

UNCLASSIFIED



# **Functional Concept for Cyberspace Operations**

**14 JUNE 2010**

**FINAL**

Distribution authorized to United States Government agencies and their contractors; Administrative or Operational Use. Other requests for this document shall be referred to HQ AFSPC/A8X.

---

UNCLASSIFIED

THIS PAGE INTENTIONALLY LEFT BLANK

# Air Force Space Command Functional Concept for Cyberspace Operations

**Submitted by:**

JOHN W. RAYMOND  
Brigadier General  
Director of Plans, Programs and Analyses

**Approved by:**

A handwritten signature in black ink, appearing to read "Michael J. Basla", is written over a horizontal line.

MICHAEL J. BASLA  
Major General  
Vice Commander, Air Force Space Command

THIS PAGE INTENTIONALLY LEFT BLANK

**REVIEW/CHANGE LOG**

Date	Description	OPR
14 June 2010	Original Document	HQ AFSPC/A8X

THIS PAGE INTENTIONALLY LEFT BLANK

## FOREWORD

*“Space and cyberspace capabilities are, in fact, critical to modern military operations and provide the US military with an advantage over our adversaries. It’s important that we maintain and sustain that advantage.”*

**General C. Robert Kehler, Commander AFSPC**

Clear, precise functional concepts are critical to describe the capabilities Air Force Space Command (AFSPC) must provide to the joint warfighter. Functional concepts explain in detail how capabilities and effects shape the operational environment from today through 2030. These concepts link AFSPC capabilities to the desired effects found in the family of Joint Concepts and the AF-level Concepts of Operations (CONOPS)/Air Force Operating Concepts (AFOpsCs) by providing a common understanding of how each capability contributes to achieving the joint warfighter effects required by our combatant commanders. AFSPC Functional Concepts are foundational documents for the AFSPC capability-based planning process (i.e., Integrated Planning Process), which feeds the AF Annual Planning and Programming Guidance (APPG), Capability Review and Risk Assessment (CRRA) and Planning, Programming, Budgeting, and Execution (PPBE) cycle. This traceability from desired warfighter effects through AFSPC capabilities is leveraged further by AFSPC Enabling and Operating Concepts that are used in the requirements development (i.e., Joint Capabilities Integration and Development System) and acquisition (Defense Acquisition System) processes.

THIS PAGE INTENTIONALLY LEFT BLANK

**TABLE OF CONTENTS**

FOREWORD.....	vii
TABLE OF FIGURES.....	x
1.0 PURPOSE .....	1
2.0 OVERVIEW .....	2
2.1 Background .....	2
2.2 Summary .....	8
3.0 SITUATION.....	9
3.1 Time Horizon .....	9
3.2 Military Challenges .....	9
3.3 Assumptions.....	11
3.4 Risks.....	12
4.0 SYNOPSIS .....	13
4.1 Desired Effects .....	13
4.2 Missions .....	15
5.0 NECESSARY AND ENABLING CAPABILITIES .....	18
5.1 Necessary Capabilities .....	18
5.2 Enabling Capabilities .....	24
6.0 SEQUENCED ACTIONS .....	30
6.1 Introduction.....	30
6.2 Nominal/Steady State Operations .....	30
6.3 Crisis/Conflict.....	31
6.4 Post Conflict: Return to Nominal/Steady State Operations.....	33
7.0 COMMAND RELATIONSHIPS .....	34
7.1 Cyberspace Defense Relationships.....	35
7.2 Cyberspace Force Application Relationships .....	35
7.3 Relationship with AF Component Commands .....	36
7.4 Relationship with Combatant Commands.....	36
7.5 Relationship with Air Force Units.....	36
7.6 Relationship with Air Force Reserve and Guard Units.....	37
8.0 SUMMARY .....	38
Appendix A: References .....	39
Appendix B: Glossary Of Terms, Abbreviations And Acronyms.....	41
Appendix C: Capability Traceability Matrix.....	53

**TABLE OF FIGURES**

Figure 1. Operational Environment ..... 3  
Figure 2. Cyberspace Relationship to Other Domains ..... 4  
Figure 3. Traceability to AF-Level CONOPS..... 6  
Figure 4. Cyberspace to AF Operational Concepts Hierarchy ..... 8  
Figure 5. Cyberspace Operations Operational View (OV-1) ..... 13  
Figure 6. Cyberspace Superiority Missions and Necessary Capabilities ..... 15  
Figure 7. Cyberspace Command Relationships..... 34

## 1.0 PURPOSE

*“Cyberspace is about operations, not communication. It is about operations, not a network. It is about how we do things to fight and win. We must assure our operations on the network.”*

**General C. Robert Kehler, Commander AFSPC**

This functional concept details capabilities and effects necessary to perform operational cyberspace functions desired by the warfighter, from the present through 2030. This concept broadly describes how AFSPC intends to conduct cyberspace operations in support of both joint and AF operations of all types, and provides a foundation for developing more detailed concept documents. Moreover, AFSPC will use this concept, along with emerging joint guidance, to organize, train, and equip forces to conduct cyberspace operations. Finally, this concept provides the operational perspective to underpin the many activities necessary to realize the AF institutional vision for a mature set of cyberspace capabilities<sup>1</sup>:

- Position the AF with enhanced and differentiated capabilities complementing those of other Services
- Assure the mission by securing the AF portion of the Department of Defense (DoD) Global Information Grid (GIG)
- Fuse cyberspace and intelligence, surveillance, reconnaissance (ISR) functions to create seamless operations
- Create unique capabilities through innovation and integration
- Build the next-generation network/cyberspace infrastructure
- Refine operations to create synergies and seamless capabilities
- Field and further develop operationally responsive capabilities
- Achieve cyberspace integration and acculturation

*“There is no exaggerating our dependence on DoD’s information networks for command and control of our forces, the intelligence and logistics upon which they depend, and the weapons technologies we develop and field. In the 21<sup>st</sup> century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace. It is therefore not surprising that DoD’s information networks have become targets for adversaries who seek to blunt US military operations.”*

**DoD 2010 Quadrennial Defense Review (QDR) Report**

---

<sup>1</sup> United States Air Force Blueprint for Cyberspace, 2 Nov 09.

## 2.0 OVERVIEW

*“The belief that Air Force networks can be protected by preventing the enemy from penetrating them is an idea no longer viable.... We now need to talk about operating a network in which the enemy is already [present]. That requires a defense in depth, with the ability to fight through attacks and keep the networks up and running so that they can continue to support the joint force.”*

**Lt Gen William T. Lord, USAF Chief Information Officer**

Advancements in communications and information technology have given birth to a virtual domain. This domain, cyberspace, is one that Americans use and depend upon daily. It is our hardware and our software, desktops, laptops, and wireless communications that have become woven into every aspect of our lives. “America’s prosperity in the 21<sup>st</sup> century will depend on securing cyberspace.”<sup>2</sup>

Cyberspace is persistent, real-time, and global. AF operations in all domains are interconnected and are focused on the needs of joint force commanders (JFCs) and the joint warfighter. Consistent with joint terminology, operating concepts and views on the joint operating environment, the AF views cyberspace as a contested, operational and warfighting domain that pervades and enables capabilities and effects in all other domains.

## 2.1 Background

*“Cyberwar is now a fact of life in 21<sup>st</sup> Century wars. Actual and potential enemies of America already know the dimensions of Cyberwar and have moved into full combat. Cyberspace is a perfect environment for United States adversaries to thrive and a domain that the United States must vigilantly protect.”*

**LTG Keith B. Alexander, Commander  
Joint Functional Component Command for Network Warfare**

Cyberspace is a domain requiring technology to enter, persist, and exploit. A major difference from the other domains (air, land, maritime, and space) is that cyberspace cannot be perceived directly by the senses. Its physics are those that govern the transmission, reception, and use of electromagnetic signals and information. As with other operations, effects of cyberspace operations can occur simultaneously in many places. They can be precise or broad, enduring or transitory, destructive or disruptive.

Cyberspace is defined as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”<sup>3</sup> Cyberspace is a place where operations are conducted and is critical to our current and future military operations. The operational environment reflects the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Understanding this environment requires a holistic

---

<sup>2</sup> President Barack Obama, White House Press Conference, *Securing Our Nation’s Cyber Infrastructure*, 29 May 09.

<sup>3</sup> CJCS CM-0363-08, *Updated Definition of Cyberspace*, 10 Jul 08.

view that extends beyond the adversary's military forces and other combat capabilities within the operational area. Such a view of the operational environment encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment (which includes cyberspace). Included within these environments and factors are adversary and friendly systems and subsystems. Figure 1 shows a conceptual view of the operational environment.<sup>4</sup>

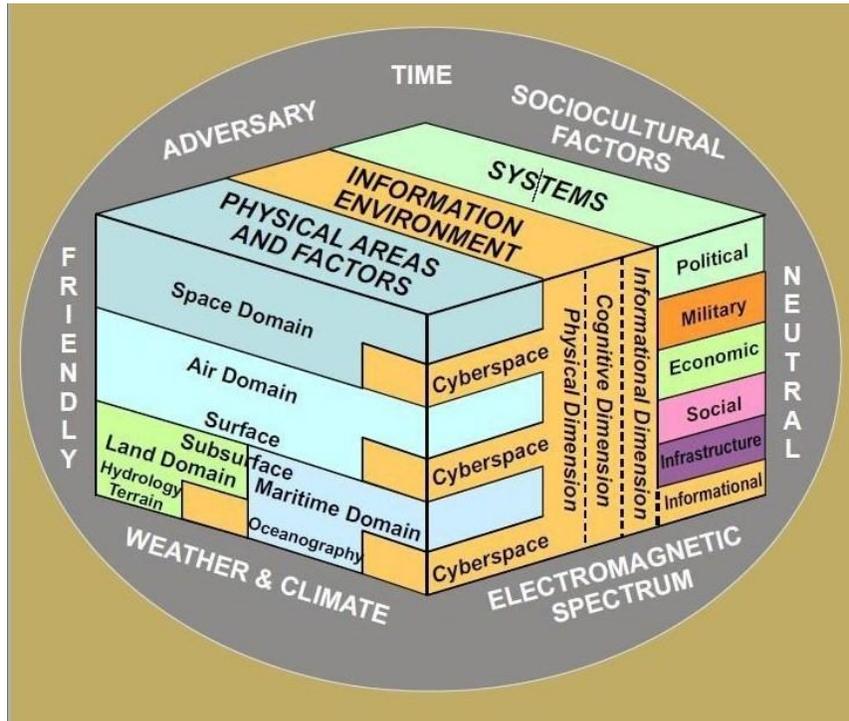


Figure 1. Operational Environment

Cyberspace is an interactively complex domain where many small, diverse, and independently operating systems, many themselves complex, comprise the structure as a whole. Cyberspace is made up of many different network types with varying degrees of functionality, levels of interconnectivity, technical complexity, and inherent vulnerabilities.

Cyberspace is a primary domain for military command, control, communications, and computers (C4), and ISR capabilities. Modern military kill-chain systems, support systems, and base infrastructure systems depend vitally on cyberspace. This dependence is recognized and these systems, like our Nation's critical infrastructures, must be protected from attack to ensure their availability. Accordingly, the United States (US) *National Strategy to Secure Cyberspace* outlines three strategic objectives:

- Prevent cyberspace attacks against America's critical infrastructures
- Reduce national vulnerability to cyberspace attacks

<sup>4</sup> JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, 16 Jun 09.

- Minimize damage and recovery time from cyber attacks that do occur

The AF seeks an expanded, overarching concept of operations that streamlines command and control, integrates cyberspace capabilities, and creates a security framework to facilitate integration and to allow cross-ideation for air, space, land, maritime, and cyberspace domains. Warfighters will determine new ways to leverage capabilities from different domains to create unique, and often “decisive,” effects. In modern warfare, all domains are interconnected via the cyberspace environment (see Figure 2).

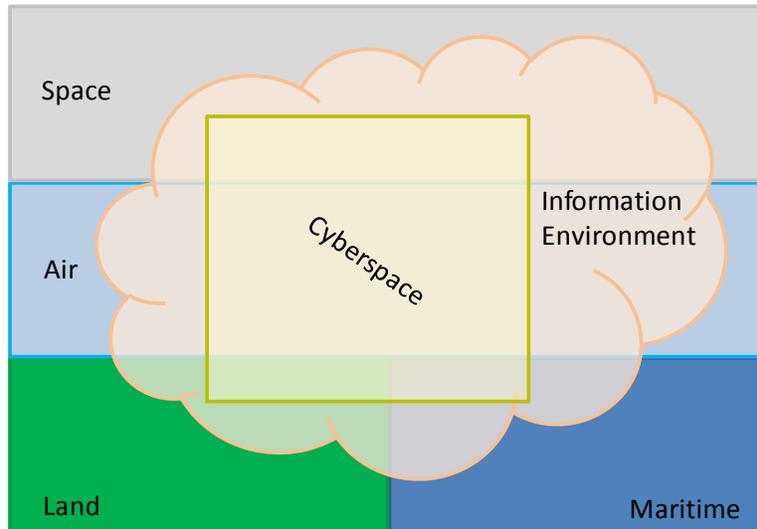


Figure 2. Cyberspace Relationship to Other Domains

### 2.1.1 Department of Defense Goals in Cyberspace

Achieving military superiority in cyberspace is a DoD strategic goal with the following strategic priorities<sup>5</sup>:

- Integrate cyberspace capabilities with other domain capabilities across the full range of military operations
- Gain and maintain initiative to operate within adversary decision cycles
- Build capacity for cyberspace operations
- Manage risk for operations in cyberspace

### 2.1.2 Air Force Intent

Gaining and maintaining cyberspace superiority is essential to the AF’s ability to deliver global power, global reach, and global vigilance. This advantage provides leverage in all other domains to increase AF reach, speed, distance, stealth, precision, and massed effects. The significance of AF operations in cyberspace is readily apparent. Not only is cyberspace vital to today’s fight, it is also crucial to the continued US military advantage over our adversaries in the future. The AF is highly dependent on cyberspace for command and control (C2) of forces,

<sup>5</sup> *The National Military Strategy for Cyberspace Operations (NMS-CO)*, Dec 06.

ISR, the logistics upon which they depend, and the weapons technology the AF develops and deploys. Joint forces cannot conduct effective operations without reliable cyberspace capabilities. Consequently, the AF is intent on providing a full range of cyberspace capabilities to JFCs, whenever and wherever needed, to achieve and sustain both information and cyberspace superiority.

The AF will contribute to the joint fight by organizing, training, and equipping expeditionary-capable cyberspace forces, which will be presented through US Strategic Command (USSTRATCOM) and US Joint Forces Command (USJFCOM) to other Combatant Commands, to conduct full spectrum operations. To this end, the AF will provide cyberspace-enabled capabilities and integrate them with capabilities in other domains to create force-multiplying effects for the joint warfighter.

### 2.1.3 Organization to Achieve Cyberspace Objectives

*“We prevailed in the Cold War through strong leadership, clear policies, solid alliances and close integration of our diplomatic, economic and military efforts. We backed all this up with robust investments—security never comes cheap. It worked, because we had to make it work. Let’s do the same with cybersecurity. The time to start was yesterday.”*

**John M. McConnell, former Director of National Intelligence**

Achieving the AF intent in cyberspace requires a command, control, and coordinating structure that goes beyond traditional boundaries. To maintain unity of effort among AF organizations, the AF consolidates cyberspace resources in AFSPC as the lead major command (MAJCOM) that organizes, trains, and equips AF cyberspace forces for the warfighter. AFSPC organized the 24th Air Force (24 AF) as the component numbered air force (C-NAF) to present AF cyberspace forces to the combatant commander. (See section 7.0 for discussion of cyberspace operations organizational/command relationships.)

Unity of effort, however, also requires close, total-force coordination with the many organizations involved, in the interagency, joint, civil, industry, academia, and international arenas. No single entity “owns” the entire cyberspace domain. The DoD is responsible for securing its own portion of the cyberspace domain, as other federal agencies are responsible for theirs. The AF and other Services may be called upon to provide support to other government and/or nongovernmental organizations (NGOs) as well as private sector and international partners in defending cyberspace.

