apportioned tactical forces conduct decentralized execution. This is consistent with how the centralized control of airpower resides at

the AOC, but mission execution is decentralized—accomplished within the command C2 architecture optimizing the ability of the front-line warfighter (e.g., strike package mission commander, air battle manager, forward air controller, etc.) to make on-scene decisions during complex and rapidly unfolding operations. The *AFTTP 3-1.General Planning* notes that centralized control should be accomplished by an Airman at the component commander level. The centralized control entity maintains a broad focus on the commander's objectives to direct, integrate, prioritize, plan, coordinate, and assess the use of air, space, and cyberspace assets in any contingency across the range of military operations. Decentralized execution is accomplished through the use of single force execution or large composite forces under tactical control of a composite force mission commander.

4.1.2 Operational Command and Control

4.1.2.1 Operational-level C2 is executed through the 624 OC, which is modeled on the AOC organizational construct. IAW *AFI 10-1701, Command and Control for Cyberspace Operations*, the 624 OC is responsible for optimizing resources in order to perform operational C2 of AFCYBER forces.

4.1.2.2 Centralized control of AF cyberspace operations resides at the 624 OC, but mission execution is decentralized—accomplished within the C2 architecture to enable the tactical level warfighter to engage, respond, adapt, and fight within the execution of DCO operations. Decentralized execution is performed through composite force mission commanders and mission leads, and forces under their tactical control.

4.1.2.3 The 624 OC maintains situational awareness on all tasked DCO missions. DCO forces are responsible for reporting ongoing, planned, and completed activities to the 624 OC through the operational chain of command. The 624 OC will issue specific guidance and establish supporting procedures to enable DCO mission reporting. Additionally, the 624 OC will direct and enable timely, accurate, and efficient synchronization and deconfliction.

4.1.3 Tactical Command and Control. In the C2 construct, tactical mission commanders are subordinate to the 624 OC. Tactical mission leads have tactical control (TACON) over forces assigned to them via the CTO during the time specified in the CTO.

4.2 Large Force Employment (LFE) Concepts. Tactical advantage is gained when leadership directs a preponderance of physical forces and material advantages to a decisive place and time of their choosing. This principle is realized in today's combat environment through individual units executing tactical missions that are packaged together in support of a larger operational mission.

4.2.1 When LFE is Advisable. The use of LFE is advisable when cyberspace forces will be operating in the same AO during the same vulnerability window and when the

capabilities will mutually support each other.

4.2.2 Force Packaging. Force packaging is the combining of forces to mutually support each other during the same vul window. Packages are a set of missions (typically multi-mission and multi-platform) grouped to ensure proper mutual support (*AFTTP 3-3.AOC*). DCO missions are not always tasked via a force package. Some missions, specifically those that do not require support from another weapons system or separate tactical force, are tasked to a single tactical force for execution.

4.2.3 Force Packaging Development and Execution. The 624 OC Strategic Plans Division (SPD) determines the size and composition of force packages based on the mission requirements and available forces. Force packages may range in size from a small number of cyberspace capabilities to a wide-scale coordinated mission. Composite force operations integrate various capabilities and support functions to form a specific mission force with a synergistic approach. The composite force mission commander (MC) is the leader designated to develop, orchestrate, and manage the assigned composite forces. MCs generally conduct their duties in addition to their role as lead for their specific CTO-designated mission. For example, the MC for a strike mission may also be the strike package commander (PC).

4.2.4 Mission Commander. The MC is designated as the tactical leader of the composite force. The MC derives this authority and responsibility from CDR AFCYBER through the CTO. The MC is responsible for all forces depicted in the assigned CTO mission during the designated vulnerability window. The MC plans (in conjunction with the MPCC), coordinates, leads, and debriefs the mission. MCs are chosen based on their situational awareness (SA) of the fight and/or preponderance of mission capability. Missions that require LFE will have a MC assigned. The 624 OC will designate in the CTO which unit will be the lead for the LFE. The lead unit will then appoint an MPCC and MC for the mission. If the CTO has already been published and operational necessity drives a CTO update that requires a LFE mission, the 624 OC/COD will appoint a lead unit for the LFE mission. The lead unit will appoint an MPCC and MC for the mission.

4.2.4.1 Example 1 – LFE Strike Mission: For a strike mission at base X on target Y, using primarily capabilities from the Air Force Cyberspace Defense (ACD) weapon system, the MC would likely be tasked from the ACD community.

4.2.4.2 Example 2 – LFE Reconnaissance Mission: For a reconnaissance mission on Enclave X, using primarily Cyberspace Vulnerability Assessment and Hunt (CVA/H) capabilities, the MC would likely be tasked from the CVA/H community.

4.2.5 Tactical C2 Pitfalls. The MC (by definition) is an individual designated to lead an LFE during a single vul window. Assigning a single individual as the MC across multiple vul windows and successive CTO days is non-doctrinal, and should be

avoided. Additionally, assigning a single, enduring MC transfers the 624 OC's responsibility for campaign management to the tactical units instead of relying on normalized Air Force operational-level C2 processes.

4.2.6 Mission Planning Cell Chief (MPCC). The MPCC leads the mission planning cell (MPC) as a proxy for the MC to develop the tactical plan. Responsibilities include coordinating with the MC, collateral organizations, and higher headquarters. In addition, the MPCC establishes the planning timeline, develops an initial game plan, and assigns mission tasks based on functional area expertise and plans for contingencies. For more information, reference the MPCC roles and responsibilities sections of the AFTTP 3-1.*General Planning* as well as the *24 AF, AFCYBER and JFHQ-C AFCYBER Tactical Mission Planning, Briefing, and Debriefing Guide*.

4.2.7 Mission Planning Cell Responsibilities and Composition. The MPC supports the commander's intent by providing the MC with the tools required to accomplish the assigned mission. The MPC is responsible for planning tactical missions in accordance with MC direction, with responsibilities beginning upon receipt of the initial tasking. MPC teams are comprised of the MPCC, and as applicable, tactical mission leads (e.g., access, reconnaissance, etc.) and key personnel from assets executing the mission.

4.2.8 Package Commander. During LFE missions, individual package leads are referred to as package commanders. For example, if a strike mission requires access and surveillance support, the strike, access and surveillance forces would be led by their respective PCs. PCs are subordinate to the MC during mission execution. PCs may also be dual-hatted as the MC.

4.2.9 Tactical Planning Framework. Tactical-level planners employ the ME3C-(PC)² tactical mission planning framework codified in AFTTP 3-1.*General Planning*. This framework provides a systematic approach to mission planning by stepping through nine major planning steps: mission, environment, enemy, effects, capabilities, plan, phasing, contracts, and contingencies. For more information reference the ME3C-(PC)² sections of the AFTTP 3-1.*General Planning* as well as the *24 AF, AFCYBER, JFHQ-C AFCYBER Tactical Mission Planning, Briefing, and Debriefing Guide*.

4.3 Cyberspace C2 Documents. AFCYBER (24 AF) and 624 OC publish multiple documents to direct and scope the planning and execution of cyberspace operations. The tasking documents continue to be refined as the community matures its C2 processes and lessons learned.

4.3.1 In order to coordinate and release orders in a timeframe that is responsive to ongoing cyber operations, 24 AF / CDR AFCYBER has delegated signature authority to 24 AF/A3 to approve Warning Orders (WARNORDs), Fragmentary Orders (FRAGOs), and Tasking Orders (TASKORDs).

4.3.2 WARNORD. A WARNORD provides advance notice of an order or action

which is to follow.

4.3.3 FRAGO. A FRAGO provides quick changes to Operations Orders (OPORDs) or TASKORDs that eliminates the need to completely rewrite orders when situations/conditions change.

4.3.4 TASKORD. A TASKORD provides overarching guidance and outlines associated objectives, desired effects and tasks necessary for mission completion.

4.3.5 Cyber Operations Plan (CyOP). The CyOP published semiannually and is the overarching document addressing CDR AFCYBER's foundational strategy. The CyOP guides the employment of full-spectrum cyber capabilities.

4.3.6 Cyber Operations Directive (CyOD). The CyOD is published weekly and provides overarching guidance for planning, execution, and assessment of cyberspace operations.

4.3.7 Cyber Tasking Order (CTO). The CTO is published daily and is influenced by the guidance outlined in the weekly CyOD. The CTO tasks assigned and attached cyber forces to perform DCO, offensive cyber operations (OCO), and DoDIN operations to meet AF and Joint requirements. The CTO provides mission identification number, mission priority, tasked unit(s), time over target/terrain, AO information and any additional mission comments (e.g., lead unit for an LFE, additional SA or deconfliction information).

4.3.8 Special Instructions (SPINS). SPINS are published as required and codify procedures and processes for operations directed in the CTO. SPINS detail special considerations and/or special items of interest (or amplifications for execution planning) for units in the performance of specific tasks. The 624 OC publishes standing SPINS, weekly SPINS, and exercise and operation-specific SPINS.

4.4 Current Cyberspace Mission Definitions. Foundational cyberspace mission definitions are defined below and illustrated in Figure 1, Cyberspace Mission Definitions Illustrated. A more inclusive list of terms and definitions can be found in the appendices. Standard mission definitions include:

4.4.1 Tactical Missions. Tactical missions are operations conducted with specific objectives and tasks. Tactical missions are conducted by unit(s) with relevant capability. Tactical missions are commanded by a tactical commander on specific terrain and target(s) during an authorized vulnerability window.

