



THE WAY AHEAD FOR CYBERSPACE OPERATIONS: A JCIDS ANALYSIS

GRADUATE RESEARCH PROJECT

Tim Treat, Major, USAF
AFIT/IC4/ENG/07-08

**DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY**

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

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

AFIT/IC4/ENG/07-08

**AN ANALYSIS OF HOW THE JOINT CAPABILITIES INTEGRATION AND
DEVELOPMENT SYSTEM (JCIDS) STRENGTHENS
THE WAY AHEAD FOR CYBERSPACE OPERATIONS**

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of C4I Systems

Timothy J. Treat

Major, USAF

June 2007

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

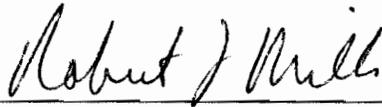
AFIT/IC4/ENG/07-08

THE WAY AHEAD FOR CYBERSPACE OPERATIONS: A JCIDS ANALYSIS

Timothy J. Treat

Major, USAF

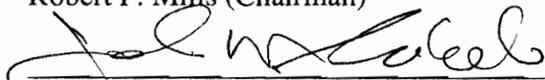
Approved:



Robert F. Mills (Chairman)

6 JUN 07

Date



John M. Colombi, Lt Col, USAF (Member)

6 JUN 07

Date

Abstract

As the mission of the military becomes increasingly interdependent on machine-to-machine operations and interoperability, the need for cyberspace superiority becomes more and more critical for our military to dominate in all domains. To achieve cyberspace superiority, our military services must field fully joint cyberspace capabilities that are designed and acquired to operate in a joint environment. Joint Capabilities Integration Development System (JCIDS) analysis can facilitate a broad focus and military leaders must understand and mandate its use to field truly joint capabilities in cyberspace.

Acknowledgments

I would like to express my sincere appreciation to my faculty advisors, Dr Robert Mills and Lt Col John Colombi, for their guidance and support throughout this effort. Their insight and experience was greatly appreciated.

Timothy J. Treat

Table of Contents

	Page
Acknowledgments.....	v
Table of Contents.....	vii
List of Figures.....	ix
List of Tables.....	x
Abstract.....	v
I. Introduction.....	1
II. Explanation of JCIDS.....	2
Chapter Overview.....	2
Where JCIDS fits in Capabilities Development.....	2
Objectives of JCIDS.....	7
The Joint Capabilities Document (JCD).....	8
The Initial Capabilities Document (ICD).....	11
The Flexibility of JCD and ICD Relationships.....	12
Summary.....	13
III. The Need for an Integrated/Joint Approach in Cyberspace.....	14
A National Security Issue.....	14
The Cyberspace Definition.....	16
Integrated/Joint Approach.....	18
The Air Force and Cyberspace.....	19
Summary.....	22
IV. The Cyberspace Defense Example.....	23
Chapter Overview.....	23
The Cyberspace Defense JCD.....	24

The Cyberspace Defense ICD	32
Summary.....	37
V. Strengthening the Cyberspace Way Ahead.....	38
VI. Lessons Learned	40
Measure of Effectiveness (MOE).....	40
Team Makeup.....	40
Use of Scenarios	41
Analysis Pitfalls.....	41
Understand Combatant Commanders, Services, Agencies, etc roles/relationship.....	42
VII. Conclusion.....	43
Appendix A. Cyberspace Defense JCD.....	44
Appendix B. Cyberspace Defense ICD	101
Bibliography	170

List of Figures

	Page
Figure 1: Transformation from Bottom Up to Top Down Joint Acquisition.....	3
Figure 2: DoD Acquisition Philosophy Changes.....	4
Figure 3: JCIDS Relationship to DoD 5000	5
Figure 4: JCIDS Joint Architecture Emphasis	6
Figure 6: JCIDS Process	9
Figure 7: Linkage of FAA and FNA to JCIDS Process.....	10
Figure 8: JCIDS Analysis	11
Figure 9: JCIDS Document Relationships.....	12

List of Tables

	Page
Table 1: Cyberspace Defense Tasks with Associated INFOCATs and MOEs	30
Table 2: Cyberspace Defense Capability Gaps.....	32
Table 3: Cyberspace Defense Recommended Solution (Phased Approach)	36

I. Introduction

This paper documents how the JCIDS process can be used to strengthen the cyberspace way ahead. The JCIDS process is not just for joint staff officers, but can be used by all services to perform joint based analysis on missions. The vast complexity of cyberspace lends it to be probably the most challenging domain for joint operations and understanding. As leaders continue to shape the environment and move forward, the domain is consistently changing. This graduate research project provides reasons why properly using JCIDS and taking advantage of its joint focus will allow cyberspace leaders and staff officers to create a library of capabilities documents that can be modified to evolve with the cyberspace mission.

II. Explanation of JCIDS

Chapter Overview

The purpose of this chapter is to explain the relationship between JCIDS analysis and how the DoD develops and acquires capabilities. The chapter provides an understanding of how JCIDS works with the DoD 5000 process for acquisition as well as the Planning, Programming, Budgeting, and Execution (PPBE) process for funding. In effect, the JCIDS process has enabled the DoD to move from platform based acquisition to integrated capabilities based acquisition for fighting in asymmetric joint environments.