Operationally, the AF will:

- Gain and maintain cyberspace superiority, while executing military operations at the time and in the “place” of our choosing
- Deny adversaries freedom of action in the friendly cyberspace environment
- Maintain situational awareness (SA) in cyberspace to globally command and control AF forces and, when tasked, joint cyberspace forces

- Assure AF missions with freedom of action in cyberspace, to include freedom to attack, freedom from attack, and the ability to fight through cyberspace attacks

#### 2.1.4 Relationship to Air Force Concepts of Operation (CONOPS)

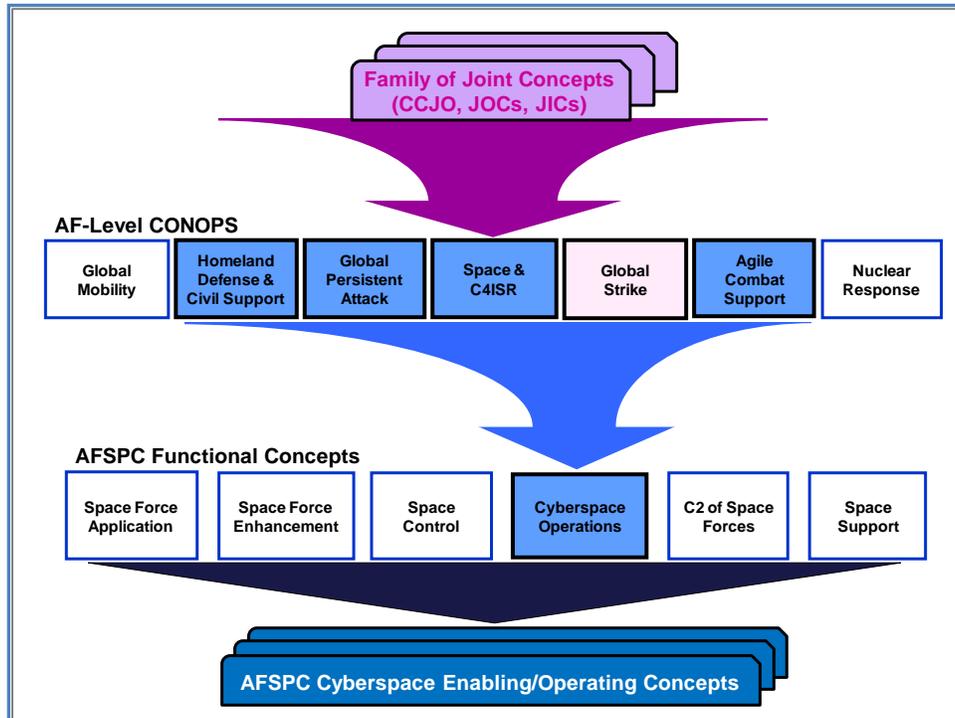


Figure 3. Traceability to AF-Level CONOPS

As shown in Figure 3, the capabilities defined in this functional concept directly trace to capabilities in the following AF CONOPS:

##### 2.1.4.1 Homeland Defense and Civil Support

- Prevent cyber attacks on the homeland by deterring, detecting, predicting, planning for, and preempting threats
- Protect the air, space, and cyber avenues of attack against the Homeland
- Respond to all attacks on the US through the air and space mediums while supporting operations in the cyber, land, and maritime domains

##### 2.1.4.2 Global Persistent Attack

- Freedom to Maneuver: Dominating the air, space, and cyberspace domains to enable joint forces' unhindered conduct of air, space, cyber, land, and maritime operations without interference from the opposing force
- Persistent Engagement: Dominating the enemy through sustained kinetic and non-kinetic means in all domains unconstrained by combat support functions

- Defend friendly operations and freedom to attack adversary electromagnetic operations to achieve dominance in the electromagnetic spectrum

#### **2.1.4.3 Space & Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (S&C4ISR)**

- Kinetic and non-kinetic strike operations will be conducted from/through the air, land, maritime and space mediums, as well as the information environment (i.e., cyberspace)
- Provide for the defense of systems and networks on which friendly information is transported, stored, retrieved, and processed
- Continuously monitor friendly networks; detect, analyze, and discern origin of threats; promptly respond to offensive threats
- Persistently collect data on information systems; this capability will detect changes to complex information networks, effectively characterize targets, improve weaponing, monitor execution, mature measures of effectiveness, and assure information systems to directly enable friendly operations

#### **2.1.4.4 Global Strike**

- Reduce or avoid destruction and collateral damage by applying non-kinetic methods (such as cyberspace attack) to set the conditions for follow-on persistent forces
- Rapid Strike: Quickly neutralize an adversary's key high value targets (HVTs) operating in air, space, and cyberspace domains, at the time of our choosing
- Attacking the enemy in cyberspace can reduce collateral damage and mitigate the impact of enemy strategies to disperse critical systems away from HVT areas, or to re-locate mobile systems

#### **2.1.4.5 Agile Combat Support**

- Communications Infrastructure: Establish communications infrastructure includes actions necessary to provide a communications infrastructure to support a full range of information services; examples of this type of service include secure/non-secure reachback, data, voice, command and control, client support, postal, and air traffic system infrastructures

#### **2.1.5 Relationship to the AF Operating Concepts (AFOpsCs)**

This functional concept describes the AF cyberspace capabilities required to achieve warfighter-needed capabilities and effects as are expected to be defined in the evolving Cyberspace Joint Operating Concept (JOC) and AFOPsCs (see Figure 4). This document will be updated as the AFOPsCs are developed later this year.

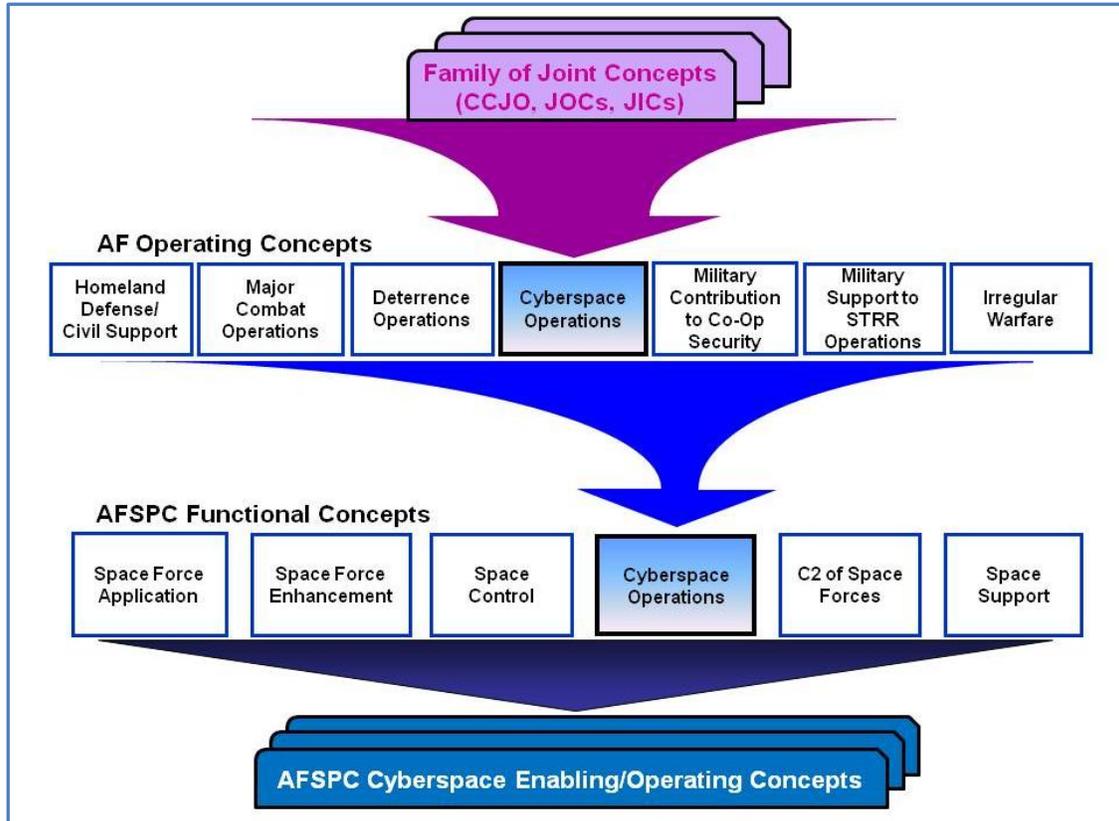


Figure 4. Cyberspace to AF Operating Concepts Hierarchy

## 2.2 Summary

The AF views cyberspace as a contested operational domain that pervades and enables capabilities and effects in all other domains. Cyberspace is persistent, real-time, and global in nature. AF operations in air, space, and cyberspace are interconnected and focused on the JFCs' needs.

Operationally, the AF will:

- Gain and maintain cyberspace superiority while executing military operations at the time and in the “place” of our choosing
- At the time and place of our choosing, deny adversaries freedom of action to affect friendly force operations in the cyberspace environment
- Maintain SA in cyberspace to globally command and control AF forces and, when tasked, joint cyberspace forces
- Assure AF missions with freedom of action in cyberspace, to include freedom to attack, freedom from attack, and the ability to fight through cyberspace attacks

Protecting AF cyberspace and using cyberspace for AF activities both represent significant challenges. Consolidating critical AF cyberspace resources into AFSPC allows the command to lead the AF into a new era of cyberspace operations that are coordinated with other Services, federal, state, local, NGO, private sector, and international partners.

## **3.0 SITUATION**

### **3.1 Time Horizon**

The time horizon of this functional concept is the present through 2030. This concept supports planning processes that allow AFSPC and other AF MAJCOMs to translate capability decisions into organize, train, and equip activities.

### **3.2 Military Challenges**

#### **3.2.1 Threats to Cyberspace Operations**

Cyberspace exploitation and attack have grown more sophisticated and more serious. Our information technology infrastructure—including the Internet, telecommunications networks, wireless communications, computer systems, and embedded processors and controllers—is targeted for exploitation, and potentially for disruption or destruction, by a growing array of state and non-state adversaries. Adversaries can be structured or unstructured, well-organized and well-funded with long-term objectives; or smaller, less organized groups with limited support and motives. Structured threats include activities by state-sponsored, criminal-sponsored, or hostile or radically-oriented groups with generally long-term objectives. Unstructured threats are generally those threats that originate from individuals or small groups with a limited support structure and limited motives. In either case, adversaries may capitalize on low-entry costs, widely available civilian and commercial resources, and minimal technological investment to potentially inflict serious harm. The expanded availability of commercial off-the-shelf (COTS) technology provides adversaries with increasingly flexible and affordable technology to adapt for hostile purposes. These low barriers to entry make cyberspace targets and the cyberspace domain attractive to adversaries. A related threat is the “insider” who has some level of authorized access to information and information infrastructure within an organization.

The risk of a cyberspace loss or failure must be considered when planning and executing AF operations, to include mitigation actions and/or alternatives.

#### **3.2.2 Mission Essential Functions (MEFs)**

The vast number of cyber-related assets to which numerous ongoing missions depend makes it difficult to know the impact when one of those assets is rendered inoperable (intentionally or unintentionally). MEFs must be accomplished to achieve mission objectives. This entails prioritizing mission essential activities, mapping mission dependence on cyberspace systems/assets, identifying vulnerabilities, mitigating risk of known vulnerabilities, identifying threats and adversary intent, and neutralizing the adversaries’ ability to attack/exploit friendly force vulnerabilities.

MEFs are the specified or implied tasks required to be performed by, or derived from, statute, executive order, or other appropriate guidance, and those organizational activities that must be performed under all circumstances to

achieve DoD component missions. Failure to perform or sustain these functions would significantly affect the DoD's ability to provide vital services or exercise authority, direction, and control.

### **3.2.3 Compressed Decision Cycle of Cyberspace Operations**

The fact that operations can take place nearly instantaneously requires the formulation of predetermined or automated responses to potential cyberspace attacks. The compressed decision cycle follows rules (predetermined responses) for actions that enable counterattacks against time-sensitive and fleeting targets, as allowed. This compressed decision cycle places a premium on battlespace awareness (BA). A key element of BA, particularly with regard to cyberspace operations, is intelligence preparation of the operational environment (IPOE). IPOE provides a foundational and predictive analytic understanding of the battlespace, its environment, adversary capabilities, and intent. However, to truly be effective in aiding decision making, BA must also rely on the other pillars of predictive battlespace awareness or PBA (target development, ISR strategy & planning, ISR execution, and assessment), as well as cyberspace indications and warning (I&W) and threat attribution and characterization. Through constant integration of these cyber ISR processes, friendly forces can rapidly identify potential adversary threats/courses of action (COAs) and develop plans to counter or exploit those COAs.

### **3.2.4 Anonymity and the Inherent Attribution**

The nature of cyberspace, government policies, and international laws/treaties make it very difficult to determine the origin of cyberspace attacks and network intrusions. The ability to hide the true (originating) source of an attack makes it difficult to identify the attacker. Furthermore, the design of the Internet lends itself to anonymity. Anonymity results from:

- The large number of cyberspace users/actors
- The massive volume of information flowing through the networks
- Features that allow users to cloak their identity and activities

There is little the US can do about anonymity; however, the same features utilized by terrorists, hackers, and criminals (anonymity and the ability to hide) can also strengthen US surveillance and law enforcement efforts.

Attribution is a significant challenge because of the dynamic and pervasive nature of cyberspace, where flexibilities are often achieved by embedded, distributed dependencies that change frequently, and can be difficult to identify.

### **3.2.5 Legal Considerations**

DoD must conduct cyberspace operations within applicable US laws and international agreements, and in accordance with relevant Government and DoD policies. The legal framework applicable to cyberspace operations depends on the nature of the activities to be conducted, such as offensive or defensive military operations, defense support to civil authorities, service provider actions,

law enforcement and counterintelligence activities, intelligence operations, and defense of the homeland. The actions of cyber warfare<sup>6</sup> and exploitation may have different legal and approval requirements/authorities. Before conducting cyberspace operations, commanders, planners, and operators must understand the relevant legal framework in order to comply with laws and policies. As in all other military operations, US Armed Forces conducting cyberspace operations must comply with the law of armed conflict (LOAC).

Cyberspace forces may at one moment be operating under Title 10, US Code, *Armed Forces*, at another moment under Title 50, US Code, *War and National Defense*, and even in some instances under Title 18, US Code, *Crimes and Criminal Procedure*. In addition, some cyberspace forces may operate under Title 32, US Code, *National Guard*. The rules for operating under different Titles of US Code are very different, and the authority to transition from one to another may be held at a very high level (even that of the President of the United States).

### 3.3 Assumptions

The following assumptions guide the formulation of this functional concept:

- Resources are in place and the AF is committed to increasing and improving cyberspace mission capabilities. Ineffective cyberspace mission capabilities will significantly reduce the AF's ability to understand, shape, and command the cyberspace domain for the joint warfighter
- Both traditional and irregular forms of warfare will require cyberspace defensive, exploitative, and offensive elements
- Timely and responsive requirements, acquisition, certification, integration, and testing processes are in place to field cyberspace capabilities
- Adversaries will continue to have access to the cyberspace domain as technology proliferates
- Cyberspace forces and resources will have the ability to operate continuously (i.e., 24/7/365), providing persistent global and theater effects throughout the spectrum of conflict
- Military operations will continue to depend upon civil, allied, and commercial cyberspace systems and infrastructure
- Sufficient and responsive all-source cyberspace capabilities, ISR systems, infrastructure, and personnel are in place and consistently available to planners, operators, and decision makers
- Policy and legal authorities are in place to enable effective cyberspace operations
- The AF and other Services will organize, train, and equip cyberspace forces, and develop and sustain cyberspace systems, in a de-conflicted and complementary manner

---

<sup>6</sup> See Appendix B for definition and Joint Test Publication 3-12, *Cyberspace Operations (Draft)*, for in-depth discussion.

### 3.4 Risks

- An incomplete understanding of friendly and adversarial cyberspace resource uses, capabilities and intent, and their interdependencies, could impact our ability to protect/defend our cyberspace capabilities/assets as well as to counter/affect an adversary's cyberspace capabilities at the time and place of our choosing
- Failure to plan and employ cyberspace capabilities as an effective means to shape the adversary's perception, confidence, and tactics, techniques and procedures (TTPs) could result in loss of operational advantages across the range of military operations
- Failure to accurately anticipate and understand technology advances and new capabilities could give an advantage to adversaries, and hinder our ability to adequately react and respond to threats

## 4.0 SYNOPSIS

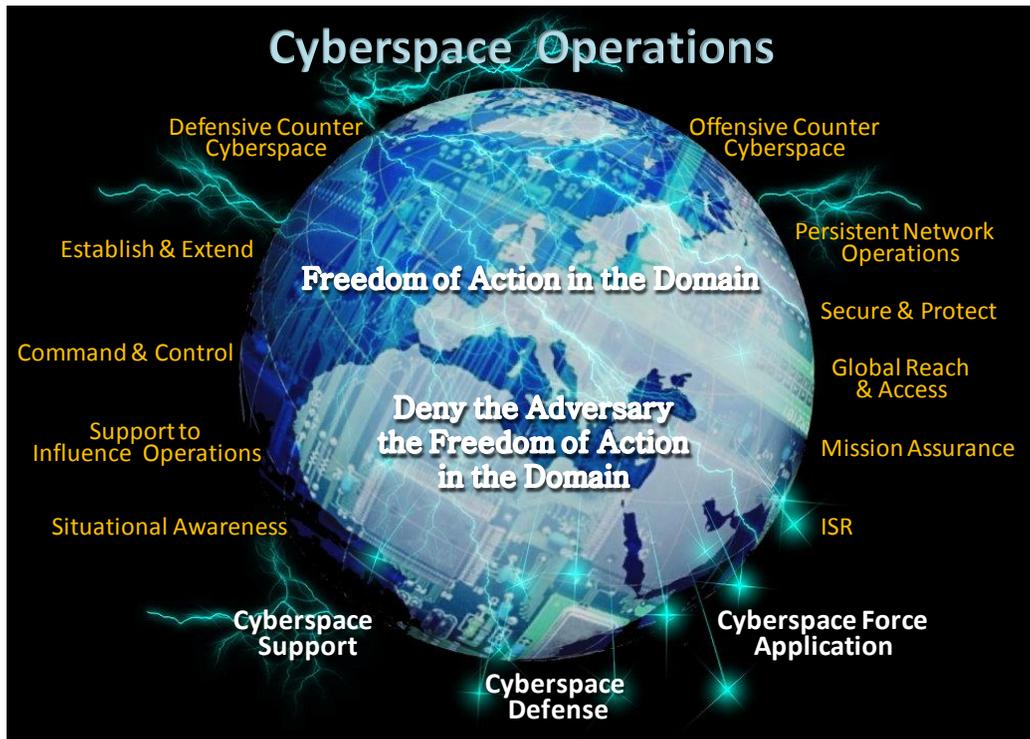


Figure 5. Cyberspace Operations Operational View (OV-1)

### 4.1 Desired Effects

To meet the needs of the JFC, AFSPC must ensure combat-ready forces are organized, trained, and equipped to conduct sustained operations in, through, and from the cyberspace domain, and fully integrate these with land, maritime, air, and space operations. As shown in Figure 5, AFSPC will provide the JFC capabilities to affect and control the cyberspace domain, execute decision making, accelerate operations, provide battle-changing opportunities, and deny those capabilities to our adversaries, as required. The following effects must be realized to meet the needs of the warfighter.