4.4.2 Vulnerability (vul) Window. A window of opportunity and direction for a tactical commander to conduct tactical operations. A vul window is time bounded (start by/finish by) to give a tactical commander the authorized and suspended timing available to plan and execute missions. Deviations from the assigned vul window must be approved by the 624 OC.

4.4.3 Time-Over-Target/Terrain (TOT). The exact timing directed by the tasking authority specified in the tasking order to execute a mission. The TOT is based on the available vul window (can be an enduring or time-sensitive requirement) and must be planned and tasked within the vul window.

4.4.4 On/Off Station. Cyberspace forces are considered to be on station when the cyberspace operation commences on tasked terrain and targets. Cyberspace forces are considered to be off station when assigned tasks are completed and cyberspace forces are no longer engaging assigned targets or performing mission in the tasked terrain.

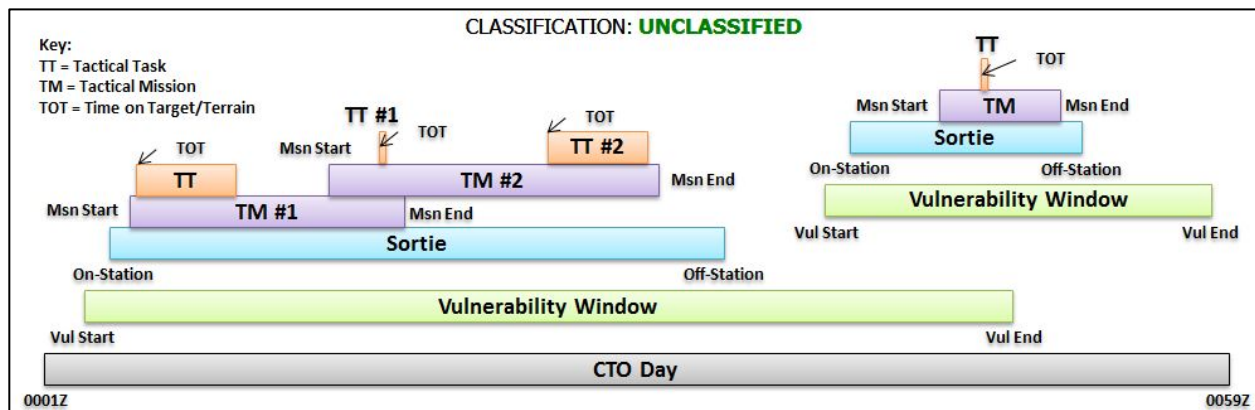
4.4.5 Sortie. A cyber sortie (combat or training) constitutes the actions individual cyberspace forces take to accomplish a tasked mission. The base unit for a sortie is a single tactical mission conducted by a single tasked cyberspace force. Cyberspace forces begin a single sortie when they come on station and complete a single sortie when the operators come off station.

4.4.6 Terrain. Cyber terrain is defined as telecommunications networks, computer systems, embedded processors and controllers, Internet Protocol (IP) address(es), associated subnet, domain, or transport space within the tasked AO.

4.4.7 Target. An entity or object that performs a function for the adversary considered for possible engagement or other action. As it relates to DCO, targets may include, but are not limited to: malicious code, enemy ingress/egress routes, compromised credentials, network traffic and/or processes residing in or on the terrain.

4.4.8 Pre-approved Actions (PAA). PAAs are defined as standing orders, rules of engagement, intelligence gain/loss considerations, and actions (i.e., TTP, standard operating procedures, checklists, etc.) authorized by the tasking authority that are implemented when specified thresholds or conditions are met. PAAs enhance the mission effectiveness by enabling forces to rapidly neutralize adversary activity inside the tasked AO and optimize the tactical leader's ability to make on-scene decisions during complex and rapidly unfolding operations.

Figure 1, Cyberspace Mission Definitions Illustrated



4.5 Targeting

4.5.1 Dynamic Targeting Processes

4.5.1.1 624 OC's role in Dynamic Targeting

4.5.1.1.1 The 624 OC routinely conducts time sensitive targeting (TST). The 624 OC utilizes an accelerated nomination and approval process to quickly coordinate and approve dynamic targets while developing a targeting solution using the find, fix, track, target, engage and assess (F2T2EA) model.

4.5.1.1.2 The 624 OC Combat Operations Division (COD) performs real-time assessment of threats and determines whether or not to strike a target. If COD decides to engage the target, they are responsible for assigning appropriate forces. This may include dynamically designing an LFE and appointing a mission lead. The following steps detail COD's process for dynamic targeting:

4.5.1.1.3 (FIND) Initial Report/Inputs/Requests are fed to Senior Intel Duty Officer (SIDO). SIDO evaluates the target nomination to determine whether the target is valid; whether it meets CyOP/CyOD objectives; whether it violates ROE, no-strike list, restricted target list; determine impact of not servicing the target; determine intelligence gain/loss; etc.

4.5.1.1.4 (FIX) SIDO determines positive identification (PID) of target.

4.5.1.1.5 (TRACK) Maintain PID of target through employment of ISR capabilities.

4.5.1.1.6 (TARGET) 624 OC/COD DCO cell matches best capability against target while considering target location, authorized service interruptions (ASI), periods of non-disruption (POND), deconflictions, etc. Mission tasking message (MTM) is developed by 624 OC/COD DCO cell; MTM includes clear guidance to tactical unit, definitive target description and unambiguous amplifying guidance. Senior Duty Officer (SDO) and SIDO review and approve MTM.

4.5.1.1.7 (ENGAGE) 624 OC/COD DCO cell transmits MTM to tactical unit.

4.5.1.1.8 (ASSESS) 624 OC/COD DCO cell analyzes the initial assessment from the tactical unit and determines if a restrike is necessary. If initial reports are positive, SIDO coordinates with follow-on intelligence, surveillance and reconnaissance (ISR) tasking and

passes info to ISR Division (ISR Division) and 624 OC/SPD Operational Assessment Team (OAT) for analysis.

4.5.1.1.9 While the 624 OC/COD is the operational lead for dynamic targeting, other OC divisions have a role to play. Each 624 OC division is responsible for determining if and/or how the threat will be addressed in follow-on missions based on their role in the development of the CTO production cycle. For more information, reference the ATO production processes outlined in *AFTTP 3-3.AOC*.

4.5.1.2 Tactical Units Role in Dynamic Targeting

4.5.1.2.1 Tactical mission leads plan for the servicing of dynamic targets during the MPC.

4.5.1.2.2 Unless otherwise directed, TSTs require coordination with 624 OC/COD during mission execution.

4.5.2 Deliberate Targeting Processes

4.5.2.1 The 624 OC will perform operational-level planning for, and task, deliberate targeting missions.

4.5.2.2 Tactical forces plan for servicing deliberate targets during the MPC. Unless otherwise stated, deliberate targets tasked by the OC do not require permission before strike actions are executed. Any target not tasked in the CTO requires coordination with COD during mission execution.

4.6 DCO Mission Types. Tactical missions are executed to achieve tactical objectives, which in turn, achieve operational objectives. Table 1, DCO Tactical Mission Types, depicts an overview of different tactical mission types and associated operational objectives. These tactical missions can be packaged together to create layered or complementary effects. Due to the variety in weapon system capabilities and areas of operations, weapon system operators uniquely conduct their tactical missions using their own TTP and processes in a way that best leverages their capabilities.

Table 1, DCO Tactical Mission Types

Tactical Mission Type	Objective
Surveillance	Collect relevant data and information in/on the AO
Reconnaissance	Collect relevant data and information on threats in the AO
Access	Provide sufficient access for supported cyber forces
Strike	Damage or destroy an objective or a capability
Escort	Provide support to cyber weapon system(s) conducting primary missions in assigned AO
Strike Coordination and Reconnaissance (SCAR)	Conduct or facilitate dynamic targeting in the AO. Includes actions conducted under other tactical missions such as Surveillance, Reconnaissance and Strike.
Secure	Enhance the defenses of the AO to mitigate risks.
Threat Emulation	Replicate realistic TTP of specific cyber threats to evaluate cyber defenses and prepare DoD DCO

4.6.1 Surveillance. The foundation for surveillance missions is based on Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* definition for surveillance “The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.” As applied to cyberspace, surveillance missions are activities involving systematic observation of assigned AO to collect data and information.

4.6.1.1 Objective: Collect relevant data and information on assigned AO

4.6.1.2 Tasks include, but are not limited to:

4.6.1.2.1 Collect and monitor network infrastructure status, changes, trends and events

4.6.1.2.2 Collect and monitor network traffic characteristics and trends

4.6.1.2.3 Collect/monitor network user characteristics and trending

4.6.1.2.4 Collect and monitor data from individual system(s)

4.6.1.2.5 Conduct technical and non-technical evaluations to identify vulnerabilities and/or risks in assigned AO

4.6.1.3 Examples:

4.6.1.3.1 Cyber Command and Control System (CSCS) operators plan and execute a mission to observe changes to network architecture (e.g., unidentified servers being activated in a network DMZ)

4.6.1.3.2 Air Force Cyberspace Defense (ACD) operators plan and execute a mission to collect and monitor system data for a network host in support of a dynamic targeting mission

4.6.2 Reconnaissance. The foundation for reconnaissance missions is based on Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* definition for reconnaissance “A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area.” As applied to cyberspace, reconnaissance missions acquire information about the activities and resources of an enemy, adversary, or threat in the assigned AO.