In addition, the chapter also highlights what the objectives of JCIDS are and introduces the documents that are developed during the JCIDS process. In the end, readers should have a better understanding of how cyberspace leaders and professionals can leverage the JCIDS process to be successful in:

- 1) understanding joint cyberspace tasks and activities
- 2) providing a defendable and credible set of prioritized capability gaps
- 3) providing a list of well thought out Measures Of Effectiveness (MOEs) to gauge future success
- 4) offering the best Doctrine, Organization, Training, Materiel, Leadership/Education, Personnel and Facilities (DOTMLPF) cyberspace solutions, from both near and long term perspectives

Where JCIDS fits in Capabilities Development

The evolution of technology and the focus to fight wars in a joint military environment has instigated a number of changes in how we nominate, fund, and acquire military capabilities. In the past, and for the most part today, military nomination, funding, and acquisition of military capabilities is handled by each individual service. The process has historically been very platform based where the leadership of each service knows the specific platforms required to

perform their respective missions. However, a significant push is being made to provide for a way where the DoD has the ability to acquire capabilities that suffice for all services rather than just a platform that is limited to one service's needs. To date, the platform based process has worked well and allowed the separate services to field capabilities that are essential to support the missions and requirements of combatant commanders, but the redundancy and inefficiencies in the service specific platform approach is being replaced by a more affordable capabilities based approach.

Figure 1, shows how JCIDS is transforming the way DoD acquires capabilities and weapon systems. The left hand side shows the traditional approach where the Requirements Generation System allowed each service to push up requirements that were stove piped and flavored toward how each service felt was the best way to build capabilities and platforms.

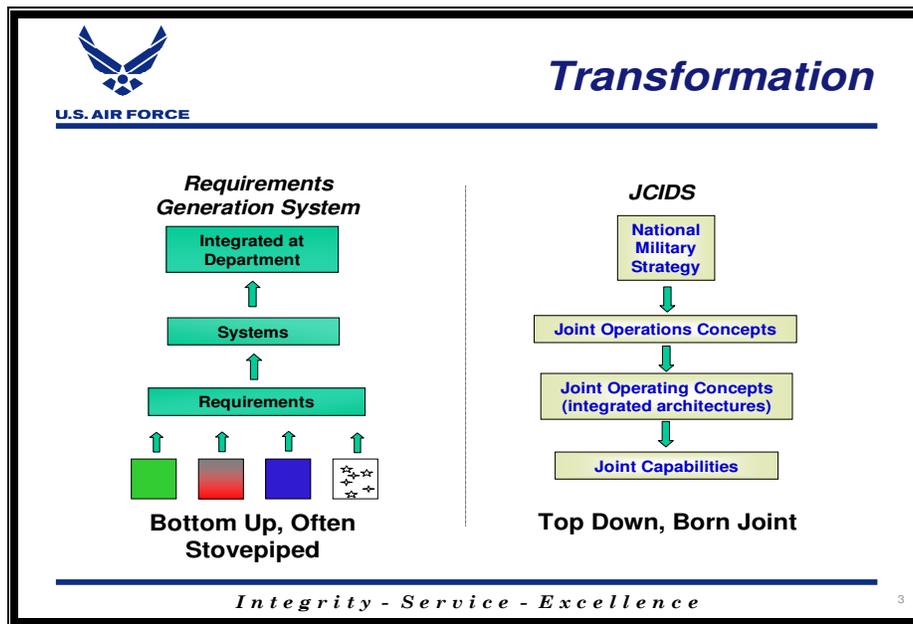


Figure 1: Transformation from Bottom Up to Top Down Joint Acquisition

This is unlike the right hand side of the figure where National Military Strategy, Joint Operating Concepts, and other overarching strategic documents drive the requirements for joint

capabilities. The transformed approach shows the initial national pedigree that is required for any joint capability before being funded and acquired.

There have been many drivers for the transformation. We fight in a joint environment. The cold war is over and our military is evolving. Technology is driving an asymmetric battlespace where traditional military doctrine breaks down. There is an increased shift from development of threat based requirement to capability based requirements to produce effects in the battlefield. The military's increased reliance on fighting as a joint force to support combatant commanders. The list of drivers is endless, not to mention how expensive the platform based acquisition approach has become. Ultimately, the DoD came to terms with the fact that the military needed to make some philosophical changes to how military capabilities are acquired.

Figure 2, is a diagram that shows how the DoD aligned three formerly independent processes in order to overhaul the acquisition process. Essentially, JCIDS was a key part to