#### 4.1.1 Information Superiority

Information superiority provides decision makers real-time, persistent, pervasive and global SA across the network-centric environment. Information superiority is dependent on integrated C2 architectures, communications networks, integrated ISR capabilities, and cyberspace domain technical expertise. The physical and virtual components of these assets must be merged into a seamless network architecture that provides real-time SA to facilitate the incorporation of defensive and offensive cyberspace actions into coordinated warfighting operations. AFSPC will advocate merging C2 and ISR capabilities and systems to build a truly network-centric operational capability reliant on an integrated C2 architecture that connects sensors and platforms to commanders and warfighters.

#### 4.1.2 Cyberspace Superiority

*“Cyberspace Superiority is the operational advantage in, through, and from cyberspace over adversaries to defend, exploit and conduct offensive operations at a given time and place, without effective interference.”*

**Joint Test Publication 3-12, Cyberspace Operations**

To achieve cyberspace superiority, we must ensure freedom of action in the domain for the joint warfighter, while denying the same advantage to the adversary, at the time and place of our choosing. Freedom of action is achieved by creating and sustaining the access and control of cyberspace infrastructure required for joint operations. This access permits both the movement of data/information, as well as the execution of cyberspace operations by friendly forces. Access may be gained via maneuver, or it may be developed by identifying, acquiring, and sustaining key elements within the domain.

As adversaries become more dependent on the cyberspace domain, our cyberspace operations will be able to deny their ability to organize, coordinate, and conduct effective military operations. These operations may deny, degrade, disrupt, deceive, and/or destroy an adversary's ability to use the cyberspace domain for his military/warfighting operations. Cyberspace operations may produce physical, lethal, non-lethal, and/or virtual impacts on operations in all other domains. Denying adversary freedom of action in cyberspace requires the ability to identify the key resources they use to gain operational advantage. It is also important to understand that the joint warfighter and adversary may share similar cyberspace infrastructure operated by allied/coalition nations, US Government, private entities, and/or non-combatants. The potential operational impact to attain one outcome may affect other activities.

Achieving cyberspace superiority leads to the following operational advantages:

- The warfighter gains military advantage by executing operations in, through and from cyberspace
- Adversaries are unable to gain and maintain operational advantage derived from their use of cyberspace
- The warfighter has freedom of action to operate in cyberspace without compromising US access to cyberspace
- Cyberspace operations are planned, integrated and closely synchronized with other domain operations to meet warfighter needs and attain the desired outcome(s)

4.2 Missions

*“Cyberspace pervades every other domain and transcends traditional boundaries. Without question, cyberspace is vital to today’s fight and to the future US military advantage over our adversaries. It is the intent of the United States Air Force to provide a full spectrum of cyberspace capabilities to Joint Force Commanders whenever and wherever needed.”*

**SECAF/CSAF Letter to Airmen – Air Force Cyberspace Mission Alignment**

Cyberspace operations are more effective when component capabilities are mutually supporting. Some capabilities offer the warfighter an opportunity to gain and maintain the initiative; other capabilities must be actively layered to ensure freedom of action throughout the range of military operations. Figure 6 shows the established cyberspace missions and necessary capabilities.<sup>7</sup> Section 5.1 of this concept further defines/describes those necessary capabilities.

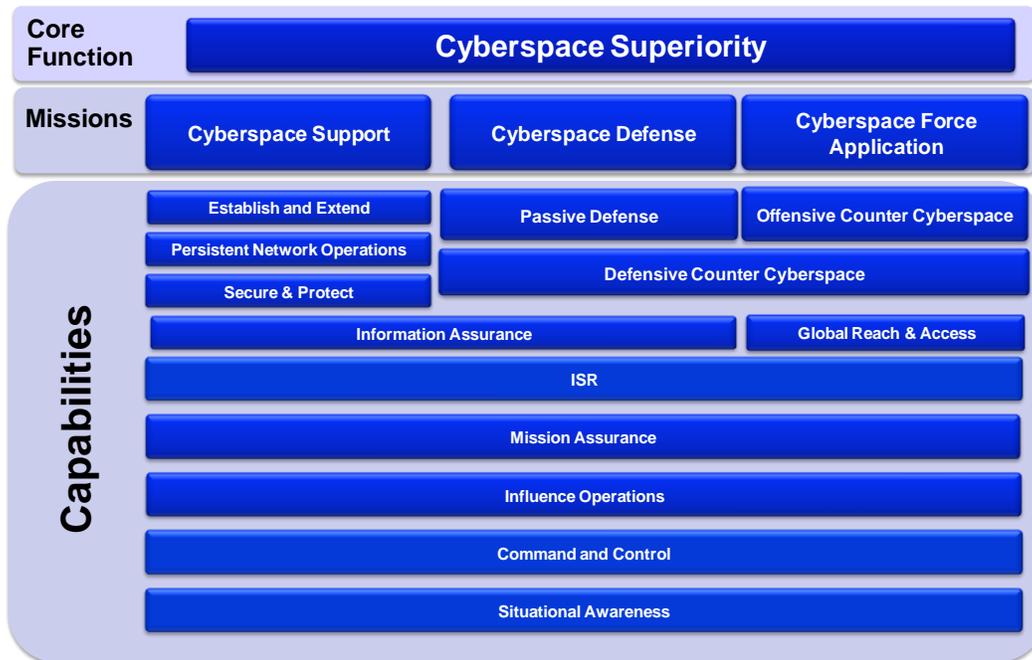


Figure 6. Cyberspace Superiority Missions and Necessary Capabilities

<sup>7</sup> AFSPC/CC approved Cyberspace Superiority Hierarchy, 25 Mar 10.

### 4.2.1 Cyberspace Support

*“... our efforts to protect ... interests in [space and] cyberspace must be as ambitious as our reliance on these domains. We must be able to deter and defend against attacks on our space and cyber capabilities, and fight through any degradation, disruption, or even denial of these vital capabilities.”*

**General Norton A. Schwartz, USAF Chief of Staff**

The cyberspace support mission establishes and secures a defensible network. Cyberspace support refers to foundational, continuous, and/or responsive operations to ensure information integrity, confidentiality, authentication, and mission assurance to achieve freedom of information transport in, through, or from AF controlled infrastructure and its interconnected portions of the cyberspace domain. This is a force-multiplying mission to improve the effectiveness and efficiency of AF operations and joint military forces. Inherent within this mission is the ability to establish, extend, secure/protect, and sustain assigned networks. It includes *cyber defense* and *cyber enabling* activities. It also incorporates all elements of AF network (AFNet) management, information transport, storage, retrieval and processing. The primary capabilities under cyberspace support are "establish and extend", "persistent network operations", and "secure and protect" (discussed in section 5.1.1). Cross-cutting cyberspace capabilities supporting this mission are ISR, SA, C2, information assurance (IA), mission assurance (MA) and influence operations.

### 4.2.2 Cyberspace Defense

The cyberspace defense mission uses passive, active and dynamic capabilities to protect from and respond to imminent or on-going adversary actions against the AF's portion of the GIG (i.e., AFNet), including expeditionary networks. This mission provides expanded active and passive defense operations, and prepared defensive measures that can neutralize or limit an adversary's ability to degrade or exploit friendly cyberspace systems. An effective cyberspace defense will preserve, protect, recover, and reconstitute friendly cyberspace capabilities before, during, and after an adversary attack. Actions include responsive identification and association/attribution of hostile activity; cyberspace defenses are expected to react with preapproved actions, employed within seconds-to-minutes of indications or adversary action. This mission contains aspects of *cyber enabling* and *cyber attack*, as well as aspects of influence operations. The primary capabilities under cyberspace defense are passive defense and defensive counter cyberspace. The cross-cutting cyberspace capabilities extensively support this mission as well.

### 4.2.3 Cyberspace Force Application

Cyberspace force application entails combat operations in, through, and from cyberspace to achieve military objectives, and influence the course and outcome of conflict by taking decisive actions against approved cyberspace or other data/information infrastructure targets. Potential targets and vulnerabilities must be identified, and plans developed, exercised, and tested to ensure freedom of

action. Cyberspace force application will be used cautiously and employed precisely to affect resources. This mission will be employed only when approved by US leadership in an authorized supporting or supported role through a signed execution order.

Similar to other combat operations, cyberspace combat assessment and/or battle damage assessment must be employed to determine success and/or re-plan of cyberspace force application efforts. Examples of specific cyberspace force application activities include infiltration, maneuver, interdiction, and counterattack. The primary capabilities under cyberspace defense are offensive counter cyberspace, defensive counter cyberspace and global reach and access with cross-cutting cyberspace capabilities also supporting this mission.

## 5.0 NECESSARY AND ENABLING CAPABILITIES

*“The United States must ... translate our intent into capabilities. We need to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with an evidentiary trail that can support diplomatic, military and legal options—and we must be able to do this in the milliseconds of network speeds.”*

**John M. McConnell, former Director of National Intelligence**

### 5.1 Necessary Capabilities

This section details the necessary capabilities for cyberspace operations required to support joint warfighting needs across the full range of military operations. Appendix C provides a crosswalk between this concept’s capabilities and the joint warfighter capabilities as defined in the six JOCs. The following necessary capabilities create the desired effects described earlier in this document.

#### 5.1.1 Cyberspace Support Capabilities

##### 5.1.1.1 Establish and Extend

The AF will employ capabilities to engineer and establish links, nodes, and tactical communications system infrastructure within the cyberspace domain to provide a network-centric operating environment with advanced capabilities for AF, joint, and allied/coalition operations. The AF will engage other Services, federal, state, local, NGO, private sector, academia, and international partners to leverage innovative and adaptive technology solutions and techniques to modernize the network-centric operating environment.

Additionally, the AF will provide capabilities that protect/secure, transport, store, retrieve, and process information. These services will be provided through a combination of terrestrial, airborne and space-based assets and will support both garrison and expeditionary forces. These capabilities will connect and interoperate, as required, across all cyberspace forces, DoD users, and mission partners to allow users to share actionable information, provide access to systems and information, and provide connectivity. The ability to extend or expand fixed and mobile platforms networks services should include, but not be limited to: texting; imagery such as digitized photos; forms/publications; email; messaging; webpages; chat sessions; audio files; or voice services, such as radio, phone, interphone, satellite, voice-over IP, or public address systems, and video services, such as streaming video, video conferencing, live transmissions, or recorded video. The AF will provide and expand, as necessary, its data and tactical communication services for AF, joint, and allied/coalition operations. The capability to *establish and extend* includes frequency sharing and managing access to, and use of, the electromagnetic spectrum.

### **5.1.1.2 Persistent Network Operations**

The AF will provide continuous network operation capabilities for worldwide AF garrison and deployed networks to ensure necessary support for military operations. The AF will continuously monitor networks in order to provide secure and protected network operations in response to threats and persist with capabilities ensuring military operations are uninterrupted in a contested cyberspace environment. Constant evaluation and modernization of network operations to enable AF cyberspace security and protective measures are required to adequately meet and defeat constantly evolving cyberspace technologies.

### **5.1.1.3 Secure and Protect**

Secure and protect capabilities (i.e., active and passive measures/activities) continuously monitor, analyze, and protect the AF cyberspace architecture, data, and processes. These capabilities include identification and restoration of information and information systems affected by hostile activity. Actions allow operators to protect the friendly use of cyberspace, as well as detect, determine the source of the attacks, and respond to hostile actions as they occur. These actions include IA (measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation), and restoration of information systems by incorporating protection, detection, and restoral capabilities. The development, implementation, and sustainment of protective measures ensure a state of inviolability from hostile acts or influences.

Secure and protect cyberspace capabilities include tenets similar to those within the AF Wingman Program, where every Airman is committed to cultivating a culture that protects and preserves friendly use of the domain while remaining vigilant to deny adversaries access to, and use of, cyberspace to achieve hostile purposes.<sup>8</sup>

## **5.1.2 Cyberspace Defense Capabilities**

### **5.1.2.1 Passive Defense**

Passive defense capabilities provide continuously protective measures used to reduce probability of and minimize effects by adversaries' actions to ensure an operationally defensive posture for garrison and expeditionary AF networks. It includes capabilities to detect events through intrusion detection systems from AF boundaries to individual components. These capabilities are employed to configure and operate network boundary protection, status, vulnerability scanning, assessment, and techniques for detecting intentional or unintentional intrusion, abuse, or denial of service within systems or networks. The development, implementation, and sustainment of passive defensive measures help defend critical cyberspace resources and ensure freedom of action.

---

<sup>8</sup> Adapted from guiding principles in the "Rise of the Cyber Wingman" philosophy.

### 5.1.2.2 Defensive Counter Cyberspace (DCC)

Defensive counter cyberspace capabilities enable the AF to plan, execute, and monitor responsive activities against imminent or on-going hostile activity to assure AF and joint operations. DCC capabilities provide a full range of active and dynamic defensive measures taken to detect, identify, acquire information, track, and defend AF operations against adversaries' actions or operations to penetrate, dissuade, degrade, disrupt, or corrupt friendly cyberspace freedom of action and operation. This includes integrated dynamic operational planning, coordination, and synchronization of cyberspace defensive and intelligence capabilities against imminent or on-going adversary activities. Responses include measured actions ranging from tailored messages to weapons employment within authorized parameters and protective measures within AF's safeguarding responsibilities, self defense activities guided by approved rules of engagements (ROEs), approved influence operations, and preparatory activities that enable transition to cyberspace offensive operations as directed by the appropriate authorities. In sustained cyberspace defensive operations, DCC capabilities are undertaken to restore pre-attack conditions, and are directed at limited objectives. These capabilities are highly dependent on fused all-source ISR, integrated I&W, accurate threat characterization and attribution, SA, and responsive C2.

Note: DCC capabilities also apply to the Cyberspace Force Application mission.

### 5.1.3 Cyberspace Force Application Capabilities

#### 5.1.3.1 Offensive Counter Cyberspace (OCC)

Offensive counter cyberspace operations are conducted to deny an adversary attaining his purpose in attacking. OCC capabilities disrupt, deny, degrade, divert, neutralize, destroy, or manipulate (i.e., corrupt or usurp) to prevent an adversary's use of cyberspace or other information infrastructure to conduct activities or maintain freedom of action.<sup>9</sup> This can be a large scale offensive undertaken by a defending force to seize the initiative from the attacking adversary, or it could be a small scale (e.g., single action) to dissuade/deter an adversary from further aggression.

OCC capabilities allow us to support and execute missions across all domains, providing reach and speed, distance, stealth, massed effects, and precision, irrespective of natural and manmade boundaries. The AF will control elements of cyberspace against the adversary using kinetic and non-kinetic, lethal and non-lethal, global and theater effects. Potential targets for offensive counter cyberspace actions could include, but are not limited to:

- Military bases and/or military storage sites
- C2 facilities and resources
- Telecommunications/computer network nodes, links, and systems

---

<sup>9</sup> Adapted from JP 1-02 and JP 3-0.

- Strategic and tactical integrated air defense systems
- Air/naval forces and support infrastructure (e.g., airfields, ports, etc.)
- Energy production/storage facilities and distribution resources
- Supervisory control and data acquisition (SCADA) systems

### **5.1.3.2 Global Reach and Access**

AF capabilities will reach globally to achieve access in support of joint operations in more than one geographic area. Global reach also allows the AF the opportunity to act globally to achieve regional/theater effects as required. Assured access enables timely positioning of AF cyberspace forces operating in rapidly changing and complex environments, and in distributed, simultaneous or sequential operations, often with other agencies and nations. Denial of global reach and access can limit the AF's ability to project forces against irregular, catastrophic, disruptive, or conventional threats.

### **5.1.4 Cross-Cutting Capabilities**

Cross-cutting capabilities are foundational to all cyberspace operations and applicable to more than one cyberspace mission area.

#### **5.1.4.1 Intelligence, Surveillance, and Reconnaissance (ISR)**

The capabilities of ISR are usually thought of as a whole, but each has a distinctive purpose. "Intelligence is the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; it is the information and knowledge about a topic obtained through observation, investigation, analysis, or understanding."<sup>10</sup> Surveillance and reconnaissance are methods of collection, the products of which are turned into intelligence through exploitation and analysis. Surveillance is the sustained systematic observation of areas, places, persons, or things to gather information by a collector, or series of collectors, having timely response and persistent observation capabilities, a long dwell time and clear continuous collection capability. Reconnaissance, on the other hand, is transitory in nature and generally collects information for a specified time by a collector that does not dwell over the target or in the area. Reconnaissance is undertaken to obtain information about the activities and resources of an adversary or about an operational environment.<sup>11</sup>

ISR operations are a combination of the three capabilities aimed at determining adversary capabilities/intent, and the application of the resulting intelligence, are critical to attaining superiority across all three cyberspace mission areas. ISR operations are conducted in all domains to provide integrated, accurate, relevant, timely, and understandable intelligence to decision makers through the effective employment of ISR capabilities, capitalizing on the interoperability among all ISR systems, including intelligence community (IC) and non-traditional sources. ISR

---

<sup>10</sup> JP 2-0, *Joint Intelligence*, 22 June 2007.

<sup>11</sup> Adapted from AFDD 2-9, *Intelligence, Surveillance and Reconnaissance Operations*, 17 July 2007.

operations significantly contribute to decision making by providing commanders and other decision makers the intelligence and SA necessary to successfully plan and conduct operations.

All ISR capabilities are dependent upon sensors and assets that collect data and information, and the people, systems and processes that refine and apply intelligence from those sources. The ISR operations process relies on the ability to:<sup>12</sup>

- Plan and direct collection: determine what to collect and how to collect
- Collect: task appropriate assets (e.g., collection management)
- Process and exploit: transform raw data into usable information
- Analyze and produce: analyze, integrate, evaluate, interpret the information and produce in actionable format
- Disseminate: pass the information to the user in a timely, understandable manner

Cyberspace ISR services and products are provided as: I&W; current intelligence; PBA; and threat attribution and characterization. Combined, the conduct and integration of ISR PCPAD operations increases predictive SA, enables cross-domain unity of effort and reduces uncertainties in cyberspace planning and C2 decision making processes.