4.6.2.1 Objective: collect relevant data and information on threats in the assigned AO

4.6.2.2 Tasks include, but are not limited to:

4.6.2.2.1 Find and track specified enemies, adversaries, and threats in the cyber terrain

4.6.2.2.2 Understand and characterize specified enemies, adversaries, and threats in the assigned AO

4.6.2.3 Examples:

4.6.2.3.1 CPT operators plan and execute a mission to analyze AOC network traffic for specific threat indications and warnings

4.6.2.3.2 ACD or CPT operators plan and execute a mission to find a certain file associated with an adversary in assigned AO

4.6.3 Access. Access missions enable follow-on forces to achieve their mission in the assigned AO.

4.6.3.1 Objective: Provide sufficient access for supported cyber forces

4.6.3.2 Tasks include, but are not limited to:

4.6.3.2.1 Configuring firewall rules and/or policies

4.6.3.2.2 Routing configuration changes

4.6.3.2.3 Providing SSL certificates

4.6.3.2.4 Provisioning/configuring accounts

4.6.3.2.5 Configuring permission(s)

4.6.3.3 Example: CSCS operators plan and execute a mission to provide ACD operators remote access into a compromised system by allowing access through the base and host firewalls

4.6.4 Strike. The foundation for strike missions is based on the Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* definition for strike “An attack to damage or destroy an objective or a capability.” As applied to cyberspace, strike missions eliminate adversary presence in the assigned AO.

4.6.4.1 Objective: Damage or destroy an objective or a capability

4.6.4.2 Tasks include, but are not limited to:

4.6.4.2.1 Destroying resident adversary/malicious code or other artifacts in assigned AO

4.6.4.2.2 Quarantining malicious code and/or preventing code execution

4.6.4.2.3 Manipulating, denying, degrading, or disrupting adversary network traffic

4.6.4.3 Examples:

4.6.4.3.1 CSCS and ACD operators plan and execute a mission to remove adversary malware from five computers in PACAF

4.6.4.3.2 CPT tasked to neutralize a known adversary process on a compromised enclave host

4.6.4.3.3 CPT operators plan and execute a mission to limit bandwidth on an enclave host to degrade adversary movement/C2

4.6.4.3.4 ACD operators plan and execute a mission to contain potential malicious code

4.6.5 Escort. The foundation for escort missions is based on Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* definition for escort “Aircraft assigned to protect other aircraft during a mission.” As applied to cyberspace, tactical cyber units and weapon systems can provide protection, defense and support to other cyber units to assure their primary mission.

4.6.5.1 Objective: Provide defensive support to cyber weapon system(s) or mission partners conducting primary missions in the AO.

4.6.5.2 Tasks include, but are not limited to:

4.6.5.2.1 Deploying countermeasures

4.6.5.2.2 Ensuring all required forces have the necessary level of access to assigned AO during the mission vul window

4.6.5.3 Example: Adversary presence in the AO is expected; 624 OC tasks CSCS to escort ACD into the AO to assure a reconnaissance mission.

4.6.6 Strike Coordination and Reconnaissance (SCAR). The foundation for SCAR missions is based on Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* definition for SCAR “A mission flown for the purpose of detecting targets and coordinating or performing attack or reconnaissance on those targets.” As applied to cyberspace, SCAR forces are tasked to an AO or kill box and conduct dynamic targeting (e.g., F2T2EA) in response to credible adversary threat. Cross-cueing of tactical data and intelligence from other tactical cyber units and weapon system platform sensors is essential for effective execution of SCAR missions.

4.6.6.1 Objective: Conduct strike coordination and reconnaissance in response to adversary activity within the AO

4.6.6.2 Tasks include, but are not limited to:

4.6.6.2.1 Patrolling the AO, or a portion of the AO, to conduct or support strike and/or follow-on Intelligence Preparation of the Environment (IPOE) missions

4.6.6.3 Example: CPT and enterprise cyber defense forces execute SCAR patrols in the 603d Air Operations Center network during a conflict in the European Command AOR.

4.6.7 Secure. Secure missions provide mission assurance for tasked mission sets and cyber terrain. The overall goal is to conduct mission mapping, identify cyber key terrain, enhance processes to minimize vulnerabilities and counter threat.

4.6.7.1 Objective: Enhance the defenses of the assigned AO in response to active threats.

4.6.7.2 Tasks include, but are not limited to:

4.6.7.2.1 Enhancing the defenses of cyber key terrain

4.6.7.2.2 Reconfiguring network appliances to a more secure configuration in response to active threats

4.6.7.3 Example: AFCYBER forces plan and execute a mission to reconfigure industrial control system (ICS) network to make it more secure.

4.6.8 Threat Emulation. Threat emulation missions replicate a realistic adversary and threat tactics, techniques and procedures (TTP) to evaluate cyber defenses. Threat emulation missions often support secure missions or exercise scenarios.

4.6.8.1 Objective: Replicate realistic TTP of specific cyber threats to evaluate cyber defenses.

4.6.8.2 Tasks include but are not limited to:

4.6.8.2.1 Emulate known adversary TTP

4.6.8.2.2 Identify unmitigated vulnerabilities

4.6.8.2.3 Assesses defensive posture and processes

4.6.8.3 Example: CPT forces plan and execute a mission to conduct threat emulation against the AF Satellite Control Network program management office (PMO) systems.

5. Tactical Mission Planning.

5.1 *Air Force Instruction 10-1703, Volume 3, Cyberspace Operations and Procedures* mandate an appropriate amount of mission planning be conducted prior to each mission. ME3C-(PC)² is the AF standard planning framework for tactical missions and is codified in *AFTTP 3-1.General Planning*.

5.2 The ME3C-(PC)² tactical planning framework is used by the MPC for planning (either as part of an LFE or single-ship mission). For more information, reference *AFTTP 3-1.General Planning* or the *24 AF, AFCYBER & JFHQ-C AFCYBER Tactical Mission Planning, Briefing and Debriefing Guide*.

6. Force Presentation

6.1 The fundamental concept for tasking capability and capacity is similar across all Services and joint operations: forces are presented to commanders for operational tasking; commander intent and desired end-state are provided to scope operations; presented forces are apportioned and tasked to conduct operations through a respective operations center. Adopting this methodology ensures CDR AFCYBER maintains situational awareness on all assigned forces.

6.2 The following framework presents AFCYBER force capability and capacity by identifying:

6.2.1 Unit and associated cyber weapon system (WS) or capability

6.2.2 Tactical mission type and relevant unit/WS

6.2.3 Number of sorties that a unit/WS can generate in a vul window

6.2.4 Assigned sortie duration (ASD) for each mission type

6.2.5 Availability for tasking; based on Zulu time, ASD, unit location/time zone, and unit capacity

6.2.6 Total number of sorties, by type, capable of being generated in a 24-hour period/day (e.g., 4x Air Force Intranet Control (AFINC) reconnaissance sorties per 24-hour period)

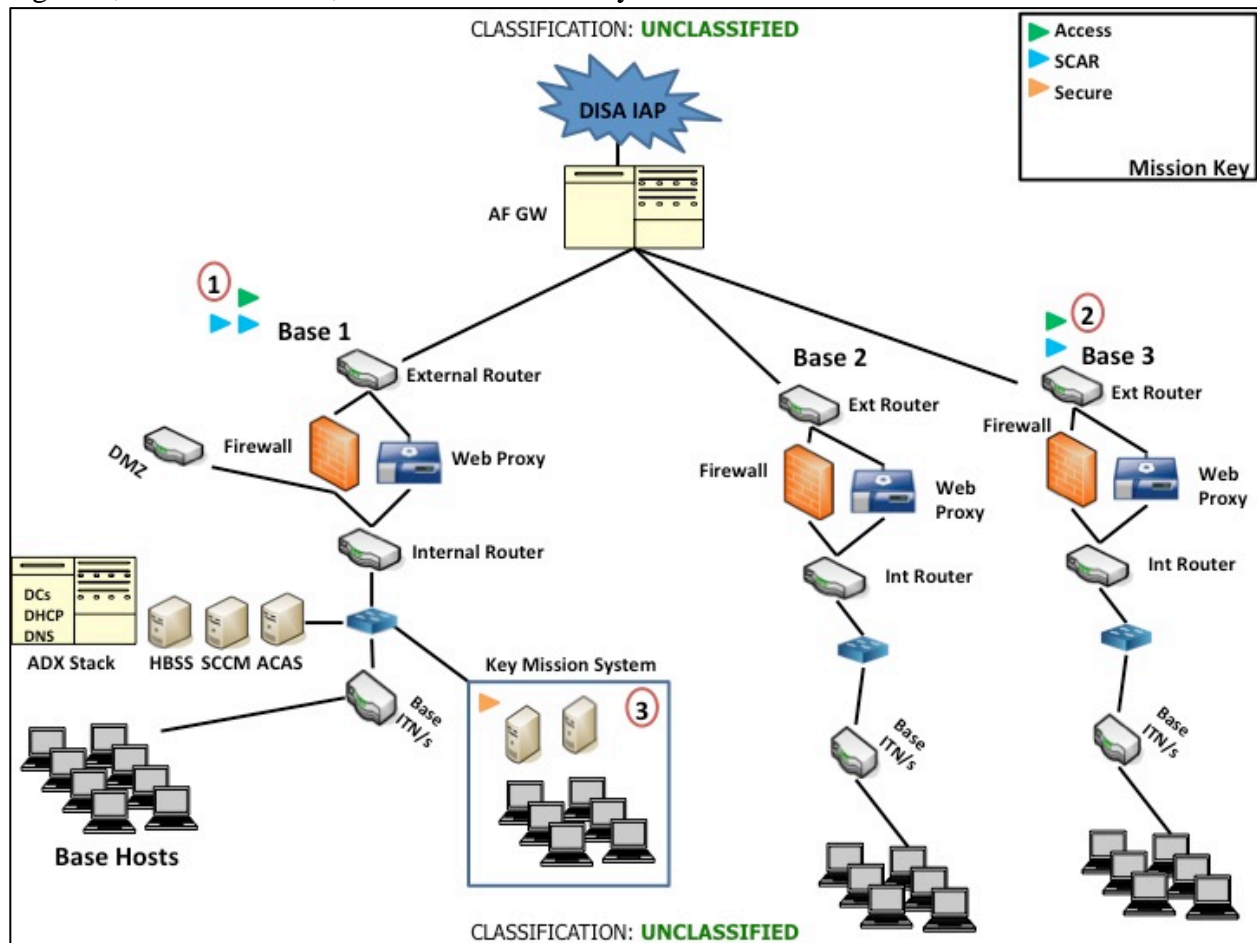
6.3 Based on this framework, operations centers and unit commanders will have an accurate representation of capability and capacity to conduct cyberspace operations.