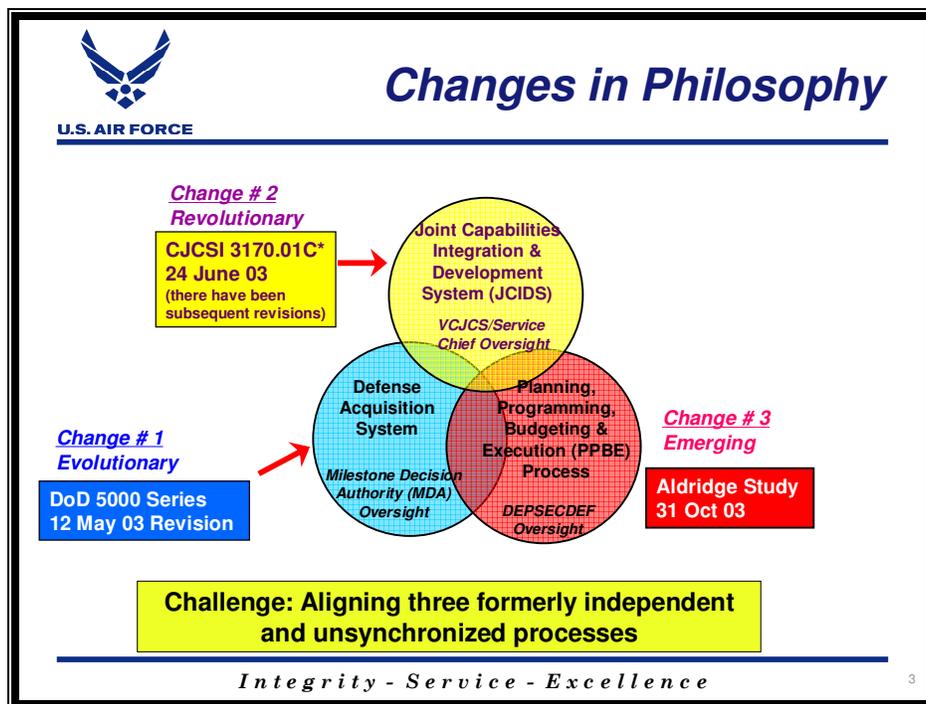


Figure 2: DoD Acquisition Philosophy Changes

bring the acquisition system (in blue) and the planning, programming, and budgeting system (in red) together to fund and acquire joint capabilities that are born joint from the start. This is different from the past where capabilities were first born by the service, then made to work in the joint environment. Now, the entire acquisition process is integrated to ensure that joint integrated capabilities are funded and fielded to support combatant commanders engaging enemies and protecting the homeland.

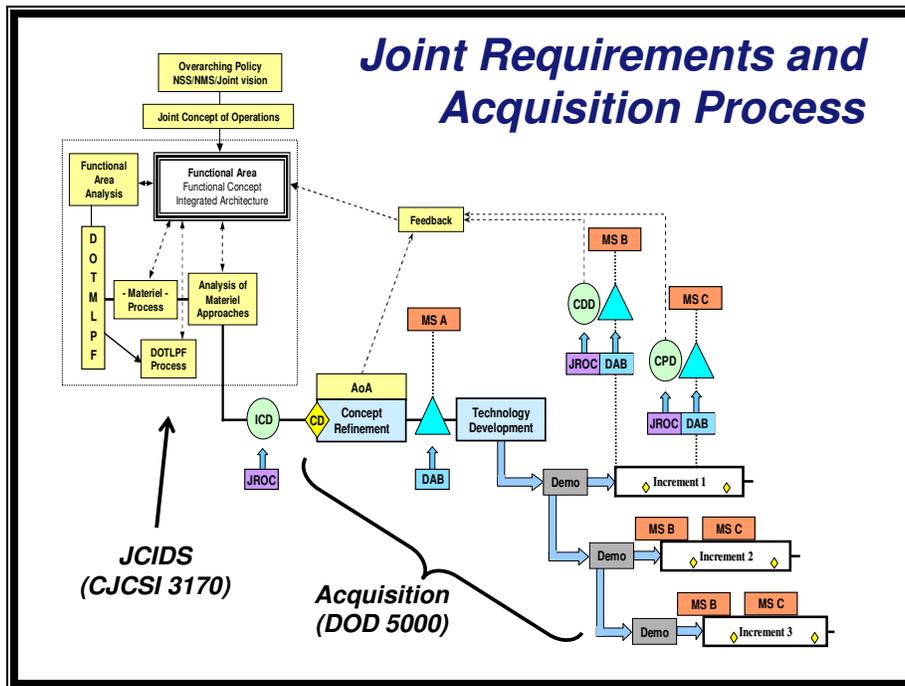


Figure 3: JCIDS Relationship to DoD 5000

The change in philosophy is extremely relevant. Figure 3 shows how the JCIDS and DoD 5000 processes work together. The JCIDS analysis process, which we'll discuss in more depth later, produces an Initial Capabilities Document (ICD) that is approved by the Joint Requirements Oversight Council (JROC) and feeds into the DoD 5000 acquisition process to be acquired by the services. The details of Figure 3 are not important for this paper, but the figure provides a glimpse at how complex both the JCIDS analysis and the DoD 5000 processes are.

Most importantly, the DoD 5000 process cannot get started without an approved ICD from the JROC. This ensures a joint born, top down capability is acquired.