The integration of cyberspace ISR PCPAD operations requires development of both non-materiel (e.g., training, TTPs, etc.) and materiel (e.g., hardware, software, infrastructure) capabilities. For example, cross-domain integrated and net-centric ISR capabilities enable information derived from a wide variety of sources to be available to trained networked warfighters (e.g., sensor-to-shooter). This SA and subsequent analysis contributes to a high-fidelity, fused common operating picture/user defined operational picture (COP/UDOP) to facilitate situational comprehension for decision makers and warfighters.

Finally, advancement of cyberspace missions/operations requires rapid and adaptable ISR capability/supportability across the general military and science & technical (S&T) ISR doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) spectrum to shape cyberspace ISR forces, tools and TTP development (e.g., Cyberspace Tactics Analysis and Reporting Program; National Technical Integration, etc.).

#### **5.1.4.2 Situational Awareness**

SA capabilities provide the competitive advantage to commanders and their forces to allow them to make better-informed decisions, and to implement them faster than adversaries can react. SA provides information needed to understand patterns of behavior, constraints, and opportunities of geography, topography, culture, environment, and forces that allow us to predict, pre-empt,

---

<sup>12</sup> PCPAD (planning & direction, collection, processing & exploitation, analysis & production, and dissemination) based on the ISR process from the Global Integrated ISR Core Function Master Plan (Draft).

and/or misdirect or redirect our adversaries' threat activity. SA can provide a more accurate visualization of the operational environment, and facilitate situational comprehension and a compressed decision making cycle thereby aiding the decision making process. With SA information, analysis and judgment is applied to determine the relationships of the factors present, and to form conclusions concerning threats to mission accomplishment, opportunities for mission accomplishment, and gaps in information. SA allows leaders to avoid surprise, make rapid decisions, and choose when and where to conduct engagements to achieve decisive outcomes. Understanding the threat situation, indicators, and probable intent helps decision makers determine proper COAs to address a threat.

#### **5.1.4.3 Command and Control**

AF cyberspace C2 operations capabilities must be centralized and directly responsive to the JFC. The structure and organization must be integrated to provide robust AF information security and mission assurance, as well as surge to meet global and/or critical tactical situations. AF-resourced operations centers will plan, direct, coordinate, and control AF cyberspace forces and operations in support of the JFC. Cyberspace operations centers will integrate a real-time intelligence reporting capability to provide rapid, responsive, adaptive, and successful C2.

Operations centers will unify cyberspace forces, expand SA, and support operations across other warfighting domains. The AF will engage to provide commanders and warfighters the ability to sense, understand, decide, and act faster than an adversary.

#### **5.1.4.4 Mission Assurance**

Mission assurance capabilities ensure AF resources are available, and are secured to support specific missions, force employment, and intelligence operations. Proactive actions ensure the network remains available, ready and positioned to support mission requirements. Capabilities can be deployed (physically or virtually) to actively secure the network and engage any threat found on the network. Mission assurance requires ISR capabilities to focus on specific adversaries and threats that could endanger AF networks, and requires mapping the critical elements of a mission to the network architecture supporting that mission. Focusing on the portion of the network mapped to a specific mission may require accepting risk in other portions of the network.

Supporting mission assurance is the process of mission mapping, which identifies, links, and documents cyberspace operational interdependencies within the AFNet, the GIG, and Defense Industrial Base (DIB), analyzes their risk and exposure to adversary operations, and develops defensive operations to improve protection, increase survivability, and reduce risk. Understanding DIB linkages helps assess risk to AF operations. The AF will work with other Services, federal, state, local, NGO, private sector, academia and international partners to assess information architectures supporting military and civilian critical

infrastructures, and characterize and catalog interdependencies among infrastructure sectors.

#### **5.1.4.5 Influence Operations**

Influence operations capabilities (i.e., psychological operations [PSYOP], military deception [MILDEC], and operations security [OPSEC]) allow commanders to prepare and shape the operational battlespace by conveying selected information and indicators to target audiences, shaping the perceptions of decision-makers, securing critical friendly information, defending/protecting against sabotage and espionage, gathering intelligence, and communicating selected information about military activities to the global audience. The use of these influence operations capabilities in support of cyberspace operations can result in differing behavior or a change in the adversary's decision cycle, shaping the adversary cyber actions to align with the commander's objectives. For example, influence operations could be used to manipulate a system administrator to shut down unnecessarily a server thus forcing the adversary onto a network/server we can exploit, or to compel an adversary to move operations onto a communications system with known vulnerabilities by making the adversary think their primary communication is compromised

In addition, cyberspace capabilities complement, enable and support influence operations through global access to affect the perceptions and behaviors of intended audiences. The proliferation of cyberspace infrastructure (e.g., email, web pages, and social networking sites) can provide greater access for individuals/organizations to shape perceptions.

### **5.2 Enabling Capabilities**

This section describes those inherent capabilities that are essential to successfully execute cyberspace operations and attain the defined desired effects.

#### **5.2.1 Cross-Domain Planning and Development**

Developing and combining AF capabilities from two or more domains creates a force multiplier effect that can bring more capacity for JFCs. These capabilities create unique effects, and enable or enhance cyberspace operations by providing capabilities not possible in one domain alone.

#### **5.2.2 Adaptive TTP Development and Application**

The AF will establish and resource a group of responsive experts from the intelligence, technology, and acquisition communities to adapt AF TTPs and cyberspace capabilities in response to changing adversary attack techniques, tools, and methodologies. This group will be comprised of members in similar communities of interest, with a goal of adapting AF concepts in hours-to-days vice months-to-years.

### 5.2.3 Research and Development Processes

The AF must strengthen existing and create new patterns of interaction with the cyberspace research and innovation communities, and anticipate and articulate needs for the science and technology community. The AF will seek to create a flexible research and development process that is responsive to the needs of the cyberspace operator. This process will rapidly produce technologies and systems, and transfer them to operational forces to meet warfighter requirements, while also mitigating existing and future vulnerabilities with a forward-looking approach. This helps ensure AF capabilities maintain their edge over potential adversaries. Rapid technology advancements inherent in this domain require the AF to continually strive to pioneer the future by developing new partnerships with academia and industry. The AF needs to rapidly exploit technical advances by establishing a continuous process for working with the science, industry and academic communities that form the leading-edge information technology sector to shape our activities in the cyberspace domain.<sup>13</sup>

### 5.2.4 Responsive Cyberspace Capability Development Processes

Advanced cyberspace technological development will support future warfighting needs and defeat emerging threats. The cyberspace domain requires continuous investment in upgrades to existing systems through recapitalization, modernization, and modification. The AF will develop, test, and field new systems that deliver enhanced offensive and defensive capabilities, information superiority tools, and network-centric communications infrastructure. The AF must champion collaboration across federal, state, local, NGO, private sector, academia, and international partners to optimize the development of technologies essential for the emergence of critical future capabilities. Technological compatibility with other systems and platforms must be ensured as new technologies are developed, tested, and applied.

The AF will codify, resource, and establish responsive cyberspace capability development processes to produce effective results in hours-to-days-to-weeks. Rapid development will evolve as best practices are identified, and in some cases establish cyberspace acquisition techniques, organizations, processes, procedures, funding, certification, and approvals. These constantly improving processes will enable the rapid advancement of cyberspace tool/capability development. Personnel involved in rapid development will work from strategy to conception, through development decisions, to prototype and fielding. By leveraging existing DoD organizations, commercial and governmental entities, best practices, operational and tactical lessons learned, and standard and innovative techniques, the AF will maintain the advantage in supporting, defensive, and offensive cyberspace operations. The AF will develop requirement thresholds to determine whether the need is real-time (now), rapid (short-term), or foundational (long-term). An agile and adaptive requirements process will ensure the AF optimizes limited resources while responding to future

---

<sup>13</sup> Adapted from *The United States Air Force Blueprint for Cyberspace*, 2 Nov 09.

operational demands. Additionally, tools, TTPs, and lessons learned from fielding rapid development capabilities should be transitioned to longer term foundational capabilities.

### **5.2.5 Partnerships**

Cyberspace transcends all other domains and national boundaries, and has changed the way military forces interact globally. Currently, private industry operates over 90% of the cyberspace infrastructure while the AF operates only a small percentage, which could potentially affect DoD mission success. Because of the shared risk and the desire to reduce vulnerabilities, the AF will establish new relationships and actively strengthen and expand its existing partnerships with other Services, federal, state, local, NGO, private sector, academia and international organizations/agencies. This necessitates the AF fostering relationships to enable and support the execution of the mission while fulfilling national objectives.

The AF maintains many unique capabilities that can be used to mitigate and manage the consequences of both natural and man-made events, and must be prepared to provide support to federal, state, and local government agencies/authorities. The AF must plan for and be able to defend the Homeland and provide support to civil authorities simultaneously, as directed. By so doing, the AF helps preserve the nation's freedom of action and ensures the ability of the US to project and sustain power wherever and whenever required.

On an international level, mutually beneficial national interests govern coalition cyberspace force involvement. The AF will cooperate with other nations to resolve regional conflicts and crises, lending support of unique capabilities, and could be supported by international partners. Coalition cyberspace forces will be tailored to each situation, and integrated as needed, based on the national interests of both the US and partner nation. The level of coalition participation is directly influenced by agreements concluded with the partner nation involved.

### **5.2.6 Intelligence Support**

Intelligence helps provide the understanding necessary to conduct AF and joint cyberspace operations. AF cyberspace forces must, where appropriate, take advantage of cyberspace intelligence products to support recurring cyberspace operations. Intelligence support products may relate adversary use of cyberspace I&W, IPOE, and battle damage assessment for decision makers, planners, and the warfighter. The application of all source intelligence remains essential for military operations, as well as supporting national-level security, diplomatic and economic goals.

Detailed accurate characterization of adversaries' cyberspace capabilities and vulnerabilities, including TTPs, is essential to successful military operations. Various IC agencies and organizations must develop I&W criteria to enable accurate anticipation, prediction, assessment, gauging and countering, and mitigation of intrusions and attacks, as well as enable denial, degradation, disruption, deception, etc., of adversary use of the cyberspace domain for hostile

intent. Intelligence support products, responsive to information requests from AFSPC cyberspace organizations, must be rapidly coordinated, prioritized, and disseminated to facilitate both operations and operations planning. Intelligence support will facilitate the cyberspace ISR capabilities and related intelligence products as described in section 5.1.4.1.

### **5.2.7 Integration and Interoperability**

To achieve the maximum potential of a joint force, and to meet AF demands for cyberspace operations, a capability-driven organization is needed to coordinate diverse assets from geographically separate locations, integrating and synchronizing them with other operations across all domains. This dynamic model will be built around components extracted from existing organizations, new operational organizations, and ongoing operational partnerships established with other AF organizations, other Services, federal, state, local, NGO, private sector, academia and international partners. Coordinating and integrating across the AF, DoD, and interagency communities will be critical to create a framework for effective cyberspace operations. Working as a component organization for USSTRATCOM will effectively infuse AF cyberspace operations into joint and interagency planning and resource allocation. Integration and interoperability will also depend on a legal and policy framework to guide common planning and operations.

All DOTMLPF processes employed throughout the AF will institutionally ensure all networks and services will be designed and operated to maximize the potential for the *right* data to be available at the *right* time, in the *right* format to the *right* place, in a properly protected manner. Activities will be conducted in a manner that supports full life-cycle decision making to avoid unintended consequences, given the high degree of interconnectivity within cyberspace, as well as between cyberspace and other warfighting domains.

### **5.2.8 Force Protection**

Cyberspace capabilities are dependent on force protection capabilities. Cyberspace resources (personnel, equipment and facilities) must be protected against all threats, including man-made major accidents, natural disasters, use of unconventional weapons (including weapons of mass destruction [WMD] and chemical, biological, radiological, nuclear, and high-yield explosive), and use of conventional weapons (kinetic and non-kinetic). Force protection includes capabilities to detect, warn of, and neutralize threats and, as necessary, survive, recover from, and operate in a hostile environment following an attack on cyberspace resources.

### **5.2.9 Total Force Team**

The AF requires a total force team of Airmen, civilians, and contractor personnel with professional skills in cyberspace mission areas. Success in all domains—air, space, and cyberspace—is and will be increasingly dependent upon the success we achieve developing core cyberspace competencies and establishing

career pathways for cyberspace warriors. With increased participation of the Air National Guard (ANG) and Air Force Reserve Command (AFRC), special emphasis to share and coordinate cyberspace operational capabilities facilitates total force integration.

### **5.2.10 Education, Training, Exercises, and Wargames**

Airmen are at the heart of the AF's success, and this will remain true as we posture to gain and sustain both information and cyberspace superiority. The key is the development and employment of skilled personnel able to operate in shifting environments, while employing expanding sets of advanced technologies to achieve effects. The AF will build a force of cyberspace professionals able to plan and execute cyberspace operations at the strategic, operational, and tactical levels.

It is imperative all cyberspace personnel receive timely professional development and high-fidelity training, and they participate in cyberspace-related exercises and wargames. Career progression should follow a building block approach, reflecting functional- and system-specific requirements. In addition, training materials, systems, and processes must be designed to support AF and joint training and exercises.

Cyberspace professionals must be properly trained to operate and exploit cyberspace capabilities. Additionally, AF cyberspace forces must have the ability to train with external organizations (other Services, federal/state/local agencies, private sector, academia, etc.) while minimizing impacts to real-world operations. This requires integrating live, virtual, and constructive training, exercise, and wargaming capabilities.

The cornerstone of cyberspace professional development is a military education continuum that reinforces AF cyberspace cultural awareness over the course of a cyberspace warrior's career. Focused professional development processes and programs are crucial to ensuring cyberspace personnel gain the appropriate competencies to acquire, operate, and support critical cyberspace activities. To that end, the cyberspace professional strategy must describe a structured approach for developing and retaining high-quality cyberspace personnel. This strategy should be built upon a construct similar to proven AF career management models with common initial training, certification, continuing education, and appropriate experiences. Conceptually, there are three levels of certification. Personnel progress from a foundation of technical competency, through demonstrated depth of knowledge, to extensive knowledge in cyberspace operations. Certification criteria are tied to years and types of experience and commensurate training and education. Additionally, certification is an integral part of the assignment process; successful attainment of appropriate certification levels will be key to filling competitive command and staff billets.

AF participates in various wargames to provide appraisals of cyberspace warfighting concepts/theories and to develop strategies to meet emerging

mission needs and mitigate evolving risks and threats. Through exploring technical, programmatic, and operational alternatives to current programs of record, wargaming allows AF to evaluate innovative options and critically assess tradeoffs in military utility between various policy/doctrinal constructs, command and control architectures and proposed force structures. Under existing lessons-learned program, AF fuses wargame findings with its strategies, doctrine, policies, programs, and corporate processes to result in cyberspace actionable insights. These insights are used to improve the Command's organize, train and equip responsibilities as well as to also makes recommendations to external agencies to improve cyberspace mission effectiveness and cross-domain integration with various mission partners. Finally, wargame insights are fed into future wargames in an iterative process to refine new concepts and alternative approaches to solving future challenges. The fundamental purpose of AF participation in wargaming is to improve future cyberspace mission capabilities.

## 6.0 SEQUENCED ACTIONS

### 6.1 Introduction

*“Citizens and businesses must be able to rely on the security of information networks. In an interconnected world, an attack on one nation’s networks can be an attack on all.”*

**Hillary Rodham Clinton, US Secretary of State**

The vision for cyberspace operations capabilities is that they will be ready and responsive to joint warfighters’ needs across the range of military operations. This section describes how these capabilities will be employed in the continuum from nominal/steady state, to crisis/conflict, to post-conflict.

### 6.2 Nominal/Steady State Operations

The cyberspace domain is a “contested environment.” Even in the nominal/steady state, there is a level of network probing by various actors searching for vulnerabilities. When cyberspace forces or systems detect an abnormality, operators will alert and coordinate response activities, examine the abnormality in view of all else that is occurring within the global operational environment, and seek to determine whether the abnormality is the result of hostile, non-hostile, or environmental effects. Cyberspace forces will evaluate and assess potential COAs, including adversary actions (e.g., capabilities, opportunities, and likely intent), conduct response activities, and provide notifications.

Nominal/steady state operations are those activities occurring on a daily basis prior to the occurrence of some escalatory event causing a change in directed military alert posture, operational state, or operating tempo. Friendly force activities focus on optimizing the operational environment, maintenance/modernization actions, developing and implementing defenses for vulnerabilities, responding to loss of physical connectivity, continuously evaluating the current state of the cyberspace environment, and system failures caused by any number of events (e.g., cable cuts, power outages, hardware failures, natural disasters, etc.).

24 AF will exercise C2 of AF networks and assigned AF cyberspace forces through the 624th Operations Center (624 OC). This control is exercised from the 624 OC through the Integrated Network Operations and Security Centers (I-NOSCs) and other 24 AF units. The 624 OC will publish the AF cyber tasking order (AF-CTO), maintenance tasking order (MTO), cyber control order (CCO), and time compliance network order (TCNO) to command and control AF cyberspace forces. AF MAJCOMs will continue to maintain their unique networks in accordance with 624 OC orders, until these mission-unique networks and their operations are subsumed by the I-NOSCs and fall under the authority of 624 OC.

Complete SA is a key aspect of our day-to-day cyberspace readiness, as limited attacks may not initially involve AF cyberspace resources. A denial of service

(DoS) attack, for example, may be targeted against a commercial entity, but our ties to that organization, or the fact we share a common service delivery point, could affect the AF infrastructure.

ISR information archives are accessed routinely to maintain awareness of cyberspace system characteristics/capabilities, and facilitate COA planning and development. Data and information are continuously fused and correlated to maintain a complete and current picture of the operational environment. Interactive two-way tasking, assessments, and evaluations are conducted with appropriate activities. Cyberspace IPOE is continuously updated and routine I&W and PBA activities (e.g., target development and ISR strategy, planning and execution) are ongoing. 24 AF/624 OC will coordinate AF cyberspace operations with United States Cyber Command (USCYBERCOM) who in turn is responsible for coordinating with other JFCs to develop cyberspace operation plans (OPLANs) and concept plans (CONPLANs).