7. DCO Mission Thread

The following mission thread provides a scenario that employs the concepts outlined in this DCO CONEMP. Figure 2, Mission Thread, Tasked Forces for day-1, depicts the AO on day-1 of a 4-day dynamic targeting mission as well as secure missions on a key mission system. Additionally:

- An AF gateway is present between the DoDIN and the AFIN.
- There are three bases in this AO: Base #1, Base #2, and Base #3.
- The blue order of battle on day-1 is as follows.
 - Base #1 and Base #3 have tactical AFCYBER DCO forces conducting access and SCAR missions.
 - Base #1 has an access mission with two individual SCAR missions paired together as a SCAR package at the base boundary (1)
 - Base #3 only has a single-ship access and SCAR mission (2)
 - Base #1 has a CPT conducting a secure mission on its key mission systems (3)

Figure 2, Mission Thread, Tasked Forces for day-1



DCO CONEMP Mission Thread Planning and Briefing

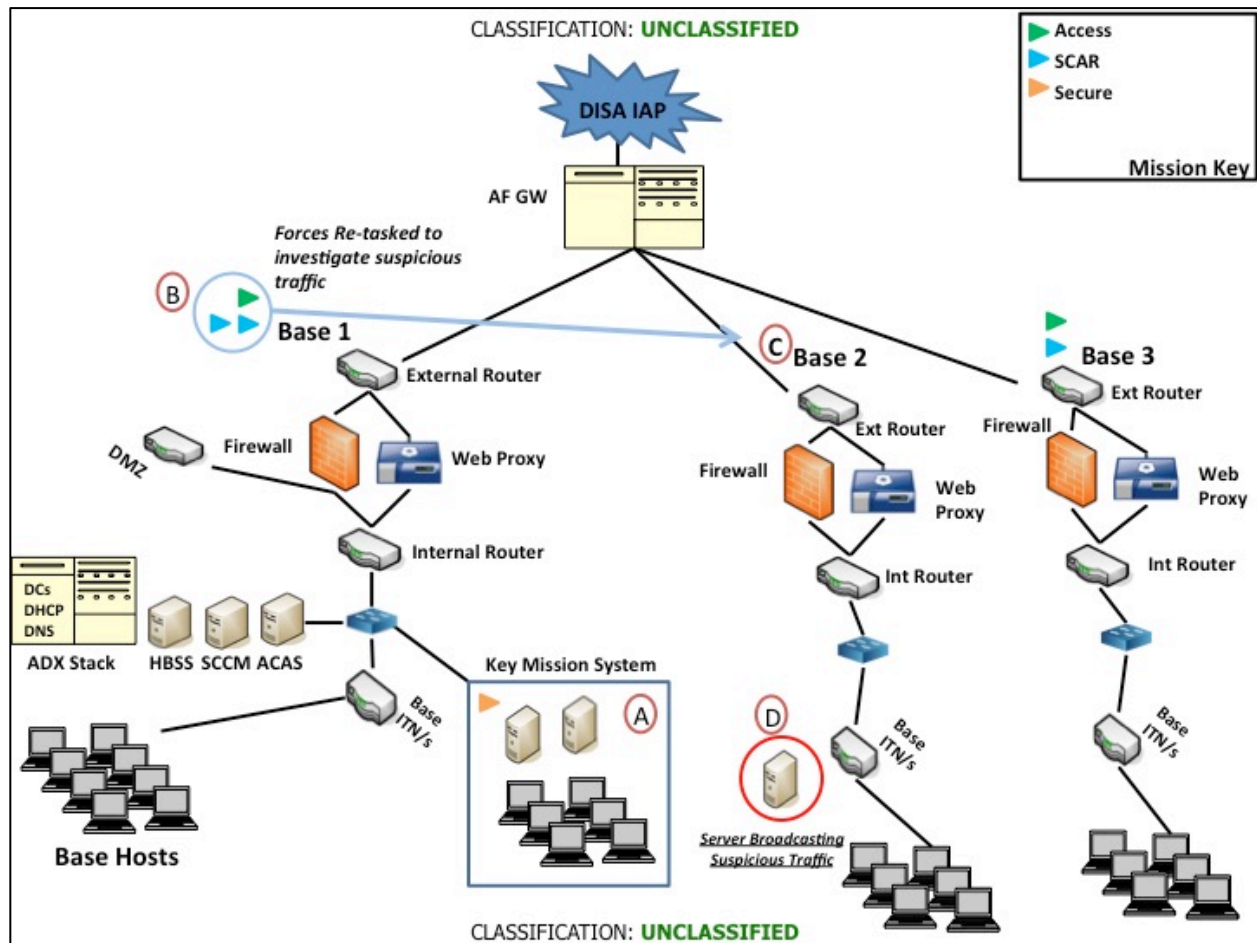
Following a 72-hr CTO cycle, operational planning of the DT mission is completed, briefed, and approved two days prior to execution. The 624 OC/SPD releases the draft CTO at least 24 hours prior to execution outlining taskings for the missions to be executed on day-1. The MPCC for the DT mission then uses tactical planning processes in an MPC to develop the tactical mission plan. During this planning, coordination between the MPC and 624 OC/SPD ensures that any required changes to the CTO to execute the tactical plan are incorporated. Prior to vul start on day-1, the designated MC conducts the cyber boss brief and upon approval, the mass brief to all forces executing access and SCAR missions at the base boundaries (see appendix for more information on the cyber boss brief and mass brief). Tactical forces complete their own pre-mission briefs before execution as well. At vul start, all the tactical cyber forces would begin executing the tactical mission plan on day-1. The CTO would also include taskings for the secure missions being executed on day-1. This is a typical daily planning, briefing and tasking cycle that would be employed each day.

Day-1 Execution and Debrief

Execution of day-1 starts as planned. However, during mission execution, the CPT performing a secure mission at Base #1 detects a potential emerging target of opportunity. One of the hosts in

the key mission enclave is receiving suspicious traffic that appears to be coming from a server at Base #2 (A). To engage this target of opportunity, the alert is cross-cue with the MC and 624 OC/COD. The MC is directed by 624 OC/COD to pull his forces at the Base #1 boundary (B) performing SCAR patrols and dynamically redirect them to the Base #2 boundary (C) and at the server (D). The MC directs one of the elements performing SCAR at Base #1 to Base #2 boundary (B) → (C) to coordinate strike actions. The MC also directs the access mission's forces and the other SCAR element forces to the server (B) → (D) to potentially strike any malicious code or processes on the server. This tactical maneuvering is illustrated in Figure 3, Mission Thread, Tactical Force Maneuvers.