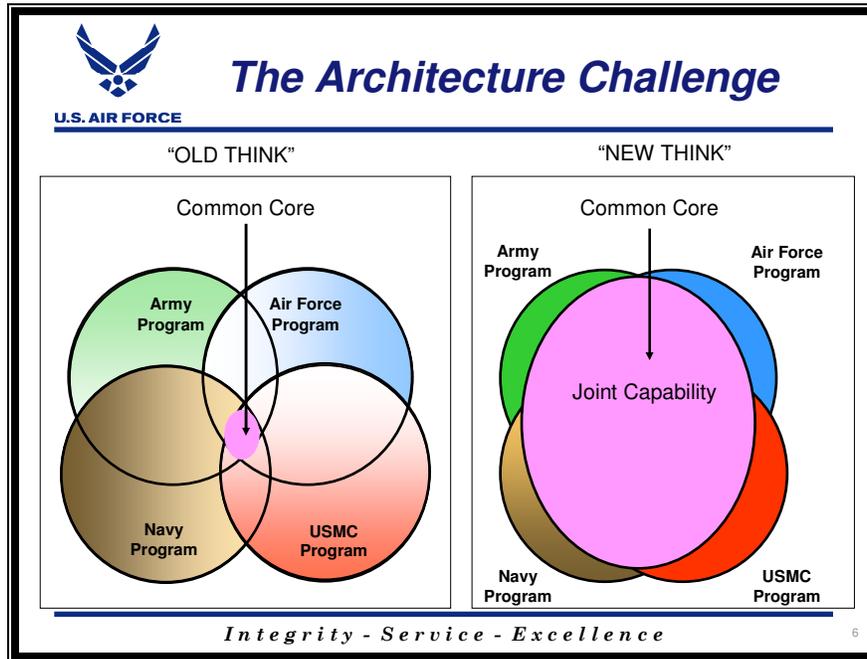


Figure 4: JCIDS Joint Architecture Emphasis

An important aspect of JCIDS is how the process helps focus acquisition toward integrated capabilities based on joint architecture. Figure 4 shows how the traditional bottom up, stove pipe approach on the left side of the diagram produced a very small cross section of joint architecture. In the past, the services have worked in a vacuum to build their respective architectures and then mold each others architectures to fit together. Now, the emphasis is to produce joint focused architecture for each service to fuse into. The JCIDS analysis enhances the services ability to fuse capabilities into joint focused architectures and drives the services to build less architecture independently.

With respect to cyberspace, the JCIDS process is probably the single most important enabler. Cyberspace is an extremely complex and broad environment. It crosses the boundaries

of all domains and the warfighting leverage the military realizes from operating in cyberspace is countered by the vast number of vulnerabilities that come with it. However, the JCIDS process provides an analysis framework to help build offensive and defensive cyberspace capabilities from a joint perspective. It also allows services to gain credibility through performing the analysis and showing the tasks that need to be performed and capability gaps inhibiting joint forces from successful execution and superiority in cyberspace.

The details for JCIDS are provided in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01E corresponding manual.

Objectives of JCIDS

The Air Force has primarily employed concept documents to advocate cyberspace and develop an operational framework. Using concept documents has done well to communicate the overall relationships and provide a conceptual understanding of the cyberspace focus. For example, the recent Draft Air Force Cyber Warfare concept document discusses the military challenges and includes the following desired end states:

- deter and prevent cyberspace attacks against vital US interests
- rapidly respond to attacks and reconstitute networks
- integrate cyber power into the full range of global and theater effects
- defeat adversaries operating through cyberspace
- freedom of action in cyberspace for US & Allied commanders
- persistent cyberspace situational awareness

The entire concept document including the end states provide a great pre-cursor for staff officers to perform JCIDS analysis. In fact, the JCIDS process is a tremendous help to provide further details of where the Air Force is going with respect to cyberspace and ensure the direction has a fully vetted and defensible joint flavor.

Ultimately, by putting the effort in upfront, Air Force cyberspace Subject Matter Experts (SMEs) can take advantage of the JCIDS objectives that seek to:

- enhance methodology to identify and describe capability gaps
- mandate broad review of capability proposals
- engage the acquisition community early
- better define non-materiel aspects of materiel solutions
- prioritize capability gaps and proposals
- improve coordination among services and agencies

In fact, all the objectives concentrate the JCIDS focus on capabilities based analysis. The objectives ensure the analysis is done from a joint perspective to help open communication lines for coordination between services and agencies. In addition, the process helps prioritization efforts, provides for early engagement with the acquisition community, and provides for an approach to better define non-materiel versus material aspects of solutions.

The objectives listed above ensure that the identified tasked and capability gaps derived from JCIDS analysis are well defined and have a joint focus. This perspective for analysis is growing ever increasingly important to provide credibility for funding and approval for joint integrated capabilities. With respect to the Air Force cyberspace way ahead, the objectives hint to a means where the vast challenges of cyberspace can be prioritized and addressed from a joint perspective.

The Joint Capabilities Document (JCD)

Overall a JCD is derived from a capabilities-based assessment that identifies and prioritizes what is important to the joint warfighter. In addition, it provides a means to evaluate future concepts and systems on how well they provide and deliver needed capabilities to combatant commanders, services, and agencies.

The focus of a JCD is on capability gaps derived from tasks identified through detailed analysis of national strategy, doctrine, Joint Functional Concepts (JFCs), Joint Operating Concepts (JOCs), Joint Integrating Concepts (JICs), the Universal Joint Task List (UJTL), etc. In addition, the JCD provides Measures Of Effectiveness (MOEs) that provide upfront direction on how the effectiveness of any solution should be measured.

Figure 6 provides a visual into how documents and concepts identified above fit together to feed the JCIDS process. The JCD is written during the assessment and analysis section of