### **6.3 Crisis/Conflict**

For this concept, a crisis is defined as an incident or situation involving a threat to the nation's cyberspace, which develops rapidly and creates a condition such that commitment of military forces/resources is contemplated to achieve and/or maintain national objectives. In comparison, a conflict describes an armed struggle/clash between organized groups within a nation or between nations in order to achieve limited political or military objectives. A conflict is defined further as an adversary's action confined to the cyberspace domain, constrained in scope and level of the action, where our response to the threat may be exercised in an indirect manner while supportive of other instruments of national power.<sup>14</sup>

#### **6.3.1 Threat Event (Surge Operations)**

When a threat is identified, cyberspace forces must rapidly execute capabilities to reduce and/or eliminate the threat. The fact that any network threat was identified increases the potential the AF cyberspace infrastructure could be affected. ISR operations must update PBA products and determine the nature of the threat, what systems and/or networks are being targeted, what the potential impact to the cyberspace infrastructure is, what defenses currently exist, and what the response, if any, will be. Cyberspace forces will develop and/or finalize response plans. TTPs to combat the identified threat will be validated and executed.

#### **6.3.2 Attack in Progress**

Even with proper safeguards, a determined adversary could successfully launch an attack against the AF cyberspace infrastructure. A primary goal during an attack is to ensure friendly forces maintain the freedom to operate. During a cyberspace attack, network-connected devices and net-enabled applications might be unavailable, and/or their reliability and accuracy would be questionable.

---

<sup>14</sup> JP 3-0, *Joint Operations*, Change 2, 22 Mar 10.

As we “fight through” the attack, cyberspace forces will respond rapidly to limit and combat the attack, and will posture cyberspace resources to support the warfighter. AF cyberspace personnel will possibly initiate a measured response to ensure we maintain the freedom to act in the cyberspace domain.

If an event is determined to be hostile, USSTRATCOM forces enter a heightened state of alert. As directed, cyberspace response forces execute or develop COAs with potential response options. The response option chosen will depend upon, among other things, identifying the source of the attack, the nature of the culpable party (state or non-state actor), the general level of peace or tension between the US and any state or non-state actor, and the impact the attack had on the US national security posture. If this act occurs in nominal/steady state, the response will be politically driven, and the choice of options (military, economic, or diplomatic) will likely reside with the President. There will be some preapproved response options focused on the survivability of cyberspace systems. These preapproved options will be executed, on order, at the tactical level, based on the appropriate attack indications.

If a military response has been authorized, responsibility for planning and executing the response will depend on the situation. For example, when a target in the source AOR is approved, and the AOR commander has sufficient forces in the region to respond, the commander will have responsibility to plan and execute the response. If there are insufficient forces in the region, an alternate commander may be called upon to support the response (e.g., USCYBERCOM). Likewise, USCYBERCOM may conduct joint cyberspace operations necessary to attain and sustain cyberspace control. Global cyberspace operations will be synchronized (e.g., effects-based plans and operations) with regional JFC operations to maximize desired warfighting effects and attain joint military objectives.

### **6.3.3 Cyberspace Offensive Operations**

Cyberspace operations may employ force application in support of combatant commander (CCDR) desired effects. The process begins with a target nomination, or a request, for a desired effect from a combatant command to USSTRATCOM, who in turn will task USCYBERCOM via a fragmentary order (FRAGO). At this point there are three potential options USCYBERCOM could exercise:

#### **6.3.3.1 Cyberspace Offensive Operations – Option 1**

USCYBERCOM tasks 24 AF to plan and/or execute a requested operation. In this situation, 24 AF could be tasked to stand up an operational planning team, consisting of appropriate A-staff, subordinate and supporting units to develop the required planning products. The products may include, at a minimum: COAs; CONOPs; employment sustainment schedule; PBA products (high value target [HVT] matrix, adversary COAs, named areas of interest [NAIs], target folders, and assessment criteria); weapon solutions; weapon fact sheet; collateral

damage expectation; and intelligence collection plan. The entire planning process is supported by the intelligence community.

Once planning is complete and the decision is made to execute cyberspace warfare operations, the requesting combatant command will engage the Joint Staff/Secretary of Defense (SecDef) and gain authorities to commence offensive operations. USCYBERCOM will validate the target and deconflict/coordinate/collaborate with interagency organizations, as necessary. Furthermore, USCYBERCOM will develop the cyberspace strike package, schedule the operation, direct the operation, and prepare revisit schedules.

When USCYBERCOM tasks 24 AF to plan/execute the operation, 24 AF, in turn, via its normal operation center processes, tasks subordinate cyberspace warfare units to execute the desired operation. Other cyberspace units will support as directed.

#### **6.3.3.2 Cyberspace Offensive Operations – Option 2**

USCYBERCOM could choose to plan the operation and task 24 AF to provide, and/or weaponize, the appropriate tool for their use.

#### **6.3.3.3 Cyberspace Offensive Operations – Option 3**

USCYBERCOM exclusively plans and executes the operation with organic assigned forces. There would be no direct 24 AF involvement.

### **6.4 Post Conflict: Return to Nominal/Steady State Operations**

Throughout the network threat/attack phase, cyberspace operators will work to transition resources back to their pre-event operational status. Constantly monitoring and assessing the cyberspace domain will enable the transition to a new steady state. Cyberspace forces will restore any compromised system(s) to operational status in a systematic manner to ensure proper support to AF forces worldwide. Cyberspace defense personnel will remain postured to deter the adversary and maintain positive control over AF cyberspace assets.

### 7.0 COMMAND RELATIONSHIPS

Controlling elements of cyberspace integral to AF missions is fundamental to delivering effects across the range of military operations. Figure 7 shows the command relationships necessary to enable the unified C2 of cyberspace forces.

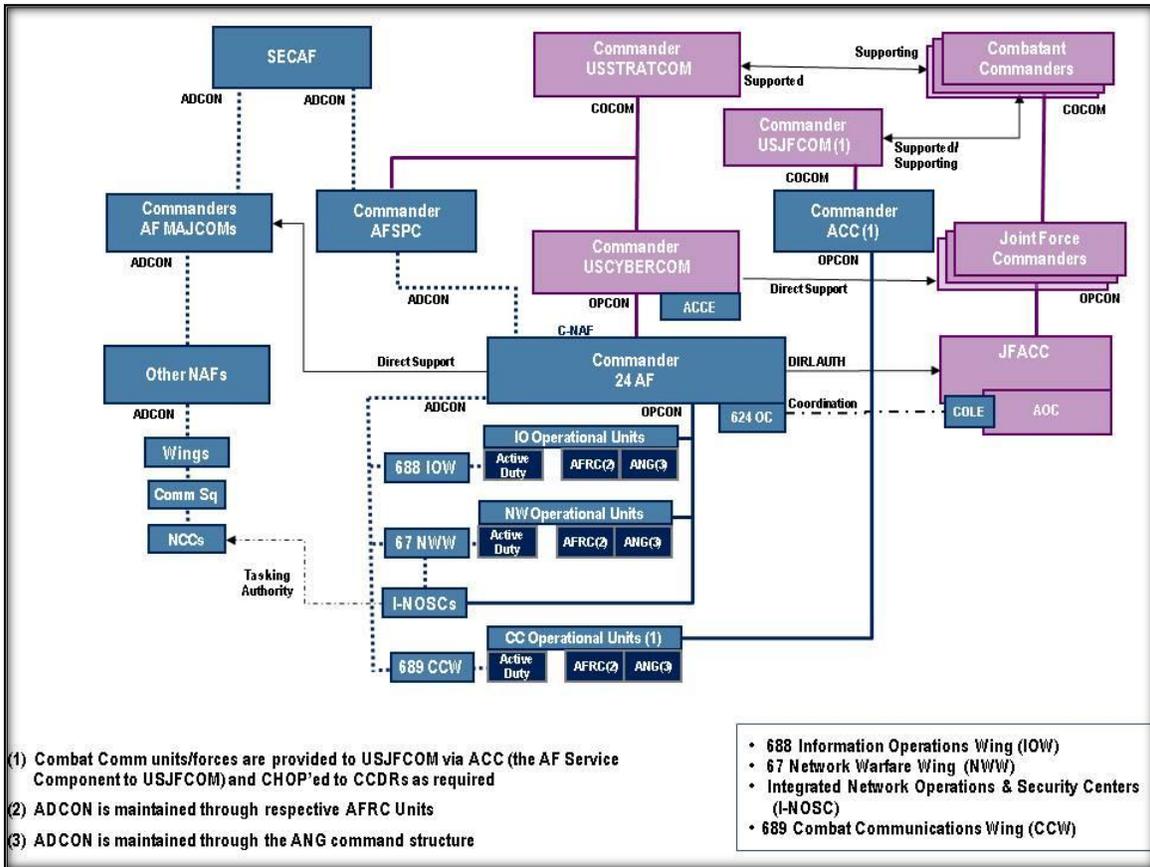


Figure 7. Cyberspace Command Relationships

AFSPC is the AF component to USSTRATCOM for space and cyberspace. In this role, AFSPC/CC is the commander, Air Force forces (COMAFFOR) for AF space and cyberspace forces, exercising administrative control (ADCON) over those forces. CDRUSSTRATCOM has delegated OPCON of assigned cyberspace forces to subordinate joint and functional commanders, including the sub-unified command, USCYBERCOM. 24 AF is the AF Component to USCYBERCOM and as such, gains the C-NAF designator 24 AF (AFCYBER). Also in this role, 24 AF Commander (24 AF/CC) is the COMAFFOR to USCYBERCOM and will execute operational tasks as directed [Note: To date USCYBERCOM has not delegated OPCON to 24 AF (AFCYBER)]. 24 AF/CC also performs AF Service-specific tasks as directed by SECAF. These responsibilities are primarily within his authority as the AF Network Operations Commander (AFNetOps/CC).

## 7.1 Cyberspace Support/Defense Relationships

24 AF is responsible (at the operational level) for the operations, defense, protection, and security of the AF portion of the DoD network.

The 624 OC conducts C2 of cyberspace defense forces. In this role, the 624 OC staff uses the commander's daily guidance, existing strategic guidance, joint direction, and ISR inputs to refine the cyberspace operations directive.

To increase AFNet defensive posture and effectively adapt to a wide range of threats, 24 AF will continue to actively strengthen/expand and directly rely on its existing partnerships with other Services, federal, state, local, NGO, private sector, academia and international organizations/agencies. These partnerships will help 24 AF understand system vulnerabilities and threats resident with the cyberspace domain and clarify potential ambiguities between the DoD and partners' cyberspace boundaries. The 624 OC will employ processes to rapidly and actively adjust AFNet defenses in response to vulnerabilities/threats occurring within partner networks.

In its mission assurance role, 24 AF will work with the MAJCOMs and deployed units to ensure network availability in support of AF operational missions. 24 AF, through the 624 OC, will ensure AFNet components supporting a mission are ready and available. The goal is to prevent a portion of the network from being degraded or otherwise impacted when that part of the AFNet is directly supporting joint and/or deployed operations.

## 7.2 Cyberspace Force Application Relationships

Current *cyber attack* relationships are codified in joint documents and war plans; 24 AF cannot modify those relationships without involvement of the affected joint commands. Currently, 24 AF units have supporting relationships with USCYBERCOM and other CCDRs. These relationships, in some cases, are non-standard and must be codified. This is unlikely to happen until the new joint command is activated and the joint staff takes a comprehensive look at all *cyber attack* command relationships. There are several considerations that will likely affect future command relationships for *cyber attack*:

- Any *cyber attack* or *cyber enabling* operations planned/commanded and controlled by 24 AF will be as a component command to USSTRATCOM (i.e., USCYBERCOM)
- Future support to other CCDRs will likely be through USCYBERCOM in its supporting relationship

To ensure 24 AF is in a position to provide real value to the joint warfighter, the following strategy is proposed for 24 AF support to USCYBERCOM. 24 AF should work with USCYBERCOM to identify AF relevant targets. Specific responsibilities entail developing and maintaining target folders, developing, testing and updating capabilities necessary to service those targets, and training and certifying AF personnel to deliver capabilities within the constraints codified in the war plans developed for USCYBERCOM. 24 AF will develop the

processes and procedures to plan and execute those capabilities through the 624 OC. Finally, 24 AF personnel will be trained and exercised in a joint environment.

Cryptologic *cyber enabling* is conducted under the authority of the Director, NSA. 24 AF units will conduct cryptologic *cyber enabling* within those authorities in support of IC, joint, and AF missions.

### **7.3 Relationship with AF Component Commands**

As the AF C-NAF commander to USSTRATCOM, the 24 AF/CC will interact with other AF component commanders in a COCOM role, dependent upon USCYBERCOM's role. In addition, the 624 OC will coordinate cyberspace operations with the component command's air and space operations center (AOC) when defensive operations are being conducted to protect the AFNet. The 624 OC will also maintain SA of operations within the combatant command assigned joint operating areas (JOAs) to ensure the network is prepared to support task orders, as appropriate.

The primary interface between the 624 OC and the AF Component Commands will be the cyberspace expertise integrated into the theater staff. During contingencies, 24 AF may deploy a cyberspace operations liaison element (COLE) to support the theater staff. As USCYBERCOM evolves, senior leader cyberspace expertise will be provided to the theater.

### **7.4 Relationship with Combatant Commands**

The 24 AF will support CCDRs based on the existing supporting/supported relationship established in applicable OPLANS. CCDRs will coordinate with the 24 AF through USCYBERCOM (via the air component coordination element [ACCE]), or with their component commands, to plan and use AF cyberspace capabilities. Those capabilities will be delivered based on standing supported/supporting command relationships. In addition, AF combat communications forces/assets are presented to JFCOM via Air Combat Command (ACC) as the AF Service Component.

### **7.5 Relationship with Air Force Units**

The 24 AF/CC is responsible for defense and management of the AF portion of the GIG. This role carries two significant global responsibilities: 1) the operational defense of the AFNet; and 2) ensuring the AFNet is prepared and ready to support assigned operations. Air, space or cyberspace operations in an assigned area of responsibility may require actions in another AOR to ensure mission success. A threat can attack part of the AFNet in one region to deny critical mission data to another region (along with potentially gaining access to other parts of the DoD GIG). Therefore, the 24 AF/CC must have a global perspective to protect and maintain the AFNet. This may require minute-by-minute coordination with component command AOCs during defensive operations and critical mission execution.

## 7.6 Relationship with Air Force Reserve and Guard Units

Current and future cyberspace forces are/will be a mix of regular, AFRC, and ANG units. Currently, AFRC and ANG units support all cyberspace missions (support, defense and force application) as well as other cyberspace functions (e.g., C2, ISR, training, etc.). During normal day-to-day operations, administrative control (ADCON) for AFRC cyberspace forces is maintained through their respective Reserve Numbered Air Force (NAF) chain (i.e., 4 AF, 10 AF and 22 AF). For ANG cyberspace forces, ADCON is maintained by their respective ANG command structure. In the case where these units are mobilized to support ongoing cyberspace operations, operational direction (OPDIR) comes from HQ AFSPC, which in turn, may delegate to a subordinate unit (e.g., 24 AF).<sup>15</sup> OPDIR will exist on a day-to-day basis when a reserve component unit has a classic association relationship with a regular AF unit (reserve component not mobilized). When an air reserve component unit is mobilized, normal OPCON will be will be employed.

---

<sup>15</sup> Operational Direction defined in AFI 90-1001, *Responsibilities for Total Force Integration*, 29 May 2007

## 8.0 SUMMARY

Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. The vastness, complexity, volatility, and rapid evolution of cyberspace place a premium on continuous I&W, PBA development, and threat attribution and characterization. Ensuring freedom of action in cyberspace is a complex undertaking that requires comprehensive SA, understanding relevant network segments, and an exceptionally rapid decision cycle to ensure freedom of action within the cyberspace domain.

Cyberspace superiority enables and enhances operations in the cyberspace, air, land, maritime, and space domains at a given time and place of our choosing. Offensive operations take advantage of cyberspace freedom of action by creating effects in other domains. Operations to achieve cyberspace superiority can be integrated with the operational rhythm of appropriate Operations centers. Gaining and maintaining access is critical to achieving the desired effects and countering adversary use of cyberspace

US forces will operate through a cyberspace attack, recognizing and isolating an attack while continuing to perform critical actions. Following an attack, they will rapidly reconstitute and regenerate capability.

Offensive operations deny, deceive, degrade, disrupt, destroy, alter, or otherwise adversely affect an adversary's ability to use cyberspace against US objectives.

Cyberspace dynamic defensive operations seek to deter adversaries from intruding on friendly networks, detect and deny access when attacks are attempted, and minimize the effectiveness of attacks.

Cyberspace personnel are trained to establish, control, and project combat power in, through, and from cyberspace. To be successful in this new era of cyberspace operations, cyberspace professional development is paramount.