Figure 3, Mission Thread, Tactical Force Maneuvers



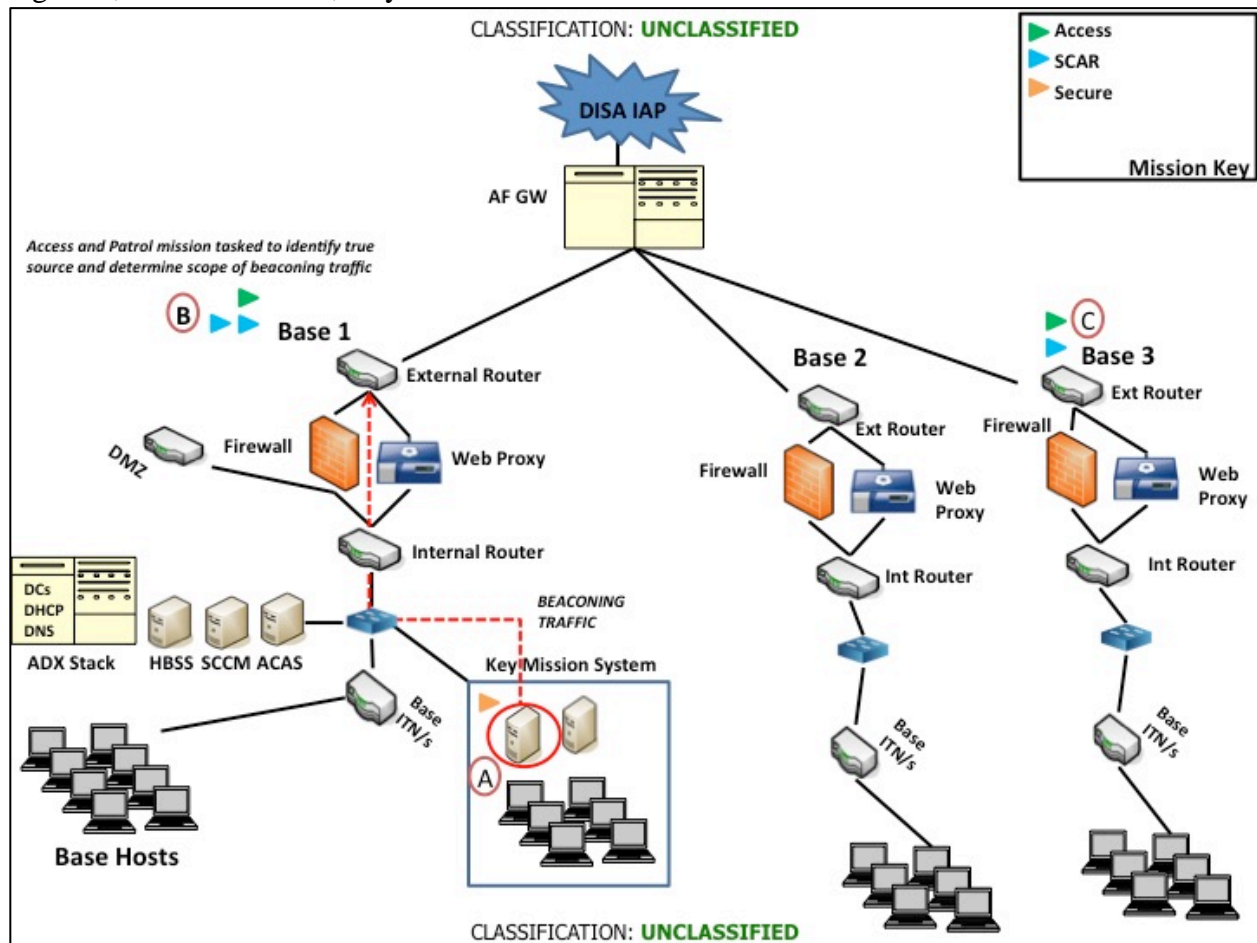
After employing their capabilities to identify and characterize the suspicious traffic at Base #2's boundary and look for malicious code or processes on the server, nothing of significance was identified. The tactical forces then report back to the MC, at which point he redirects them back to their original mission at the Base #1 boundary. Upon completion of the missions, MISREPS are submitted to the OC, and debriefs are conducted by all tactical units that executed that day. For the DT mission, the MC conducts a mass debrief with all the forces involved. All debriefs are conducted using detailed reconstruction from execution logs. After summarizing and

assessing execution, any LL are identified and recorded to improve future planning efforts and execution. This concludes day-1 DCO operations.

Day-2 Execution and Debrief and Day 3 Tactical Mission Planning

Day-2 execution also begins as planned. During mission execution, a National Security Agency Threat Operations Center (NTOC) tipper is received by SIDO that a medical server, one of Base #1 key mission systems (A), has potentially been compromised. The CPT has the preponderance of tasks and SA in that AO and is appointed by the 624 OC to lead the response effort. The CPT mission lead requests enterprise DCO force support from 624 OC. The 624 OC directs forces from to support the CPT. The CPT team lead coordinates with the MC of the DT mission and forces performing a SCAR mission at Base #1 boundary are redirected to conduct reconnaissance and strike on enemy C2 traffic at Base #1 boundary (B). Additionally, the forces conducting access and SCAR missions at Base #3 boundary are redirected to engage enemy presence on the medical server (C). The SCAR mission at the Base #1 boundary positively identifies the enemy C2 channel and interdicts the traffic, and the access/SCAR mission at the host validates that the server has been compromised and conducts strike actions and eliminates the malicious code. In conducting their missions, additional C2 traffic from one other host on Base #1 was identified. There is reason to believe that lateral movement has occurred. At this time, the vul period concludes and MISREPs are sent to 624 OC. Figure 4, Day 2 Tasked Forces and Execution depicts the sequence of events for day-2.

Figure 4, Mission Thread, Day-2 Tasked Forces and Execution



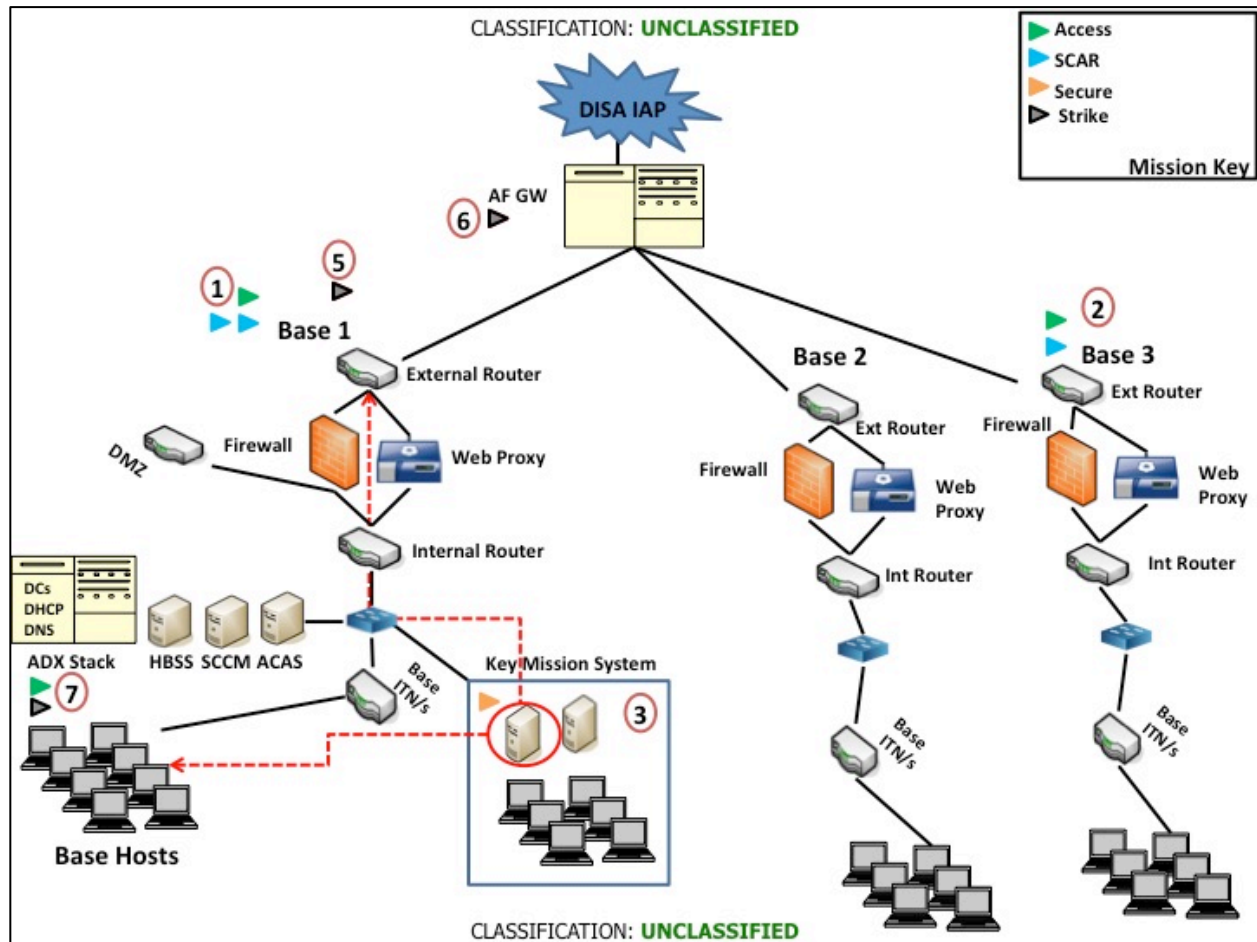
These MISREPs influence day-3 draft CTO taskings and tactical mission planning. The CTO for day-3 tasks an additional strike mission at the base boundary and an access and secure mission at the compromised host to engage the increased scope of lateral movement across Base #1. However, the MPC identifies a need for an additional strike mission at the AF gateway to leverage capabilities there. That need is conveyed to 624 OC/SPD and incorporated into the CTO for day-3. Since enterprise forces have the preponderance of mission and SA, they are the MC for day-3. Day-3 blue order of battle is depicted in Figure 5, Mission Thread Day-3 Tasked Forces and Execution, and is as follows.