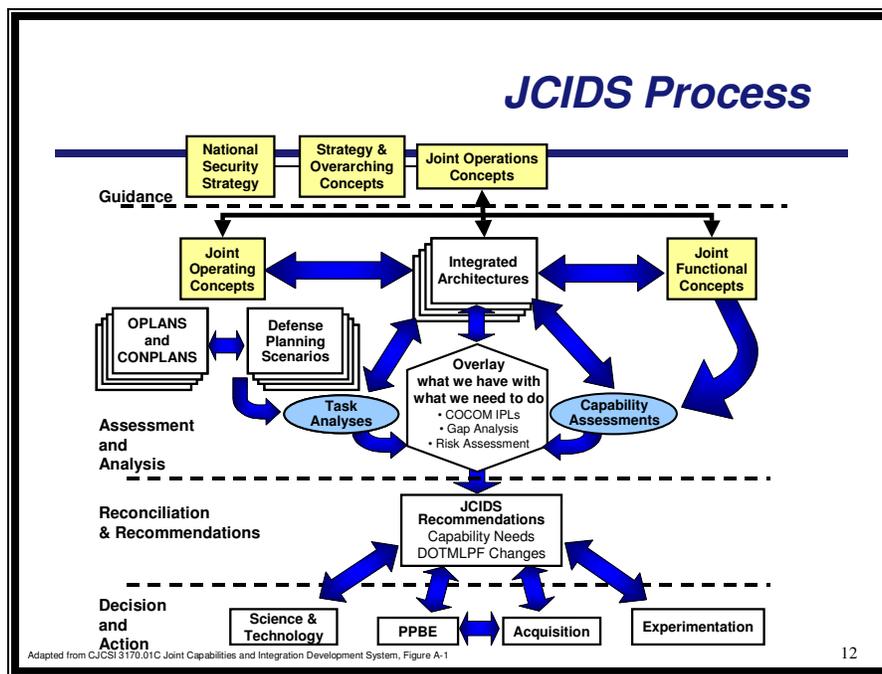


Figure 6: JCIDS Process

the figure. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01B, Enclosure D, provides the approved outline to follow when writing a JCD. The outline is used in Chapter IV for the Cyberspace Defense example and will be discussed at that time along with the example. Take note, that the current Draft Cyber Warfare Air Force Concept document would

be used along with all the guidance documentation identified at the top of the slide feeding the analysis.

In all, the JCD is broken down into a Functional Area Analysis (FAA) and a Functional Needs Analysis (FNA). Figure 7 is a build from the previous figure to show where the FAA and FNA fit in the overall analysis process. The figure highlights the fact that the FAA concentrates on task analysis, while the FNA concentrates on capabilities assessment. It is always good to remember the equation $JCD = FAA + FNA$ and keep in mind that the JCD is concentrating on required tasks and required capabilities to perform the tasks.

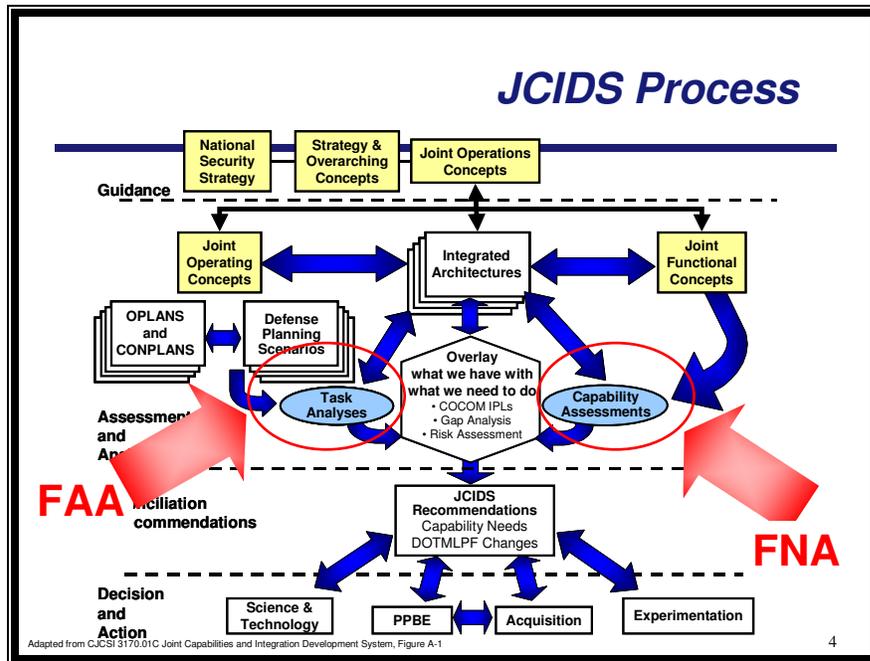


Figure 7: Linkage of FAA and FNA to JCIDS Process

In terms of order, the FAA is performed prior to the FNA mainly because it is important to gain a clear understanding of the tasks that need to be performed, and then analyze the capabilities required to perform the tasks. Given this, the next paragraphs will cover what an FAA is and be followed up by an overview of an FNA.

Figure 8 provides additional insight and specialized focus on JCIDS analysis. The figure shows that the FAA identifies tasks the warfighters need to perform and the FNA concentrates on capability gaps that inhibit the warfighters from successfully performing the tasks. In fact, tasks and capability gaps are exactly what a JCD is concerned about. The development of the JCD ultimately culminates in a thorough analysis that provides capabilities based assessment with respect to mission requirements for warfighting missions in domains like cyberspace. An example of a JCD analysis performed on cyberspace defense is provided in chapter IV.