*"Our Air Force needs to control our portion of cyberspace while protecting our information from adversary action, and integrate cyberspace planning, operations and execution into air and space operations."*

**APPENDIX A: REFERENCES**

1. *24 AF Command & Control and Operations of Cyberspace Forces*, 5 May 2009
2. *AFDD 2-9, Intelligence, Surveillance and Reconnaissance Operations*, 17 July 2007
3. *AFDD 3-12, Cyberspace Operations (Draft)*, March 2010
4. *AF Instruction 90-1001, Responsibilities for Total Force Integration*, 29 May 2007
5. *AFSPC Cyberspace Superiority Hierarchy*, 25 March 2010
6. *AFSPC Memorandum, Strategy-to-Task for Twenty-Fourth Air Force Cyberspace Operations*, 30 March 2009
7. *AFSPC High-Level Operational Concept – OV-1 – AF Cyberspace Mission*, Version 1.5, 7 April 2009
8. *AFSPC Programming Plan 09-04, Actions to Implement Phase 1 of the Secretary of the Air Force Direction to Organize Cyber Forces*, 15 June 2009
9. *Air Force Cyberspace Command Architecture; Version 1.3*, 10 June 2008
10. *Air Force Cyberspace Mission Architecture; Version 1.5*, March 2009
11. *Air Force Agile Combat Support CONOPS*, 15 November 2007
12. *Air Force Global Persistent Attack CONOPS*, 28 July 2006
13. *Air Force Global Strike CONOPS*, 27 December 2006
14. *Air Force Homeland Defense and Civil Support CONOPS*, 1 March 2006
15. *Air Force Space & C4ISR CONOPS*, 28 April 2006
16. Center for Strategic and International Studies (CSIS) Commission on Cybersecurity, *Securing Cyberspace for the 44<sup>th</sup> Presidency*, December 2008
17. Chairman of the Joint Chiefs of Staff (CJCS) Memorandum, *Definition of Cyberspace Operations*, 18 August 2009
18. CJCS Memorandum, *The National Military Strategy for Cyberspace Operations*, December 2006
19. CJCS Memorandum (CM-0363-08), *Updated Definition of Cyberspace*, 10 July 2008
20. *Cyberspace Joint Operating Concept, Working Version*, 14 May 2010
21. *Deterrence Operations JOC*, Version 2.0, December 2006
22. *DoD Homeland Defense and Civil Support JOC*, Version 2.0, 1 October 2007
23. *Irregular Warfare JOC*, Version 2.0, 11 September 2007
24. Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, Amended through 31 October 2009
25. Joint Publication 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, 16 June 2009

26. Joint Publication 3-0, *Joint Operations*, Change 2, 22 March 2010
27. Joint Test Publication 3-12, *Cyberspace Operations (First Draft)*, 23 March 2010
28. *Major Combat Operations JOC*, Version 2.0, December 2006
29. *Military Contribution to Cooperative Security JOC*, Version 1.0, 19 September 2008
30. *Military Contribution to Stabilization, Security, Transition, and Reconstruction Operations JOC*, Version 2.0, December 2006
31. Office of the President of the United States, *Cyberspace Policy Review*, 29 May 2009
32. Office of the President of the United States, *The National Strategy to Secure Cyberspace*, February 2003
33. Office of the Secretary of Defense, *Quadrennial Defense Review Report*, 1 February 2010
34. *Rise of the Cyber Wingman Philosophy*, November 2009
35. SECAF Memorandum, *USCYBERCOM and Our Way Ahead with 24th AF*, 16 August 2009
36. United States Air Force, *Blueprint for Cyberspace*, 2 November 2009
37. United States Air Force, *Global Integrated Intelligence, Surveillance and Reconnaissance Service Core Function Plan (Draft)*, March 2010
38. United States Air Force, *Space and Cyberspace Superiority Core Function Master Plan (Draft)*, March 2010
39. USAF Chief of Staff Memorandum, *Authority of Air Force Network Operations Commander to Issue Network Operations Orders for the Operation, Maintenance, and Control of Air Force Networks*, 15 May 2009
40. United States Army, *Concept of Operations, Cyberspace 2010 – 2017 (Draft)*, 3 September 2009
41. United States Government Accountability Office, *Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*, May 2005
42. United States Government Accountability Office, *National Cybersecurity Strategy, March 2009*
43. United States Marine Corps, *Cyberspace Concept*, 17 July 2009
44. United States Strategic Command Concept Plan 8039, *Cyberspace Operations*, 28 February 2008

## APPENDIX B: GLOSSARY OF TERMS, ABBREVIATIONS AND ACRONYMS

### TERMS

**Administrative Control (ADCON):** Direction or exercise of authority over subordinate or other organizations in respect to administration and support, including organization of Service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. (JP 1)

**Air Force Air and Space Operations Center (AOC):** The senior agency of the AF component commander that provides command and control of AF air and space operations and coordinates with other components and Services. (JP 3-09.3)

**Air Force Network (AFNet):** The AF-provisioned portion of the GIG that the AF has primary responsibility for procurement, operations, and defense. It provides global connectivity and services, in addition to C2 of that connectivity and those services that enable AF commanders to achieve information and decision superiority in support of AF mission objectives. The AFNet consists of fixed, mobile, and deployable facilities, and equipment, as well as processes, trained personnel and information. (Adapted from AFPD 13-3)

**Air Force Network Operations (AFNetOps):** The operational construct the AF employs for C2, and defense of the AF-GIG. It provides assured and timely network-centric services across (through and throughout) cyberspace to include: terrestrial, space, and airborne domains, at the strategic, operational and tactical levels in support of the DoD's full spectrum of warfighting, intelligence, operational support, and business missions. AFNetOps encompasses information assurance, system and network management, and information dissemination management. It includes the organizations, processes, procedures, and tasks required to plan, administer, monitor, and secure Air Force networks in support of operations and also to respond to warfighter requirements, outages and other operational impacts. (AFPD 13-3)

**Area of Responsibility (AOR):** The geographical area associated with a combatant command within which a CCDR has authority to plan and conduct operations. (JP 1)

**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 an effect, or achieving an objective; 3) Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity; 4) Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (JP 3-0)

**Attribution:** A determination based on available evidence, of responsibility for unauthorized activity (*cyber attack*, intrusion, or other malicious activity) within a network or automated information system. (Note: "Responsibility" includes

ordering, planning, or executing the unauthorized activity; “unauthorized activity” includes any activity not approved by the owner or administrator of the affected system.)

**Capability:** The ability to execute a specified course of action (JP 1-02) or the military means to achieve a desired end. (AFPD 10-28)

**Conflict:** An armed struggle or clash between organized groups within a nation or between nations in order to achieve limited political or military objectives. Although regular forces are often involved, irregular forces frequently predominate. Conflict often is protracted, confined to a restricted geographic area, and constrained in weaponry and level of violence. Within this state, military power in response to threats may be exercised in an indirect manner while supportive of other instruments of national power. Limited objectives may be achieved by the short, focused, and direct application of force. (JP 3-0)

**Command and Control (C2):** The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP 1)

**Computer Emergency Response Team/Computer Incident Response Team:** An organization chartered by an information systems owner to coordinate or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems. (The National Strategy to Secure Cyberspace)

**Counterattack:** Attack by all or part of a defending force against an adversary cyberspace attack. (Adapted from JP 1-02)

**Counterintelligence (CI):** Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 2-0)

**Counterpropaganda Operations:** Those psychological operations activities that identify adversary propaganda, contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces. (JP 3-53)

**Crisis:** An incident or situation involving a threat to a nation, its territories, citizens, military forces, possessions, or vital interests that develops rapidly and creates a condition of such diplomatic, economic, political, or military importance that commitment of military forces and resources is contemplated to achieve national objectives. (JP 3-0)

**Cyber Attack:** Cyber warfare actions intended to deny or manipulate information and or infrastructure in cyberspace. Cyber attack is considered a form of fires. (Draft JTP 3-12)

**Cyber Defense:** Actions to deter, protect, monitor, analyze and defeat any uses of cyberspace that deny friendly combat capability and unauthorized activity within the DoD information enterprise, including the GIG. (Draft JTP 3-12)

**Cyber Enabling:** Actions to search for, locate, identify, penetrate, characterize and collect data from targets in cyberspace for research, threat recognition, targeting, planning and conduct future operations and other measures short of attack to prepare potential targets for future operations. (Draft JTP 3-12)

**Cyber Warfare:** The creation of effects in and through cyberspace in support of combatant commanders' military objectives. Composed of *cyber attack*, *cyber defense*, and *cyber enabling actions*. (Draft JTP 3-12)

**Cyberspace:** A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. (CJCS CM-0363-08)

**Cyberspace Operations:** The employment of cyberspace capabilities where the primary purpose is to achieve objectives in, through, and from cyberspace. Such operations include computer network operations and activities to operate and defend the GIG. (CJCS Memorandum, 19 Aug 2009)

**Cyberspace Superiority:** The operational advantage in, through, and from cyberspace over adversaries to defend, exploit and conduct offensive operations at a given time and place, without effective interference. (Draft JTP 3-12)

**Cyberspace Tactics Analysis and Reporting Program (TARP):** The AF TARP is used to analyze and evaluate the operational tactics, training, and employment of forces of potential adversaries. The TARP reports findings in a format and timeline that satisfies the specific needs of AF operators, intelligence personnel, and operational planners. The TARP ensures all-source intelligence, to include cryptologic information, is integrated with an operational perspective to provide tailored products that support AF tactics development, operational planning, and threat replication training. (Adapted from AFI 14-120)

**Defensive Counter-Cyber (DCC):** All defensive countermeasures designed to detect, identify, intercept and destroy or negate harmful activities attempting to penetrate or attack through cyberspace. DCC missions are designed to preserve friendly network integrity, availability and security and protect friendly cyber capabilities from attack, intrusion, or other malicious activity by pro-actively seeking intercepting, and neutralizing adversarial cyber means which present threats. (JTP 3-12, proposed cyberspace lexicon)

**Direct Liaison Authorized (DIRLAUTH):** That authority granted by a commander (any level) to a subordinate to directly consult or coordinate an action with a command or agency within or outside of the granting command. Direct liaison authorized is more applicable to planning than operations and always carries with it the requirement of keeping the commander granting direct liaison authorized informed. Direct liaison authorized is a coordination relationship, not an authority through which command may be exercised. (JP 1)

**Dynamic Defense:** The synchronized real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities, and outmaneuver adversaries, in order to defend cyberspace and enable freedom of action. (Draft JP 3-13)

**Electronic Warfare (EW):** EW includes military actions using electromagnetic and directed energy to control the electromagnetic spectrum, or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support. EW is employed in the Force Application mission area. As a consolidation of effective and viable platforms, EW is a complementary asset to enable or support cyberspace effects. Cyberspace operations must de-conflict with EW operations. (JP 3-13.1)

**Exploitation:** 1) Taking full advantage of success in military operations, following up initial gains, and making permanent the temporary effects already achieved. 2) Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. 3) An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. (JP2-01.3)

**Fires:** The use of weapon systems to create a specific lethal or nonlethal effect on a target. (JP 3-0)

**Global Information Grid:** The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 6-0)

**Indications and Warning (I&W):** Through continuous surveillance, or as required reconnaissance, ISR provides timely and near-real time information necessary to assess potential (cyber) threats to the US and its allies. I&W products are derived from a worldwide I&W system that analyzes and integrates operations and intelligence to assess the probability of hostile actions, and provides sufficient warning to preempt, counter, or otherwise moderate their outcome. I&W systems rely on tip-offs from sources at all levels. (AFDD 2-9)

**Infiltration:** Penetrate areas of the cyberspace domain and avoid detection. (Adapted from JP 3-05.1)

**Influence Operations:** The AF uses this term to group the activities of PSYOP, MILDEC, and OPSEC. (JP 3-13.2)

**Information Assurance:** Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (JP 3-13)

**Information Operations:** The integrated employment of the core capabilities electronic warfare, computer network operations, psychological operations,

military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (JP 3-13)

**Information Superiority:** The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP 3-13)

**Intelligence:** The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; it is the information and knowledge about a topic obtained through observation, investigation, analysis, or understanding. (JP 2-0)

**Intelligence Preparation of the Operational Environment (IPOE):** The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the JFC's decision making process. It is a continuous process that includes defining the operational environment, describing the impact of the operational environment, evaluating the adversary, and determining adversary courses of action. (Adapted from JP 2-01.3)

**Intelligence, Surveillance, and Reconnaissance (ISR):** An activity that synchronizes and integrates the planning and operation of sensors, assets, processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. The goal of ISR operations is to provide accurate, relevant, and timely intelligence to decision makers. (JP 2-01)

**Interdiction:** An action to divert, disrupt, delay, or destroy an adversary's cyberspace capability before it can be effectively used against friendly forces or resources. (Adapted from JP 3-03)

**Joint Force Commander (JFC):** A general term applied to a combatant commander, sub-unified commander, or joint task force commander authorized to exercise combatant command (command authority) or operational control over a joint force. (JP 1)

**Maneuver:** Operation to place friendly cyberspace forces or capabilities in a position of advantage over the adversary. (Adapted from JP 3-0)

**Military Deception (MILDEC):** MILDEC includes actions executed to deliberately mislead adversary military decision makers as to friendly military capabilities, intentions, and operations, causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (JP 3-13.4)

**Network:** A system of computers, peripherals, terminals, and databases connected by communications lines. (Merriam-Webster New World Dictionary)

**Network Operations (NETOPS):** Activities conducted to operate and defend the Global Information Grid. (JP 6-0)

**Nongovernmental Organization (NGO):** A private, self-governing, not-for-profit organization dedicated to alleviating human suffering; and/or promoting education, health care, economic development, environmental protection, human rights, and conflict resolution; and/or encouraging the establishment of democratic institutions and civil society. (JP 3-08)

**Offensive Counter-Cyber (OCC):** Offensive operations to destroy, disrupt, or neutralize adversary cyberspace capabilities both before and after their use against friendly forces, but as close to their source as possible. The goal of OCC operations is to prevent the employment of adversary cyberspace capabilities prior employment. (JTP 3-12, proposed cyberspace lexicon)

**Operational Control (OPCON):** Command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority) and may be delegated within the command. Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate JFCs and Service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions; it does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. (JP 1)

**Operational Direction (OPDIR):** Authority to designate objectives, assign tasks, and provide the direction necessary to accomplish the mission or operation and ensure unity of effort. Authority for operational direction of one component member over members of another component is obtained by agreements between unit commanders (most often between Title 10 and Title 32 commanders) whereby these component commanders, in an associate organizational structure, issue orders to their subordinates to follow the operational direction of specified/designated senior members of the other component for the purpose of accomplishing their associated mission. (AFI 90-1001)

**Operational Environment:** The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission. This includes the air, land, maritime, space, and cyberspace domains, as well as the included enemy and friendly forces, facilities, weather, terrain, the electromagnetic spectrum, and the information environment within the operational areas and areas of interest. (Adapted from JP 3-0)

**Operations Security (OPSEC):** OPSEC includes a process of identifying critical information, and subsequently analyzing friendly actions attendant to military operations, to: 1) identify actions that can be observed by adversary intelligence systems; 2) determine indicators that adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and 3) select and execute measures that eliminate, or the desire to reduce to an acceptable level, the vulnerabilities of friendly actions to adversary exploitation. (JP 3-13.3)

**Predictive Battlespace Awareness (PBA):** PBA influences all elements of the intelligence process. PBA is a multidimensional understanding of the battlespace in time, space, and effect. It is the capability to correlate and fuse patterns of enemy activity and subsequent events to predict adversary intent or potential future enemy courses of action. PBA is continuous and achieved by the commander through possession of relevant, comprehensive knowledge, including an accurate forecast of pertinent influences in the battlespace. This knowledge of the operational environment, in concert with C2, permits commanders to anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities. Our ability to act with a degree of speed and certainty not matched by our adversaries permits commanders to shape the battlespace to our advantage. To achieve this level of awareness requires the development of five key elements: intelligence preparation of the operational environment, target development, ISR strategy and planning, ISR employment, and assessment. These elements are continuously refined, in parallel, to provide a comprehensive view of the battlespace which provides commanders with the capability to anticipate future conditions, assess changing conditions, establish priorities, and exploit emerging opportunities while mitigating the impact of unexpected adversary actions. (AFDD 2-9)

**Psychological Operations (PSYOP):** Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. (JP 3-13.2)

**Situational Awareness (SA):** The requisite current and predictive knowledge of the cyberspace environment and the operational environment upon which all operations depend—including physical, virtual, and human domains—as well as all factors, activities, and events of friendly and adversary forces across the spectrum of conflict. (Adapted from JP 1-02)

**Strategic Communications:** Focused efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable for the advancement of US Government interests, policies, and objectives. Strategic communications encompasses coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power. (Adapted from JP 3-13)

**Target Development:** Targeting links strategy to tactical application of air, space (and cyber) power, helping to determine the most efficient and effective means to create desired effects. Targeting is a multi-staged, iterative process, which may span the full spectrum from lethal to non-lethal applications of force. Target development is a focused, systematic analytical examination of potential target systems to determine the criticality, vulnerability, and suitability of each target as well as relationships between and within target systems in order to create the desired effects that achieve the commander's objectives. By identifying those relationships and critical vulnerabilities, the commander's utilization of PBA is enhanced through a clear understanding of how the cumulative effects impact the adversary. Target development has five distinct functions: target analysis, target vetting, target validation, target nomination, and establishing collection and exploitation requirements. (AFPAM 14-114)

**Unity of Command:** The principle of war that ensures the concentration of effort for every objective is assigned to one responsible commander. (AFDD-1)

**ABBREVIATIONS AND ACRONYMS**

24/7/365	24 hours a day, 7 days a week, 365 days a year
24 AF	Twenty-Fourth Air Force
ACC	Air Combat Command
ACCE	Air Component Coordination Element
ADCON	Administrative Control
AF	Air Force
AFCYBER	Air Force Cyberspace
AFDD	Air Force Doctrine Document
AFNet	Air Force Network
AFNetOps	Air Force Network Operations
AFOpsCs	Air Force Operating Concepts
AFRC	Air Force Reserve Command
AFSPC	Air Force Space Command
ANG	Air National Guard
AOC	Air and Space Operations Center
AOR	Area of Responsibility
APPG	Annual Planning and Programming Guidance
ATO	Air Tasking Order
C2	Command and Control
C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance
C-MAJCOM	Component Major Command
C-NAF	Component Numbered Air Force
CC	Commander or Combat Communications
CCDR	Combatant Commander
CCJO	Capstone Concept for Joint Operations
CCO	Cyber Control Order
CCW	Combat Communications Wing
CDRUSSTRATCOM	Commander, United States Strategic Command
CHOP	Change of Operational Control
CJCS	Chairman, Joint Chiefs of Staff
COA	Course of Action
COCOM	Combatant Command (command authority)
COLE	Cyberspace Operations Liaison Element
COMAFFOR	Commander, Air Force Forces
Comm	Communications