- Base #1 and Base #3 have tactical AFCYBER DCO forces conducting access and SCAR missions
 - Base #1 has an access mission with two individual SCAR missions paired together as a SCAR package at the base boundary (1)
 - Base #3 has access and SCAR missions (2)
- Base #1 has a CPT conducting a single-ship secure mission on Base #1 key mission systems (3)
- In response to the expanded scope of lateral movement on Base #1:

CLASSIFICATION: **UNCLASSIFIED**

- Two strike missions, one at the base boundary (because there are deliberate targets from day-2 MISREPs) (5) and one at the AF Gateway (6)
- An access and strike mission to engage lateral movement hosts identified in day-2 MISREPs (7)

Figure 5, Mission Thread Tasked Forces for Day-3



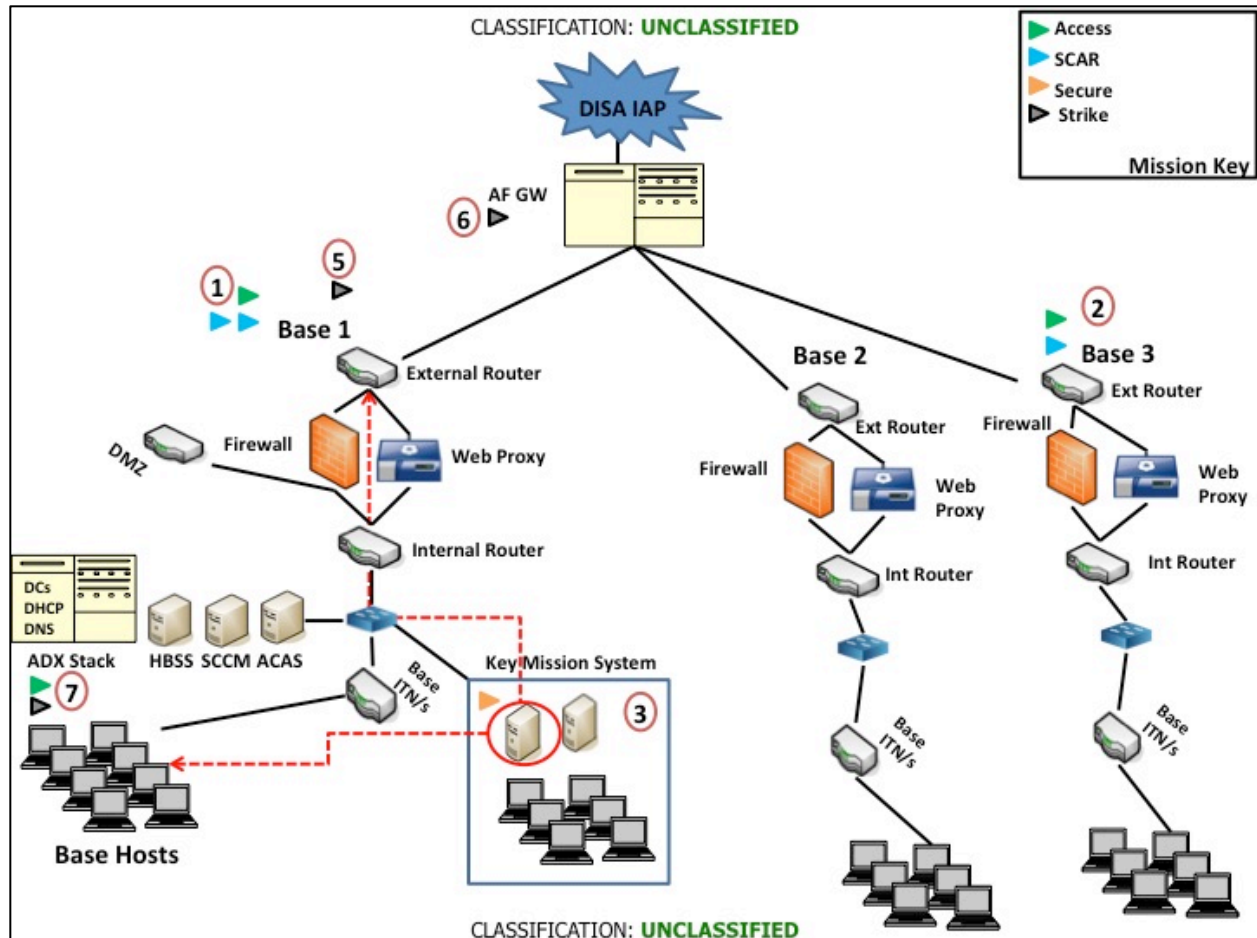
Day 3 Execution and Debrief and Day 4 Tactical Mission Planning

Day 3 execution begins as planned. The DT and secure missions are executed similar to days 1 and 2. To counter the lateral movement identified in day-2, the strike missions at the Base #1 boundary (5) and the AF gateway (6) interdict the C2 channel traffic from the target host identified in day-2. Access and strike missions engage the target on the compromised host (7). The missions execute as planned and MISREPs are sent to 624 OC at the end of the vul window. When conducting the strike mission at the AF gateway (6), a reconnaissance action was taken by the tactical forces that identified similar traffic egressing Base #2 and Base #3. Since this is identified during execution, information is tactically cross-cued to the MC and 624 OC/COD, which considered engaging these targets. The OC and MC assesses there are not enough tasked forces to engage all the targets and that additional planning is required to respond to the AFIN-wide compromise. The MC and 624 OC/COD decide to complete the current day's mission and

CLASSIFICATION: **UNCLASSIFIED**

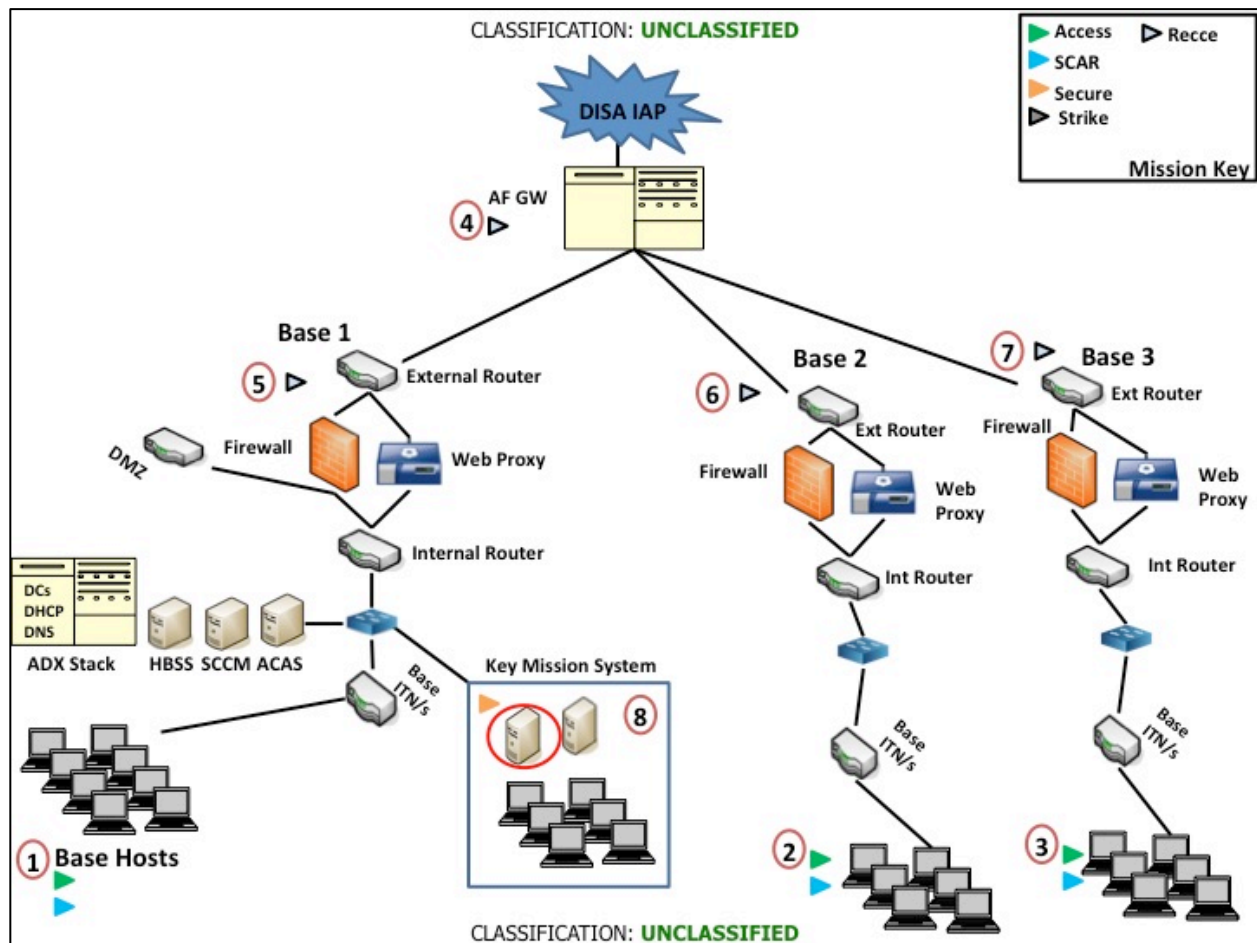
624 OC/SPD and the MPCC begin planning for day-4 execution, which will sweep all three bases. Day-3 execution ends. Figure 6, Mission Thread Day-3 Execution depicts the day-3 mission events.

Figure 6, Mission Thread Day-3 Execution



Based on the objectives and tasks in the CTO, the MPC develops a plan for day-4 to have a phased approach to engage targets on all three bases. The plan consists of an access and SCAR mission for each of the bases (1) (2) (3) to engage known targets and sweep for additional hosts that are compromised with this malicious code. Additionally, reconnaissance missions (5) (6) (7) are tasked for all the base boundaries and the AF gateway (4) to tactically cross-cue any C2 channel traffic identified with the characteristics of the compromised medical server and host to the forces conducting sweeps of base hosts. The secure missions (8) continue to be tasked.

Mission Thread Figure 6 – Tasked Forces for Day 4



Day 4 Execution

Day 4 execution begins and executes according to plan. The phases of the plan are executed across all three bases and with tactical cross-cue from the reconnaissance missions at the bases and AF gateways. At the end of day-4 vul periods, the threat has been eradicated from the AF networks. Tactical units submit MISREPS to the OC and conduct their debriefs.