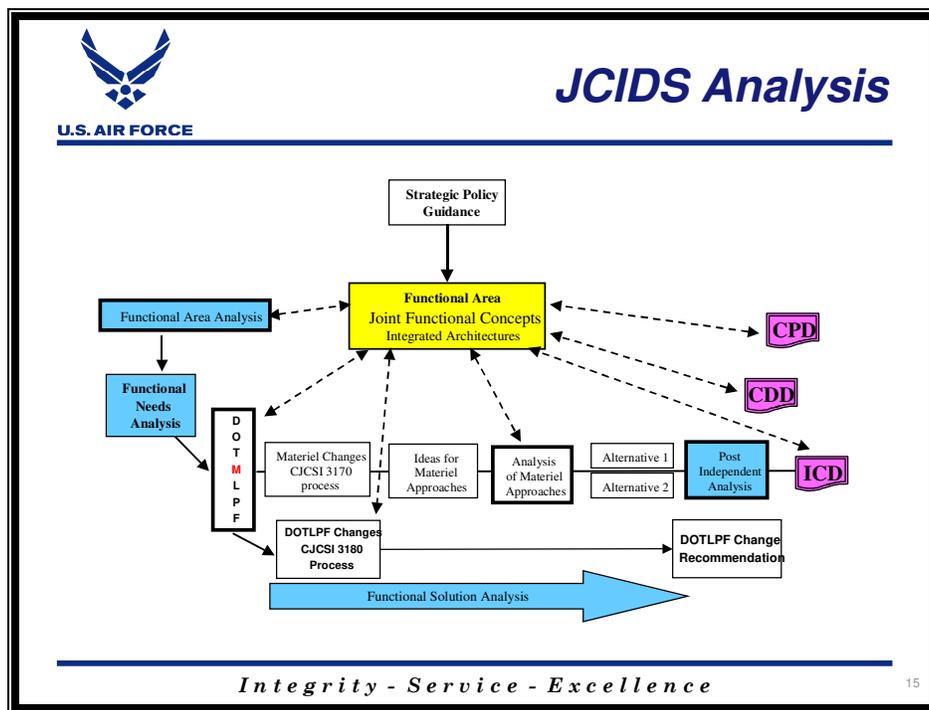


Figure 8: JCIDS Analysis

The Initial Capabilities Document (ICD)

Figure 8 also shows how the FAA and FNA of the JCD feed a Functional Solutions Analysis (FSA). The FSA is the main component of an ICD. A handy way to remember the components of the ICD is to remember the equation $ICD = JCD + FSA$. As figure 8 indicates,

the FSA performs an overall Doctrine, Organization, Training, Materiel, Leadership/Education, Personnel, and Facilities (DOTMLPF) review to materiel and non-materiel approaches and alternatives to effectively fill the capability gaps identified in the JCD. The alternatives and approaches can be new materiel/non-materiel recommendations and/or DOTMLPF change requests. An example of an ICD is provided in Chapter IV. In addition, as in the case of the JCD, The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01B, Enclosure E, provides the approved outline to follow when writing an ICD.

The Flexibility of JCD and ICD Relationships

One aspect of the JCIDS process is the flexibility how JCDs and ICDs can be interrelated. A single JCD can produce many ICDs if required and ICDs can be produced from more than one JCD.

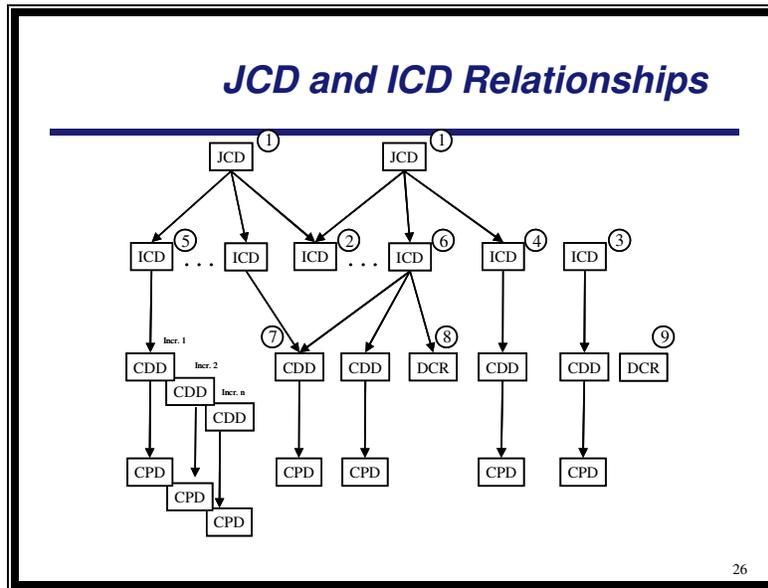


Figure 9: JCIDS Document Relationships

Figure 9 provides a visual example of the relationship. The figure also shows how the ICDs feed the Capability Development Document (CDD) and Capability Production Document

(CPD) that are part of the DoD 5000 process. Both the CDD and CPD are outside the scope of this graduate research project, but are included here to provide additional visualization of how the JCIDS process integrates into the DoD 5000 acquisition process.

Summary

The JCD and ICD are key components of the JCIDS process. The JCD and ICD work together to tell a story that helps prioritize and define capabilities important to joint warfighters. The documents do this through the result of a capabilities-based assessment that helps military leaders and personnel evaluate future systems in their ability to deliver the capabilities required by joint warfighters.

With respect to cyberspace, the JCIDS process is an important key for being successful in cyberspace and strengthen credibility for cyberspace capabilities. Since cyberspace crosses all domains and JCIDS provides for an integrated analysis of tasks versus capabilities to support joint warfighters, cyberspace leaders and visionaries should embrace the JCIDS process. As stated in the chapter overview, cyberspace leaders and professionals can leverage the JCIDS process to be successful in:

- 1) understanding joint cyberspace tasks and activities
- 2) providing a defensible and credible set of prioritized capability gaps
- 3) providing a list of well thought out measures of effectiveness to gauge future success
- 4) offering the best DOTMLPF cyberspace solutions, from both near and long term perspectives

III. The Need for an Integrated/Joint Approach in Cyberspace

A National Security Issue

Today, there is a significant amount of discussion by national leadership concerning the strategic need for the United States to possess cyberspace superiority. Given the proliferation of the internet, electromagnetic capabilities, and how technology has changed the world, it is easy to quickly derive why cyberspace dominance is so important to national security. Militarily, the cyberspace threat affects every service. Commercially, the cyberspace threat has been driven forward by creative peer competitors and terrorists who take advantage of cyberspace vulnerabilities. To this effect, the United States leadership has addressed the cyberspace threat in all of our National Strategic documents.