UNCLASSIFIED

Air Force Space Command Functional Concept for Cyberspace Operations

---

CONOPS	Concept of Operations
CONPLAN	Concept Plan
COP	Common Operating Picture
COTS	Commercial Off-the-Shelf
CRRA	Capability Review and Risk Assessment
CS	Cooperative Security (Joint Operating Concept)
CSAF	Chief of Staff of the United States Air Force
CTO	Cyber Tasking Order
DCC	Defensive Counter-Cyberspace
DepSecDef	Deputy Secretary of Defense
DIB	Defense Industrial Base
DIRLAUTH	Direct Liaison Authorized
DO	Deterrence Operations (Joint Operating Concept)
DoD	Department of Defense
DoS	Denial of Service
DOTMLPF	Doctrine, Organization, Training, Material, Leadership and education, Personnel, and Facilities
EP	Emergency Preparation
EW	Electronic Warfare
FRAGO	Fragmentary Order
GIG	Global Information Grid
HD&CS	Homeland Defense and Civil Support (Joint Operating Concept)
HVT	High Value Target
I-NOSC	Integrated Network Operations and Security Center
I&W	Indications and Warning
IA	Information Assurance
IC	Intelligence Community
IO	Information Operations
IOW	Information Operations Wing
IPOE	Intelligence Preparation of the Operational Environment
ISR	Intelligence, Surveillance, and Reconnaissance
IW	Irregular Warfare (Joint Operating Concept)
JFACC	Joint Force Air Component Commander
JFC	Joint Force Commander
JIC	Joint Integrating Concept
JOA	Joint Operating Area
JOC	Joint Operating Concept
JP	Joint Publication

---

UNCLASSIFIED

UNCLASSIFIED

Air Force Space Command Functional Concept for Cyberspace Operations

---

JTP	Joint Test Publication
LOAC	Law of Armed Conflict
MAJCOM	Major Command
MCO	Major Combat Operations (Joint Operating Concept)
MEF	Mission Essential Function
MILDEC	Military Deception
MTO	Maintenance Tasking Order
NAF	Numbered Air Force
NAI	Named Area of Interest
NCC	Network Control Center
NCOE	Net-Centric Operational Environment
NGO	Nongovernmental Organization
NMS-CO	National Military Strategy for Cyberspace Operations
NOSC	Network Operations and Security Center
NSA	National Security Agency
NWW	Network Warfare Wing
OC	Operations Center
OCC	Offensive Counter Cyberspace
OPLAN	Operations Plan
OPDIR	Operational Directive
OPLAN	Operation Plan
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OV	Operational View
PBA	Predictive Battlespace Awareness
PCPAD	Planning & direction, Collection, Processing & exploitation, Analysis & production, and Dissemination
PPBE	Planning, Programming, Budgeting, and Execution
PSYOP	Psychological Operations
QDR	Quadrennial Defense Review
ROE	Rules of Engagement
S&C4ISR	Space and Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance
S&T	Science and Technical
SA	Situation (or Situational) Awareness
SCADA	Supervisory Control and Data Acquisition Systems
SECAF	Secretary of the Air Force
SecDef	Secretary of Defense

---

UNCLASSIFIED

**UNCLASSIFIED**

**Air Force Space Command Functional Concept for Cyberspace Operations**

---

SST&R	Stabilization, Security, Transition, and Reconstitution (Joint Operating Concept)
TCNO	Time Compliance Network Order
TO	Task Order
TTPs	Tactics, Techniques, and Procedures
UDOP	User Defined Operational Picture
US	United States
USAF	United States Air Force
USCYBERCOM	United States Cyber Command
USG	United States Government
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
WMD	Weapon of Mass Destruction

**APPENDIX C: CAPABILITY TRACEABILITY MATRIX**

The below critical JOC capabilities are supported by the capabilities and effects defined in this functional concept.

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<b>Cyberspace Support</b>						
<b>Establish and Extend</b>						
<ul style="list-style-type: none"> <li>• (CS) The joint deployment and distribution enterprise must be capable of operating across the strategic, operational, and tactical continuum with a set of integrated, robust, and responsive physical, information, communication, and financial networks.</li> <li>• (CS) It must be able to rapidly establish and maintain infrastructure whenever and wherever it is needed.</li> <li>• (DO) Having the capability to sustain continuity of effective military or economic operations in the midst or wake of a major enemy attack on the US homeland.</li> <li>• (SST&amp;R) Assist an existing or new host nation government in providing security, essential public services, economic development, and governance following the significant degradation or collapse of the government’s capabilities due to internal failure or as a consequence of the destruction and dislocation of a war.</li> <li>• (SST&amp;R) DoD will also work with interagency, coalition, international, regional, non-government, and private sector partners who possess capabilities that can contribute to SSTR objectives to ensure that they can effectively share information and collaborate in the assured DoD information environment.</li> <li>• (SST&amp;R) In order to establish a sufficiently secure environment for effective civilian-led reconstruction operations to take place, the joint force must do more than just defeat organized military resistance.</li> <li>• (IW) Stability operations. (1) An overarching term encompassing various military missions, tasks, and activities conducted outside the United States in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief.</li> <li>• (IW) Build the required human infrastructure and networks.</li> <li>• (IW) The US military must provide the JFC with an effective joint force projection and sustainment system that is tailorable, survivable, and responsive to joint force requirements when engaged in IW operations.</li> <li>• (MCO) A critical element of deterrence is maintaining capable and rapidly deployable military forces and, when necessary, demonstrating the will to resolve conflicts decisively on favorable terms. This will require forces to operate in and from the global commons (space, international waters and airspace, and cyberspace) and effectively project and sustain forces in distant environments where adversaries may seek to deny us access.</li> <li>• (MCO) The US military must provide the supported JFC with a survivable, responsive, and</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
adaptable force projection and distribution-based sustainment system. This enables the building and delivery of combat power at the right times and locations as determined by the supported JFC. <ul style="list-style-type: none"> <li>• (HD&amp;CS) Integrated C2, and computer systems to enhance preemptive actions by US and coalition forces.</li> </ul>						
<b>Persistent Network Operations</b>						
<ul style="list-style-type: none"> <li>• (CS) Counter virtual domain access denial efforts, the United States must have redundant systems in place, restore access by using commercial resources, use alternative paths.</li> <li>• (SST&amp;R) DoD will support SSTR operations through the evolution and deployment of the net-centric operational environment (NCOE). The NCOE, whose cornerstone is the GIG, will provide information transport, information assurance, enterprise services, and network management, applications, and knowledge management capabilities to facilitate SSTR operations.</li> <li>• (SST&amp;R) The NCOE will link DOD garrison and deployed organizations, and reach back elements to support the full range of military operations.</li> <li>• (SST&amp;R) DoD also will work with interagency, coalition, international, regional, non-government, and private sector partners who possess capabilities that can contribute to SSTR objectives to ensure that they can effectively share information and collaborate in the assured DoD information environment.</li> <li>• (MCO) (Within the Information environment) The innovative combination of electronic weapons platforms, networking systems, and strategic- and operational-level psychological operations, enabled by the net-centric operational environment, creates significant opportunities to seize the initiative and dominate an enemy.</li> <li>• (MCO) Commanders have access to robust and persistent ISR, myriad platform sensors, and the supporting net-centric operational environment to assist in this assessment, including the broader implications associated with the contributions IO make in achieving dominant effects.</li> <li>• (HD&amp;CS) Successful detection, accurate identification, and timely response to physical and cyber threats.</li> </ul>						
<b>Secure and Protect</b>						
<ul style="list-style-type: none"> <li>• (DO) Network defense capabilities that convince such adversaries that their attacks on US computer-based networks will likely fail could play an important role in the success of deterrence operations.</li> <li>• (SST&amp;R) Protect and secure critical national and regional infrastructure, natural resources, and strategically important institutions, e.g., government buildings, religious sites, courthouses, communications needed to support SSTR efforts.</li> <li>• (IW) An effective joint force projection and sustainment system must include data about friendly and adversary forces, as well as other joint, IA, and multi-national military and civilian partners and enablers to provide a complete picture of the operational environment for IW.</li> <li>• (MCO) A critical element of deterrence is maintaining capable and rapidly deployable military</li> </ul>						