8. Responsibilities.

8.1 24 AF/AFCYBER will:

8.1.1 Present guidance and assist with the development of all primary reference documents for missions which include at a minimum: C2 relationships to include Direct Liaison Authorized (DIRLAUTH) relationships, SPINS, PAAs and ROEs.

8.1.2 Issue orders as required for DCO missions.

8.1.3 Prioritize operational objectives in the CyOP.

8.1.4 Liaise with Air National Guard (ANG) and Air Force Reserve Command (AFRC) mission partners to develop agreements for ANG/AFRC force presentation and tasking processes ISO AFCYBER DCO missions.

8.2 624 OC will:

8.2.1 Oversee development of all primary reference documents for missions which include at a minimum:

8.2.1.1 Communication plans

8.2.1.2 DIRLAUTH relationships

8.2.1.3 SPINS, PAAs and ROEs

8.2.1.4 Tactical Objectives based on Strategic and Operational Objectives (Appendix E)

8.2.1.5 Sub-tasks within the CTO

8.2.2 Identify Measures of Performance (MOPs) and Measures of Effectiveness (MOEs) unique for each mission and associated taskings.

8.2.3 Provide the CTO to tasked units 48 hours prior to mission execution.

8.2.4 Direct dynamic targeting missions within the AO.

8.2.5 Coordinate and direct dynamic, time sensitive operational mission execution, when required.

8.2.6 Standardize reporting requirements for Situation Reports (SITREPs) during mission execution and Mission Reports (MISREPs) at mission completion.

8.2.7 During LFE operations, assign different MCs (may be assigned to the same unit) across consecutive CTO days to allow for effective planning/debriefing.

8.2.8 Prioritize AFCYBER DCO objectives in the CyOD.

8.2.9 Liaise with Air Force Office of Special Investigations (AFOSI) on law enforcement and counter-intelligence matters.

8.2.10 Coordinate with AOCs for DCO support.

8.3 Cyberspace Wings and Direct Report Groups will:

8.3.1 Provide trained/certified tactical mission/crew commanders and any other AFCYBER (67 CW, 688 CW, 5 CCG) expertise necessary to ensure mission plans,

communications contracts, reporting guidance, DIRLAUTH relationships, and PAAs required for pre-mission coordination is completed and approved IOT generate the appropriate language in the publication of the SPINS developed by the 624 OC.

8.3.2 Execute/support missions as directed by 624 OC.

8.3.3 Establish a process to provide force availability and capacity daily to the 624 OC. The established process will account for changes to previously advertised force availability and capacity.

8.3.4 Force availability and capacity will be advertised to the 624 OC daily by 1600 Zulu and will be presented 72 hours in advance. Changes to force availability will be provided immediately to the 624 OC via the established process mentioned above.

8.3.5 For LFE operations, assign different MCs across consecutive CTO days to allow for effective planning/debriefing.

8.3.6 Provide certified and experienced mission-ready crew members to assist the 624 OC in operational mission planning.

8.3.7 Ensure tactical commanders have real-time communication capabilities with 624 OC during all missions.

8.3.8 Ensure tactical commanders establish real-time communication with 624 OC during mission execution.

8.3.9 Provide SITREPs and MISREPs to 624 OC as required.

8.3.10 Facilitate MPCs and appoint MPCCs, as needed.

8.3.11 Provide certified and experienced mission-ready crew members to assist the MPC in tactical mission planning.

APPENDIX A - Glossary of Terms

Apportionment — In the general sense, distribution of forces and capabilities as the starting point for planning. (JP 5-0)

Assessment — 1. A continuous process that measures the overall effectiveness of employing joint force capabilities during military operations. 2. Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. (JP 3-0)

Assigned Sortie Duration (ASD) — Weapon system-specific mission duration based on mission type. (AFI 11-102)

Campaign — A series of related major operations aimed at achieving strategic and operational objectives within a given time and space. (JP 3-30)

Commander's Intent — A clear and concise expression of the purpose of the operation and the desired military end state that supports mission command, provides focus to the staff, and helps subordinate and supporting commanders act to achieve the commander's desired results without further orders, even when the operation does not unfold as planned. (JP 3-0)

Contingency (operational) — In operational planning, a situation requiring military operations in response to natural disasters, terrorists, subversives, or as otherwise directed by appropriate authority to protect US interests. (JP 5-0)

Contingency (tactical) — In tactical planning, a planning consideration such as a change in weather, unexpected terrain variables, etc., that requires a plan or procedure for mitigation.

Crew — Also referred to as cybercrew members, consist of individuals who conduct cyberspace operations or computer network exploitation and are typically assigned to a specific weapon system. (Definition derived from "aircrew" ACPD 11-4)

Cyber-Boss — Cyber-boss is the individual who approves the tactical execution of the plan. By the nature of the tasking order, the operational organization has already approved/ordered the mission. The purpose of the cyber-boss brief is to allow for final vector check that the tactical plan is consistent with the operational objectives. Consistent with other AF operational communities, the cyber boss should be the squadron commander or director of operations, of the mission lead.

Cyberspace — A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)

Cyberspace Operations (CO) — The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. (JP 1-02)

Day — Unless otherwise specified, "day" means calendar days. When "work days" are specified,

count only duty days. (AFI 10-1703, Vol 1)

Effects — 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. (JP 3-0)

Large Force Employment (LFE) — Multiple weapons systems or forces executing mutually supportive mission types in the same AOR during the same vul period on the same or overlapping AO.

Measures of Effectiveness (MOE) — A criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (JP 1-02)

Mission — 1. The task, together with the purpose, that clearly indicates the action to be taken and the reason therefore. (JP 3-0) 2. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task. (JP 3-0) 3. The dispatching of one or more aircraft to accomplish one particular task. (JP 3-30)

Objective — 1. The clearly defined, decisive, and attainable goal toward which every operation is directed. 2. The specific target of the action taken which is essential to the commander's plan. (JP 1-02)

Operation — 1. A sequence of tactical actions with a common purpose or unifying theme. (JP 1) 2. A military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission. (JP 3-0)

Rules Of Engagement (ROE) — Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. (JP 1-04)

Task — A clearly defined action or activity specifically assigned to an individual or organization that must be done as it is imposed by an appropriate authority. (JP 1)

Weapon System — A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency. (JP 1-02)

APPENDIX B - Acronyms

24 AF/CC - Commander, 24th Air Force	LP - Learning Point
624 OC - 624th Operations Center	MAJCOM - Major Command
AFFOR - Air Force Forces	MBA - Main Battle Area
AFIN - Air Force Information Networks	MC - Mission Commander
ALR - Acceptable Level of Risk	MDS - Mission Design Series
AMAC - AFIN Mission Assurance Center	ME3C-(PC) ² - Mission, Environment, Enemy, Effects, Capabilities, Plan, Phasing, Contracts, Contingencies
ANG - Air National Guard	MINFORCE - Minimum Forces
AOR - Area of responsibility	MISREP - Mission Report
ASI - Authorized Service Interruption	MLR - Main Line of Resistance
BPT- Be prepared to	MOE - Measurement of Effectiveness
C2 - Command and Control	MOP - Measurement of Performance
CACA - Criteria, Authority, Communication, Actions	MPC - Mission Planning Cell
CC - Commander	MPCC - Mission Planning Cell Chief
CCDR - Combatant Commander	MSN - Mission
CCO - Cyberspace Control Order	MSL - Master Station Log
CDR - Commander	NAF - Numbered Air Force
CDRAFCYBER - Commander, AFCYBER	NATO - North Atlantic Treaty Organization
CDRUSCYBERCOM - Commander, USCC	NKE - Non-Kinetic Effects
CDRUSSTRATCOM - Commander, USSC	NOS - Network Operations Squadron
CFP - Communications Focal Point	OCO - Offensive Cyber Operations
COA - Course(s) of Action	OC - Operations Center
CPT - Cyber Protection Team	OPORD - Operation Order
CTO - Cyber Tasking Order	PAA - Pre-approved Action
CyOD - Cyber Operations Directive	PBED - Plan, Brief, Execute, Debrief
CyOP - Cyber Operations Plan	PC - Package Commander
DCO - Defensive Cyber Operations	PID - Positive Identification
DFP - Debrief Focus Point	PMO - Program Management Office
DISA - Defense Information Systems Agency	POA&M - Plan of Actions and Milestones
DMC - Deputy Mission Commander	POL/MIL - Political/Military
DMPCC - Deputy Mission Planning Cell Chief	POND - Period of non-disruption
DoD - Department of Defense	RFF - Request for forces
DoDIN - DoD Information Networks	RFS - Request for support
FEBA - Forward Edge of the Battle Area	ROC - Rehearsal of Concept
FRAG - Fragmentary Order	ROE - Rules of engagement
GICL - Good Idea Cut-off Line	SA - Situational Awareness
GP - General Planning	SCAR - Strike Coordination and Reconnaissance
HGI - How Goes It	SITREP - Situation Report
HVAC - Heating, Ventilation and Air Conditioning	SPINS - Special Instructions
IGL - Intelligence Gain/Loss	SPO - Special Project Office
IN - Intelligence	TACREP - Tactical Report
IOT -In order to	TCNO - Time Compliance Network Order
ISO - In support of	TGL - Technical Gain/Loss
ITO - Integrated Tasking Order	TOT/T - Time over Target/Terrain
JIE - Joint Information Environment	TO - Technical Order
JRE - Joint Regional Enterprise	USCC - United States Cyber Command
JRSS - Joint Regional Security Stack	USSC - United States Strategic Command
KIO - Knock It Off	VUL - Vulnerability
LFE - Large Force Employment	WCC - Wing Coordination Center
LL - Lesson Learned	WRT - With Respect/Regard To
LO - Lesson Observed	