For instance, the 2006 Quadrennial Defense Review (QDR) included a new domain, cyberspace, to protect and defend along with air, land, maritime, and space. In addition, the National Defense Strategy written in 2005 also highlighted the increased priority of cyberspace by noting:

“Our ability to operate in and from the global commons—space, international waters and airspace, and cyberspace—is important.”

The National Defense Strategy goes on to clearly single out cyberspace as a “new theater of operations”. The strategy also links cyberspace with Information Operations and indicates that:

“Consequently, Information Operations (IO) is becoming a core military competency. Successful military operations depend on the ability to protect information infrastructure and data. Increased dependence on information networks creates new vulnerabilities that adversaries may seek to exploit. At that time, an adversary’s use of information networks and technologies creates opportunities for us to conduct discriminate offensive IO as well. Developing IO as a core military competency requires fundamental shifts in processes, policies, and culture.”

The fundamental shifts mentioned are significant to organize United States assets and operate securely in cyberspace. The shift is necessary to posture our military and federal organizations in order to synchronize operations to ensure our offensive and defensive cyberspace capabilities are lethal enough and effectively utilized.

The 2006 QDR increased the complexity of the domain by including the need to work with our International Allies and Partners in cyberspace. It directly calls out cyberspace as a multi-national priority along with Weapons of Mass Destruction (WMD) by stating:

“Concepts and constructs enabling unity of effort with more than 70 supporting nations under the Proliferation Security Initiative should be extended to domains other than WMD proliferation, including cyberspace, as a priority.”

The emphasis shows how important cyberspace is from a multi-national perspective and foreshadows how our national leadership will focus on multinational cyberspace operational efforts in the future. This makes sense given how the global economy is evolving and technologically advanced countries are becoming more and more reliant on each other.

The 2006 QDR goes further than just identifying cyberspace as a new domain. For instance, it explains that terrorists “exploit the Internet as a cyber-sanctuary, which enables the transfer of funds and the cross-training of geographically isolated cells.” The QDR also addresses some of our peer competitors and mentions the following about China:

“China is likely to continue making large investments in high-end asymmetric military capabilities, emphasizing electronic and cyber-warfare...for employment by the Chinese military and for global export.”

This is not just the Internet, the electronic capabilities China and other countries are creating utilizes the entire electromagnetic spectrum. The comment about producing the capabilities for

global export is chilling. A technology advanced nation providing electronic and cyber-warfare capabilities for global export clearly brings cyberspace dominance to the forefront.

Ultimately, our national leadership realizes the importance of operational superiority and security in cyberspace. The domain opens up many holes that can weaken our resolve and national security if not addressed. As a nation, we must develop an overall cyberspace strategy to include how the military integrates with agencies and departments to fight enemies abroad and secure our homeland internally. Cyberspace is more than a domain America utilizes to increase efficiency and improve processes; it is a strategic high ground for critical systems and infrastructure. The domain provides a medium where a cyberspace attack can directly impact homes and work places on US soil. It can be used to cripple a nation's ability to perform life sustaining functions and maintain stability. As we continue to press forward to enhance our lives and improve processes through technology, the cyberspace threat grows as an ever increasing national security issue.

The Cyberspace Definition

The emphasis by United States national leadership and the inclusion of cyberspace in national security documents has led to a constant discussion about the definition of the cyberspace domain. In 2006, the Joint Chiefs of Staff released the following definition for cyberspace:

“Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.”

The cyberspace definition describes an incredibly complex domain that crosses multiple organizations, agencies, and institutions. In addition, not all are military and federal. Within the

military, all services rely heavily on the domain and have different strengths and weaknesses with respect to operating in and protecting cyberspace. The strengths and weaknesses stem from the fact that there are fundamental differences in how the respective military services think about how to utilize cyberspace capabilities.

The realization that our military services disagree about cyberspace is not surprising, but rather expected. The services fundamentally work predominately in different domains. The Navy works predominately in the sea domain. The Army works predominately in land domain. The Air Force works predominately in the air and space domains. These different domains lead to different views on cyberspace because of the different ways each service organizes, trains, and equips to fight and support combatant commanders.

Our ability to dominate in cyberspace will depend on how well the DoD is able to press forward to develop joint operational doctrine and field capabilities for joint operational warfighters. The definition may be complex, but the even more complex issue is how our military uses cyberspace to achieve military objectives and at the same time secure cyberspace for our federal, state, local, and commercial use.

The point is the DoD has a mandate to gain and maintain cyberspace superiority. The JCIDS focus on joint tasks and capabilities is the best vehicle available to shape our forces for cyberspace domination in today's environment. It will take many years of successes and failures before we will get it right, but cyberspace is the most squishy, boundless, mind-bending operational domain yet and all the services will have to work more closely together than ever before to ensure success.

Integrated/Joint Approach

As our adversaries continue to build cyberspace capabilities to achieve strategic military objectives we will have to fundamentally shift our military assets along with civilian assets as a counter. The shifts must provide for fully integrated synchronization with respect to military operations in support of military objectives and military assistance to federal authorities and agencies when required.