Air Force Space Command Functional Concept for Cyberspace Operations

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<p>forces and, when necessary, demonstrating the will to resolve conflicts decisively on favorable terms. This will require forces to operate in and from the global commons (space, international waters and airspace, and cyberspace) and effectively project and sustain forces in distant environments where adversaries may seek to deny us access.</p> <ul style="list-style-type: none"> <li>• (MCO) The joint force protects data, information and knowledge from exploitation through, e.g., multilevel security policies and procedures, OPSEC, computer network defense, system hardening, and deception.</li> <li>• (HD&amp;CS) Cyber attacks prevented from affecting the ability to deploy, employ, and sustain forces.</li> </ul>						
<b>Cyberspace Defense</b>						
<b>Passive Defense</b>						
<ul style="list-style-type: none"> <li>• (HD&amp;CS) Mutual sharing and collaboration of communication, control and computer information to deter threats to the DIB.</li> <li>• (DO) Passive defenses complement active defenses, reducing the effectiveness of attacks that active defenses fail to defeat. They consist of measures taken to reduce the probability of (and to minimize the effects of) damage caused by hostile action.</li> <li>• (DO) The increasingly net-centric joint force of the 21<sup>st</sup> Century will capitalize on passive defense achieved through widely dispersed forces.</li> <li>• (DO) By reducing US vulnerability to a wide range of asymmetric attacks, active and passive defenses increase adversaries' perceived probability of incurring costs from counterstrikes on key assets.</li> <li>• (HD&amp;CS) Homeland security and homeland defense are focused on active and passive prevention and deterrence of attacks.</li> <li>• (HD&amp;CS) A layered approach arrays defenses in depth so that the JFC can trade space for time in order to characterize and engage the adversary with the most appropriate instrument. Layered defenses provide more options and a greater likelihood of success than non-layered approaches.</li> <li>• (SST&amp;R) This protection will involve a mix of preventive offensive operations noted above, combined with a variety of active and passive defense measures, including the establishment of protected areas (green zones), use of special security details, and specialized sniper and counter-sniper operations.</li> </ul>						
<b>Defense Counter Cyberspace</b>						
<ul style="list-style-type: none"> <li>• (CS) Counter virtual domain access denial efforts, the United States must have redundant systems in place, restore access by using commercial resources, use alternative paths, level the playing field by denying competitor or adversary access, and disclose what the competitor or adversary is doing.</li> <li>• (CS) JFC must be able to successfully respond to adversary activities to use the virtual domain to impede the accomplishment of the combatant command's security cooperation mission.</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<ul style="list-style-type: none"> <li>• (DO) Defining characteristic of Global Strike will be its unique blend of high-end and low-end military capabilities.</li> <li>• (DO) Information operations such as cyberspace warfare also undermine adversary decision makers' confidence in their ability to use force to their advantage. For example, network defense capabilities that convince such adversaries that their attacks on US computer-based networks will likely fail could play an important role in the success of deterrence operations.</li> <li>• (DO) Our efforts must also seek to identify the adversary's potential attack means (which must be defeated or countered to deny the benefits the adversary seeks) and the most appropriate targets for attack (to impose relevant costs).</li> <li>• (SST&amp;R) Case of the beleaguered fragile government, noted above, the armed opposition may take the form of an insurgency. In such cases, the SSTR operation is called a counterinsurgency operation.</li> <li>• (SST&amp;R) The interagency coordination group would maintain communications between the lower level interagency provincial teams and the senior US representative in theater, thus helping channel information upward and guidance downward to the teams operating at the province level.</li> <li>• (SST&amp;R) When establishing a secure environment in the face of anarchy or armed opposition, US and coalition military forces will conduct offensive and defensive air and land operations in a targeted, measured and highly discriminate manner.</li> <li>• (SST&amp;R) In some cases, the opposition may take the form of an armed insurgency, which employs terrorism as one of its primary means of attack. While the joint force must map, neutralize, and eliminate these terrorist networks, it must use measured and discriminate force in doing so.</li> <li>• (SST&amp;R) Joint force locating and destroying organized armed resistance, those responsible for securing key objectives will be more deliberate in their operations, relying less on firepower and more on other capabilities, including those resident outside the military arm of the unified action SSTR efforts.</li> <li>• (IW) Conduct information operations (operations security, information security, military deception, PSYOP, electronic warfare, computer network attack and defense; and physical destruction) in support of IW campaign objectives.</li> <li>• (IW) These insurgent groups will be masters of network centric warfare, but their networks will include tribal, communal, social, and cultural nets as well as electronic ones. They will exploit the internet and cyberspace for communications, propaganda, funding, recruiting, and training. They will function more like a tribal group, crime syndicate, or extended family than like a military or paramilitary organization.</li> <li>• (IW) The US military must provide the JFC with an effective joint force projection and sustainment system that is tailorable, survivable, and responsive to joint force requirements when engaged in IW operations.</li> <li>• (MCO) The current National Defense Strategy is to contend with security challenges through an active, layered defense of the Nation.</li> <li>• (MCO) A critical element of deterrence is maintaining capable and rapidly deployable military</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<p>forces and, when necessary, demonstrating the will to resolve conflicts decisively on favorable terms. This will require forces to operate in and from the global commons (space, international waters and airspace, and cyberspace) and effectively project and sustain forces in distant environments where adversaries may seek to deny us access.</p> <ul style="list-style-type: none"> <li>• (MCO) Conflict may continue using such means as terrorism, insurgency, economic disruptions, cyber war, political actions or a number of acts of civil disobedience.</li> <li>• (MCO) The JFC applies operational art and employs forces and their robust capabilities to achieve various operational-level objectives and associated effects that shatter the enemy's plans and dispositions and preclude his ability to militarily adapt, recover, and reconstitute.</li> <li>• (MCO) Commanders gain and maintain the advantage in the information environment by employing integrated nonkinetic and kinetic methods as necessary.</li> <li>• (MCO) In the early stages of conflict, the adversary is likely to possess the initiative in the information environment. To wrest the initiative from the adversary, a comprehensive set of offensive and defensive actions must occur.</li> <li>• (MCO) Commanders have access to robust and persistent ISR, myriad platform sensors, and the supporting net-centric operational environment to assist in this assessment, including the broader implications associated with the contributions IO make in achieving dominant effects.</li> <li>• (HD&amp;CS) Effective HD&amp;CS operations require an active, externally focused defense conducted in depth by layering integrated military, interagency, and multi-national partner capabilities beginning at the source of the threat.</li> <li>• (HD&amp;CS) Specific capabilities required for deterrence operations will vary significantly from adversary to adversary, but include force projection, active and passive defenses, global strike, and strategic communication and information operations.</li> <li>• (HD&amp;CS) Cyber defensive action in the forward regions and/or approaches to prevent an attack on the Homeland.</li> <li>• (HD&amp;CS) Shared information with theater security partners to permit preemptive actions.</li> <li>• (HD&amp;CS) Successful detection, accurate identification, and timely response to physical and cyber threats.</li> <li>• (HD&amp;CS) Capability: Detect, deter, prevent, or if necessary defeat physical and cyber threats to DoD assets in the Homeland.</li> </ul>						
<b>Cyberspace Force Application</b>						
<b>Offensive Counter Cyberspace</b>						
<ul style="list-style-type: none"> <li>• (CS) The JFC must expand efforts to detect, deter, and mitigate hostile actions by adversaries in the virtual domain. Both offensive and defensive capabilities (lethal and non-lethal) are necessary.</li> <li>• (DO) Conduct cyberspace warfare to sabotage [e.g., discredit financial data] systems associated with adversary X's WMD acquisition activities and undermine their support relationships with other third-party actors. (Denying benefits).</li> <li>• (DO) Our efforts must also seek to identify the adversary's potential attack means (which</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<p>must be defeated or countered to deny the benefits the adversary seeks) and the most appropriate targets for attack (to impose relevant costs).</p> <ul style="list-style-type: none"> <li>• (SST&amp;R) The interagency coordination group would maintain communications between the lower level interagency provincial teams and the senior US representative in theater, thus helping channel information upward and guidance downward to the teams operating at the province level.</li> <li>• (SST&amp;R) When establishing a secure environment in the face of anarchy or armed opposition, US and coalition military forces will conduct offensive and defensive air and land operations in a targeted, measured and highly discriminate manner.</li> <li>• (SST&amp;R) Joint force locating and destroying organized armed resistance, those responsible for securing key objectives will be more deliberate in their operations, relying less on firepower and more on other capabilities, including those resident outside the military arm of the unified action SSTR efforts.</li> <li>• (IW) Conduct information operations (operations security, information security, military deception, PSYOP, electronic warfare, computer network attack and defense; and physical destruction) in support of IW campaign objectives.</li> <li>• (IW) Intelligence collection operations. The use of sensors, including human assets, to detect and monitor both physical and non-physical objects and events in all domains (i.e., physical – maritime, air, space, and land; virtual – cyber and information; human – social, moral, and cognitive). Observation and collection include the gathering of pertinent environmental factors that can influence operations throughout the domains.</li> <li>• (IW) These insurgent groups will be masters of network centric warfare, but their networks will include tribal, communal, social, and cultural nets as well as electronic ones. They will exploit the internet and cyberspace for communications, propaganda, funding, recruiting, and training. They will function more like a tribal group, crime syndicate, or extended family than like a military or paramilitary organization.</li> <li>• (IW) Interdict insurgent/terrorist network LOCs (ground, maritime, air, finance, cyber).</li> <li>• (IW) An effective joint force projection and sustainment system must include data about friendly and adversary forces, as well as other joint, IA, and multi-national military and civilian partners and enablers to provide a complete picture of the operational environment for IW.</li> <li>• (MCO) A critical element of deterrence is maintaining capable and rapidly deployable military forces and, when necessary, demonstrating the will to resolve conflicts decisively on favorable terms. This will require forces to operate in and from the global commons (space, international waters and airspace, and cyberspace) and effectively project and sustain forces in distant environments where adversaries may seek to deny us access.</li> <li>• (MCO) The JFC applies operational art and employs forces and their robust capabilities to achieve various operational-level objectives and associated effects that shatter the enemy's plans and dispositions and preclude his ability to militarily adapt, recover, and reconstitute.</li> <li>• (MCO) Commanders gain and maintain the advantage in the information environment by employing integrated nonkinetic and kinetic methods as necessary.</li> <li>• (MCO) In the early stages of conflict, the adversary is likely to possess the initiative in the</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<p>information environment. To wrest the initiative from the adversary, a comprehensive set of offensive and defensive actions must occur.</p> <ul style="list-style-type: none"> <li>• (MCO) Early understanding of the adversary, his likely intentions and anticipated actions gives the JFC time, albeit limited, to take either preventive or preemptive actions to nullify the enemy's desired effects.</li> <li>• (MCO) Principally, the JFC invests his time and other finite resources to rapidly determine enemy centers of gravity, intentions, capabilities, vulnerabilities, and associated decisive points through robust ISR coupled with information fusion and information exploitation.</li> <li>• (MCO) Commanders have access to robust and persistent ISR, myriad platform sensors, and the supporting net-centric operational environment to assist in this assessment, including the broader implications associated with the contributions IO make in achieving dominant effects.</li> <li>• (HD&amp;CS) The most dangerous circumstance for the US will be situations where DoD is confronted with multiple challenges simultaneously. The technical advances of hostile state and non-state actors, the proliferation and diffusion of key technologies, and the continued advancement of weapons and delivery systems will provide destructive mechanisms and the ability to deliver them to an increasing number of adversaries who will continue to threaten US territory, population, and critical infrastructure.</li> <li>• (HD&amp;CS) Leveraged computer networks to help defeat an adversary in the forward regions and/or approaches.</li> <li>• (HD&amp;CS) Detect, deter, prevent, or if necessary defeat physical and cyber threats to DoD assets in the Homeland.</li> </ul>						
<b>Global Reach and Access</b>						
<ul style="list-style-type: none"> <li>• (DO) Advanced cyberspace warfare capabilities, capabilities to disable space systems, and electromagnetic pulse weapons could all provide adversaries means of undermining potentially decisive US advantages.</li> <li>• (DO) Potentially urgent employment timelines, Global Strike will primarily rely upon long-range, high-speed, and kinetic (advanced conventional and nuclear) and non-kinetic effects, unmanned systems, cyber systems, and/or small numbers of special operations forces employed over extended distances.</li> <li>• (DO) Conduct cyberspace warfare to sabotage (e.g., discredit financial data) systems associated with Adversary X's WMD acquisition activities and undermine their support relationships with other third-party actors. (Denying benefits.)</li> <li>• (SST&amp;R) In some cases, the opposition may take the form of an armed insurgency, which employs terrorism as one of its primary means of attack. While the joint force must map, neutralize, and eliminate these terrorist networks, it must use measured and discriminate force in doing so.</li> <li>• (SST&amp;R) Joint force locating and destroying organized armed resistance, those responsible for securing key objectives will be more deliberate in their operations, relying less on firepower and more on other capabilities, including those resident outside the military arm of the unified action SSTR efforts.</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<ul style="list-style-type: none"> <li>• (IW) Conduct information operations (operations security, information security, military deception, PSYOP, electronic warfare, computer network attack and defense; and physical destruction) in support of IW campaign objectives.</li> <li>• (IW) These insurgent groups will be masters of network centric warfare, but their networks will include tribal, communal, social, and cultural nets as well as electronic ones. They will exploit the internet and cyberspace for communications, propaganda, funding, recruiting, and training. They will function more like a tribal group, crime syndicate, or extended family than like a military or paramilitary organization.</li> <li>• (IW) Intelligence collection operations. The use of sensors, including human assets, to detect and monitor both physical and non-physical objects and events in all domains (i.e., physical – maritime, air, space, and land; virtual – cyber and information; human – social, moral, and cognitive). Observation and collection include the gathering of pertinent environmental factors that can influence operations throughout the domains.</li> <li>• (IW) These insurgent groups will be masters of network centric warfare, but their networks will include tribal, communal, social, and cultural nets as well as electronic ones. They will exploit the internet and cyberspace for communications, propaganda, funding, recruiting, and training. They will function more like a tribal group, crime syndicate, or extended family than like a military or paramilitary organization.</li> <li>• (IW) Interdict insurgent/terrorist network LOCs (ground, maritime, air, finance, cyber).</li> <li>• (MCO) A critical element of deterrence is maintaining capable and rapidly deployable military forces and, when necessary, demonstrating the will to resolve conflicts decisively on favorable terms. This will require forces to operate in and from the global commons (space, international waters and airspace, and cyberspace) and effectively project and sustain forces in distant environments where adversaries may seek to deny us access.</li> <li>• (MCO) Seizing the initiative or advantage allows more persistent application of air, ground, maritime, space, cyber, and special operations to occur as planned.</li> <li>• (MCO) As the JFC gains operational access and initiative, he aims to dominate the enemy in all domains and dimensions.</li> <li>• (MCO) The joint force protects data, information, and knowledge from exploitation through, for example, multilevel security policies and procedures, OPSEC, computer network defense, system hardening, and deception.</li> <li>• (HD&amp;CS) Detect, deter, prevent, or if necessary defeat physical and cyber threats to DoD assets in the Homeland.</li> </ul>						
<b>Cyberspace Cross Cutting Capabilities</b>						
<b>Intelligence, Surveillance, and Reconnaissance</b>						
<ul style="list-style-type: none"> <li>• (CS) The ability to acquire, analyze, produce, and disseminate (across the joint force as well as with interagency partners) all-source intelligence on the current situation in a particular area.</li> <li>• (DO) ISR efforts must be persistent across time, scalable from the global to local level,</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<p>seamless across key geographic regions, shared across US government and multinational partners, and optimized to leverage the full spectrum of traditional and not-traditional collection capabilities within and beyond DoD.</p> <ul style="list-style-type: none"> <li>• (DO) However, considerable insight into the critical content of adversary decision calculations can be developed through dedicated analytical effort and intelligence collection.</li> <li>• (SST&amp;R) The ability to conduct persistent surveillance of critical enemy activities in difficult and denied areas by using sensors to capture timely, relevant, and interoperable source data.</li> <li>• (IW) Persistent global intelligence operations will play a decisive part of any IW campaign.</li> <li>• (MCO) Commanders have access to robust and persistent ISR, myriad platform sensors, and the supporting net-centric operational environment to assist in this assessment, ...</li> <li>• (MCO) Reliable and actionable intelligence coupled with accurate targeting is essential.</li> <li>• (HD&amp;CS) Develop and maintain SA and shared understanding throughout the HD&amp;CS/CS/emergency preparation (EP) environments.</li> <li>• (HD&amp;CS) A net-centric joint force is able to maintain an accurate presentation of the operational environment built through the integration of ISR, blue force SA, geospatial mapping, and related database elements.</li> <li>• (HD&amp;CS) Superior decision making involves working at the leading edge of visionary, predictive intelligence fusion and analysis; staying ahead of adaptive, evolving threats; and facilitating information sharing with partner organizations.</li> </ul>						
<b>Situational Awareness</b>	✔	✔		✔	✔	✔
<ul style="list-style-type: none"> <li>• (HD&amp;CS) Develop and maintain SA and shared understanding throughout the HD&amp;CS/CS/EP environments.</li> <li>• (HD&amp;CS) A net-centric joint force is able to maintain an accurate presentation of the operational environment built through the integration of ISR, blue force SA, geospatial mapping, and related database elements.</li> <li>• (HD&amp;CS) Based on common real-time SA and a clear understanding of SecDef directions, strategic objectives, and commander's intent, a decentralized Joint Force can conduct operations at lower echelons, thereby allowing greater autonomy and freedom of action.</li> <li>• (HD&amp;CS) Hostile space and infrastructure activity located and tracked.</li> <li>• (MCO) To achieve this high level of SA, the joint force exploits myriad technical sensors, artificial intelligence, high-altitude long-loiter technologies, and other intelligence collection assets combined with increased computer power to assist leaders in a collaborative "intelligence" environment.</li> <li>• (CS) Activities provide pre-crisis SA, set the foundation for operational access, and develop the relationships and organizational precursors that enable effective partnerships in times of crisis.</li> <li>• (CS) These operations seek to mitigate extremism, deny sanctuary to terrorists, enhance SA, and improve security by stemming the proliferation of WMD.</li> <li>• (DO) Direct capabilities required for deterrence include the ability to carry out: force</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<p>projection operations, including the capability to decisively defeat regional aggression; kinetic and non-kinetic global strike operations. All of these efforts are enabled by global situational awareness, command and control, forward presence, security cooperation and military integration, plus deterrence assessment and experimentation.</p> <ul style="list-style-type: none"> <li>• (DO) The ability to translate foreign language open source media and web-based chatter, as well as concealed information (electronic or hardcopy), in near-real time is imperative for improving US capabilities to assess the decision making of both state and non-state adversaries.</li> <li>• (DO) Global SA of adversaries' perceptions identifies the key benefits adversaries seek to gain from courses of action we intend to deter.</li> <li>• (IW) Operations provides timely situational and target awareness in an appropriate form and by any suitable means to the joint force, supporting commands, and agencies. It ensures that the intelligence is understood and considered by the commanders and agency directors.</li> </ul>						
<b>Command and Control</b>	✔	✔	✔	✔	✔	✔
<ul style="list-style-type: none"> <li>• (DO) All military capabilities supporting deterrence operations rely on robust, reliable, secure, survivable, timely, unambiguous, and sustainable DoD-wide net-centric environment to enable command and control.</li> <li>• (DO) In addition to physical net-centric C2 systems, today's organizational C2 constructs may prove inadequate for the Joint Force of 2025.</li> <li>• (DO) Without robust, reliable, secure, survivable, timely, unambiguous, and sustainable net-centric systems supporting C2 capabilities, an adversary might perceive a decisive asymmetric advantage in launching a surprise attack.</li> <li>• (HD&amp;CS) To ensure DoD can meet its responsibilities for HD&amp;CS, CS, and EP, the JFC, leveraging operational environment awareness, develops multiple courses of action, recommends the best course of action, and directs force employment using the NCOE that facilitates rapid command decision making and information sharing with all applicable mission partners.</li> <li>• (HD&amp;CS) Prevent cyber attacks from affecting the ability to deploy, employ, and sustain forces.</li> <li>• (IW) In the future, combatant commanders will have alternative C2 mechanisms for conducting and supporting IW when a JTF is not required to conduct large-scale combat operations.</li> <li>• (MCO) Disrupt enemy ability to C2 his forces.</li> <li>• (MCO) The types of missions involved include global operations such as operations against terrorist networks, space operations, integrated global strike by both kinetic and non-kinetic means, global missile warning, and ISR support.</li> <li>• (MCO) An intelligent enemy understands that to survive the onslaught of US military warfighting capabilities and avoid decisive defeat, he must disperse, hide, preserve his strength, keep his C2 apparatus elusive.</li> <li>• (CS) A shared appreciation of the situation supported by common information to enable rapid</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<p>collaborative joint engagement, maneuver, and support.</p> <ul style="list-style-type: none"> <li>• (CS) The concept’s capability for active interaction with host nation security organizations in the region is largely oriented toward building partnerships. These partnerships require the establishment and cultivation of relationships built on trust.</li> <li>• (SST&amp;R) All domains and the monitoring of execution, assessment of effects, adaptation of operations, application of appropriate joint command and control, management of focused logistics, and force management that allows for successful SSTR transitions.</li> </ul>						
<b>Mission Assurance</b>	✓	✓	✓		✓	✓
<ul style="list-style-type: none"> <li>• (DO) US deterrence strategy needs to take these potential US vulnerabilities fully into account, eliminating them where feasible, and compensating for them when necessary.</li> <li>• (DO) Having the capability to sustain continuity of effective military or economic operations in the midst or wake of a major enemy attack on the US Homeland.</li> <li>• (SST&amp;R) In order to establish a sufficiently secure environment for effective civilian-led reconstruction operations to take place, the joint force must do more than just defeat organized military resistance.</li> <li>• (SST&amp;R) Conduct operations to secure in stride: population centers, essential national and regional resources, and key infrastructure, including critical transportation and communications nodes, and key medical, water, sanitation, and power generation facilities.</li> <li>• (SST&amp;R) The rapid reconstruction of critical infrastructure, including key transportation systems and telecommunications networks, and the restoration of essential public services must be accomplished with an eye toward the creation of a durable foundation that supports a wide range of longer term efforts to develop a diversified, modern economy in the host nation that is effectively integrated into the global economy.</li> <li>• (MCO) A critical element of deterrence is maintaining capable and rapidly deployable military forces and, when necessary, demonstrating the will to resolve conflicts decisively on favorable terms. This will require forces to operate in and from the global commons (space, international waters and airspace, and cyberspace) and effectively project and sustain forces in distant environments where adversaries may seek to deny us access.</li> <li>• (MCO) Seizing the initiative or advantage allows more persistent application of air, ground, maritime, space, cyber, and special operations to occur as planned.</li> <li>• (MCO) The joint force protects data, information, and knowledge from exploitation through, for example, multilevel security policies and procedures, OPSEC, computer network defense, system hardening, and deception.</li> <li>• (HD&amp;CS) The most dangerous circumstance for the US will be situations where DoD is confronted with multiple challenges simultaneously. The technical advances of hostile state and non-state actors, the proliferation and diffusion of key technologies, and the continued advancement of weapons and delivery systems will provide destructive mechanisms and the ability to deliver them to an increasing number of adversaries who will continue to threaten US territory, population, and critical infrastructure.</li> <li>• (HD&amp;CS) A secure physical and cyber environment for DoD assets in the Homeland.</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<ul style="list-style-type: none"> <li>• (HD&amp;CS) Integrated command, control, and computer systems to enhance preemptive actions by US and coalition forces.</li> <li>• (HD&amp;CS) Project power to defend the Homeland. Disruptions to US space assets, either by direct attack, jamming, or cyber attack, could reduce the joint force’s ability to project power or degrade certain enabling capabilities.</li> <li>• (HD&amp;CS) Detect, deter, prevent, or if necessary defeat physical and cyber threats to DoD assets in the Homeland.</li> <li>• (CS) JFC must support activities by the host nation or larger multinational community to detect, deter, and mitigate Military Contribution To Cooperative Security.</li> <li>• (CS) Interact with HNs to develop solutions to protect and safeguard critical resources and infrastructure.</li> <li>• (SST&amp;R) Conduct operations to secure in stride: population centers, essential national and regional resources, and key infrastructure, including critical transportation and communications nodes, and key medical, water, sanitation, and power generation facilities.</li> <li>• (SST&amp;R) SSTR operations, especially within a contested, hostile environment, efforts to reconstitute critical infrastructure and restore essential services will primarily be a military-led activity.</li> <li>• (SST&amp;R) The rapid reconstruction of critical infrastructure, including key transportation systems and telecommunications networks, and the restoration of essential public services must be accomplished with an eye toward the creation of a durable foundation that supports a wide range of longer term efforts to develop a diversified, modern economy in the host nation that is effectively integrated into the global economy.</li> <li>• (MCO) A critical element of deterrence is maintaining capable and rapidly deployable military forces and, when necessary, demonstrating the will to resolve conflicts decisively on favorable terms. This will require forces to operate in and from the global commons (space, international waters and airspace, and cyberspace) and effectively project and sustain forces in distant environments where adversaries may seek to deny us access.</li> <li>• (MCO) The US military must provide the supported JFC with a survivable, responsive, and adaptable force projection and distribution-based sustainment system. This enables the building and delivery of combat power at the right times and locations as determined by the supported JFC.</li> <li>• (HD&amp;CS) A secure physical and cyber environment for DoD assets in the Homeland.</li> <li>• (HD&amp;CS) Mutual sharing and collaboration of communication, control, and computer information to deter threats to the DIB.</li> </ul>						
<p><b>Support to Influence Operations</b></p>						
<ul style="list-style-type: none"> <li>• (CS) The CS priorities of the USG will be shaped by several fundamental characteristics of the future global operating environment that directly affect America’s ability to influence world affairs.</li> <li>• (DO) Weapons that are reliable, accurate, and flexible will retain a qualitative advantage in their ability to demonstrate US resolve on the world stage.</li> </ul>						

Joint Operating Concept	Cooperative Security (CS)	Deterrence Ops (DO)	Stabilization, Security, Transition, and Reconstitution (SST&R)	Irregular warfare (IW)	Major Combat Operations (MCO)	Homeland Defense & Civil Support (HD&CS)
<ul style="list-style-type: none"> <li>• (DO) Effectively integrating offensive and defensive operations can powerfully influence an adversary's perception.</li> <li>• (SST&amp;R) Since SST&amp;R operations are largely won or lost in the political and information domains, global communications and information dissemination are vital factors.</li> <li>• (IW) Conduct information operations (operations security, information security, military deception, PSYOP, electronic warfare, computer network attack and defense; and physical destruction) in support of IW campaign objectives.</li> <li>• (MCO) A critical element of deterrence is maintaining capable and rapidly deployable military forces and, when necessary, demonstrating the will to resolve conflicts decisively on favorable terms. This will require forces to operate in and from the global commons (space, international waters and airspace, and cyberspace) and effectively project and sustain forces in distant environments where adversaries may seek to deny us access.</li> <li>• (HD&amp;CS) DoD will keep the American public apprised of HD and CS actions by its contribution to the USG strategic communication campaign through IO related capabilities of public affairs, civil military operations, and defense support to public diplomacy.</li> </ul>						

THIS PAGE INTENTIONALLY LEFT BLANK