APPENDIX C - Strategy to Task

Planning Artifact	Document	Publication Frequency	Office of Primary Responsibility	
Strategic Objectives	CyOP or Campaign Plan (CP)	CyOP - Every 6 months CP - As needed	624 OC/SPD 24 AF/A5	624 OC (Operational Level)
Operational Objectives	CyOD	Weekly	624 OC/SPD	
Tactical Objectives	CyOD and CTO	Weekly or Daily	624 OC/SPD	
Measures of Effectiveness	CyOD	Weekly or Daily	624 OC/SPD Operational Assessment Team	
Tactical Tasks	Tactical Mission Plan	Daily	CPT Network Warfare Cyber Planner or MPCC	Tactical Units (e.g. CPTs, ACD, AFINC, CSCS) (Tactical Level)
MPC Tactical Tasks - Measures of Performance	Tactical Assessment Plan and MISREP	Daily	CPT Network Warfare Cyber Planner or MPCC	

Table 3 - AFCYBER Strategy to Task Planning and Tasking Artifacts

Strategy to Task Example

Strategic Objective (SO): USANYCOM is able to execute Ballistic Missile Defense (BMD) ops in support of US policy objectives, theater strategic plan and specified OPLANs during steady state and crises.

Example Operational Objective (OO): USANYCOM's BMD Cyber-Key Terrain (C-KT) is free of Tier II and III Cyber Threats Actors during phases 1-3 (Deter, Seize the Initiative, Dominate).

Example Tactical Objective (TO): "Protect the use of Remote Desktop Protocol (RDP) from malicious use on assigned AO."

Example Tactical Tasks (TT):

Secure Mission:

- 1.1 Identify what endpoints are allowed to be managed via RDP (Identify)
- 1.2 Update risk / network model with authorized RDP endpoints
- 1.3 Validate updated risk/network model with mission owner cyber support / System administrators
- 1.4 Identify the list of administrators and other authorized RDP users (Identify/Characterize)
- 1.5 Develop Group Policy Object (GPO) to prevent unauthorized users from using RDP (Mitigate)
- 1.6 Ensure Windows Event Log auditing logs successful and failed RDP sessions (Identify)

Strike Coordination and Reconnaissance:

- 2.1 Identify RDP sessions from network traffic analysis (Identify)
- 2.2 Identify RDP sessions from host artifacts (Identify)
- 2.3 Identify potentially malicious RDP activity (Characterize)
- 2.4 Execute PAAs to respond to malicious RDP activity (Strike)

CPT Cyber Threat Emulation:

- 3.1 Exercise use of inactive user credentials to RDP to key servers [Tier III threat emulation] (Validate)
- 3.2 Exercise use of user credentials to RDP to key servers [Tier III threat emulation] (Validate)
- 3.3 Exercise use of stolen/copied legitimate administrator credentials to RDP to key servers from an unauthorized source host not ever used to administer such key servers [Tier II threat emulation] (Validate)

Surveillance (ACD Example):

- 4.1 Identify any attempted or successful RDP sessions to or from Lackland AFB IP space and pass 5-Tuple data sets (Src IP/Dest IP/Src Port/Dest Port/UTC Time) via chat to CPT forces upon discovery

Surveillance (AFINC Example):

- 5.1 Configure firewalls to monitor for RDP egressing the AFNET on non-standard ports (not TCP 3389)

Reconnaissance (Cyberspace Defense Analysis (CDA) Example):

- 6.1 Identify content egressing the AFNet which contains USANYCOM's RDP configurations
- 6.2 Conduct research to identify if any of USANYCOM's RDP or Microsoft Terminal Services configurations are posted/accessible anywhere on the Internet (e.g., google searches, pastebin, etc.)

APPENDIX D - Cyberspace LFE Foundations

Operation MONGOOSE WEDGE (OMW). DCO LFE concept development had its genesis as part of OMW. AFCYBER forces were tasked to identify/characterize domain name service (DNS) connections attempting to resolve to suspected advanced persistent threat (APT) hosted domains and IP space. The operation was significant because it marked the first-ever use of an enterprise-level DCO MC, tasked through the CTO with planning and executing tactical-level operations, including timing and deconfliction across multiple cyberspace weapon system platforms. Operational-level C2 elements included delegated special instructions (SPINS), rules of engagement (ROE), pre-approved actions (PAA), and decision matrixes for tactical execution.

Operations Linoleum Needle (OLN) and Cobalt Needle (OCN). Successful OMW execution led leadership to direct the planning and execution of a series of local exercises (OLN) designed to expand on OMW LL and validate force package concepts, ROE, etc., associated with LFE employment. These initiatives were later continued by the 624 OC under OCN.

DCO LFE Operations and Lessons Learned. Lessons learned (LL) from early LFE events were directly applied to subsequent operations.

Operation FLYING MONKEY (OFM) – Countering APT attempts to compromise AF public facing networks. OFM LL led to capacity constructs and the clarification of C2 constructs.

Operation PHANTOM FORTRESS (OPF) – Countering APT SQL injection techniques. OPF LL drove AFCYBER to formalize Operational Planning Team (OPT) processes and increase tactical unit participation in operational level planning.

Operation COBALT CASTLE (OCC) – Countering APT spear-phishing techniques. OCC LL drove AFCYBER to refine campaign planning and assessment processes.

Operation HEARTBLEED (OHB) – Survey the AFIN to identify and remediate vulnerabilities associated with weaknesses in Open Secure Socket Layer (SSL) protocol implementation. OHB LL led to the development of daily DCO tasking orders.

Operation SAVAGE KNIGHT (OSK) – An intel-driven collection operation to detect and defend against SQL injection attempts. OSK was also significant because it proved the concept of daily rotating MCs and MPCCs for DCO LFE missions.

Operation COBALT SIRIUS (OCS) – Survey the AFIN to identify and remediate vulnerabilities associated with weaknesses in secure shell (SSH) implementation. OCS LL highlighted the need for enduring missions to be campaign managed by the operational C2 entity vice allowing tactical units to manage campaign progress and generate tactical unit tasking.

Operations CRAFTY HORNET, CRAFTY WASP, CRAFTY EAGLE and CRAFTY SCORPION – Employing AFCYBER Enterprise forces in conjunction with CPTs in a phased approach to defend critical C2 nodes. LL from the CRAFTY series of missions drove tighter integration between CPT and enterprise DCO forces.

APPENDIX E - References

1. AFI 10-1701, *Command and Control (C2) For Cyberspace Operations*
2. AFI 10-1703v1, *Cybercrew Training*
3. AFI 10-1703v2, *Cybercrew Standardization and Evaluation Program*
4. AFI 10-1703v3, *Cyberspace Operations and Procedures*
5. AFRD 10-17, *Cyberspace Operations*
6. AFSPC GM 10-03, *Operations*
7. AFSPCI 10-415, *Weapons and Tactics Program*
8. AFTTP 3-1.General Planning
9. AFTTP 3-1.CWO
10. AFTTP 3-1.Threat Guide
11. AFTTP 3-1.ACD
12. AFTTP 3-3.AOC
13. CMF CFCOE and Annexes
14. FB 12-12, *Defensive Cyberspace Operations-Tactical Coordinator*
15. FB 14-19, *Defensive Cyber Operations Large Force Employment Considerations*
16. FB 15-12, *The Taxonomy of a Defensive Cyber Mission*
17. MULTI-SERVICE BREVITY CODES, AFTTP 3-2.5, September 2014
18. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*

APPENDIX F - Contributing Authors.

The following individuals assisted in writing and preparing this CONEMP:

Lt Col John Moesner	624 OC/SPD
Maj Angela Waters	92 IOS/DO
Capt Erik Brown	92 IOS/DOK
Capt Christopher Chin	83 NOS/DOK
Capt Joseph Citro	33 NWS/DOK
Capt Jay Crawford	624 OC/COD
Capt Donald Franklin	26 OSS/OSK
Capt Daryl Godfrey	624 OC/SPD
Capt Eric Griffin	624 OC/COD
Capt Nathaniel Kendall	318 OSS/OSK
Capt Robert Mayo	561 NOS/DOK
Capt Casey Miller	24 AF/A5I
Capt Adam Scheuer	26 OSS/OSK
Capt Jeremy Sparks	24 AF/A3TW
Capt Andre Wolf	624 OC/SRD
Capt Christopher Wong	26 NOS/DOK
1Lt David Burton	38 CYRS/SCO
1Lt Leonard Schoonover	561 NOS/DOK
1Lt Kristopher Whitmire	318 OSS/OSK
SSgt Mark Frailey	624 OC/SPD
Mr. Jason Buster	24 AF/A5X
Mr. Jim Lance	624 OC/COD
Mr. Brian MacDougald	26 OSS/OSK
Ms. Stacey Mitchell	39 IOS/Det 1
Mrs. Lacey Moen	24 AF/A5X
Mr. John Partain	318 OSS/OSK
Mr. Andrew Pippin	318OSS/OSK
Mr. Dave Purkiss	26 OSS/OSK
Mr. Kevin Rook	24 AF/A3TW