This idea of a fundamental shift should not intimidate military professionals. It just means leaders and staff officers writing the way ahead for cyberspace will have to be more knowledgeable of joint operations/doctrine/organization as well as other services operations/doctrine/organization. And, more effort will have to be made by the services to train their leaders to understand how different services organize, train, and equip. The training doesn't have to include a high level of expertise, merely an understanding of the way different services do business. This in-turn ensures cyberspace leaders and subject matter experts better understand different perspectives where cyberspace is concerned.

This kind of joint focused training is already seen today through joint professional military training at the company grade officer level and above. In addition, all the services send officer and senior enlisted personnel to each other's graduate schools for advanced academic degrees. The inter-service activities and efforts back up the premise of this paper, and shows that we are headed the right direction for service-level subject matter experts to use JCIDS and perform a joint focused analysis of cyberspace. The immersed cyberspace subject matter experts are more capable of identifying, documenting, and prioritizing tasks that need to be performed in a joint operational environment. Likewise, these tasks are less service-centric and more joint-centric to effectively field integrated, joint capabilities.

The Air Force and Cyberspace

On December 7, 2005, the Air Force added cyberspace to its mission statement as a result of the on going concerns with respect to gaining superiority in cyberspace. Since then, there have been numerous initiatives and changes in the Air Force in order to increase the priority of cyberspace and mature our cyberspace capabilities. As with any new changes to a large organization, the challenges have been daunting and progress has been slow. However, the Air Force is making forward progress and it can be seen in how the leadership and personnel are working hard to create a lethal cyberspace force.

The Secretary of the Air Force, the Honorable Michael W. Wynne, recently discussed the Air Force's cyberspace vision and the underlying focus for cyberspace by noting:

“Just as water molecules and principles of hydrodynamics define the sea domain and just as air molecules and principles of aerodynamics define the air domain, so do the electromagnetic spectrum (EMS) and associated electronics and energy propagation define cyberspace. This includes all signals that flow through the EMS – those from cell phones, the Internet, and remote-detonation devices. If it emits, transmits, or reflects, it uses cyberspace.”

This overarching revelation by the Secretary is colossal. The level of effort required to meet these expectation clearly shows the reasoning for adding cyberspace to the Air Force mission statement. Success in such a broad all encompassing environment where anything that “emits, transmits, or reflects” is included requires some creative leadership and well focused efforts; both of which are coming together in the Air Force.

By making cyberspace a direct part of the Air Force mission, it is clear that the Air Force is taking serious the major cultural and institutional changes required to be successful. Although the progress may be somewhat slow, forward progress is being made. From the highest Air

Force leadership down, more emphasis is being placed on cyberspace. Resources and personnel are being reallocated to support the fundamental shifts required to dominate cyberspace.

On November 2nd, 2006, Secretary Wynne announced the establishment of a new Air Force Cyberspace Major Command and stated:

“The new Cyberspace Command is designated as the 8th Air Force...under the leadership of (Lt. Gen. Robert J. “Bob” Elder Jr.) He will develop the force by reaching across all Air Force commands to draw appropriate leaders and appropriate personnel.”

The step to stand up a major command for cyberspace clearly shows the commitment the Air Force is showing to stand up a formidable cyberspace force. The Air Force is pressing forward and the Cyberspace Major Command will be stood up officially in the fall of 2007.

Lt. Gen. Elder has been providing a tremendous amount of direction and feedback about where the Air Force Cyberspace Command is headed. He’s been upfront about the fact that cyberspace is a warfighting domain for the Air Force. His organization is in the process of staffing the Draft Cyber Warfare Air Force Concept document discussed earlier to help shape the direction of the command and interaction with combatant commanders, other services, and agencies. He has also discussed some examples in three categories that are worth noting below:

- Electromagnetic Spectrum Operations
 - o Electronic Spectrum Jamming (Electronic Warfare)
 - o Jam-resistant communications
 - o Self forming, airborne networks
- Electronic System Operations
 - o Sensor Dazzlers (Electronic Attack)
 - o Electronic chip set (hardware code) integrity testing
 - o Electro-magnetic pulse resistant electronics
- Network Operations
 - o Networked system attack
 - o Adaptive firewalls, database wrappers, database encryption
 - o Survivable and secure computer networks

All three categories are perfect areas for further JCIDS analysis. In fact, there are other important aspects of what Lt. Gen. Elder is touching on that are worth noting. Along with the three categories above, he has discussed the foundation for the future of cyberspace using following bullets:

- Requirements
 - o Survivable C2 (warfighting) network operations
 - o Secure, defendable C2 and administrative networks
 - o Net-centric service and data architectures
 - o Self-forming, high-capacity, expeditionary IP networks
 - o Global Air, Space & Cyberspace C2 Capabilities
 - o Operational capabilities against closed networks
- Near-term Focus Areas
 - o Cyber Force Training and Career Development
 - o Systems Design (Resilience, Program/Data Protection)
 - o Software Design (Applications Assurance)
 - o Mission/Security Balance (Risk Management)
 - o Cyberspace Innovation Center (Industry/Academic)

All bullets give a good understanding of the sophisticated and immense work load facing the Air Force. Lt Gen Elder also stresses the importance of a fully joint interdependent cyberspace force to “ensure freedom to operate across all domains; deny cross-domain freedom to adversaries”.

As the cyberspace command evolves, the JCIDS process can be a significant enabler if embraced by Air Force leaders. Every one of the bullets highlighted by Lt Gen Elder is a great place to start JCIDS analysis on. For some of the ideas, the Air Force and other services are already doing a tremendous amount of work to press forward, while many of the other ideas haven’t had as much thought put to them. In addition, Lt Gen Elder highlights the importance of multi-service integration by making note of it in his recent article titled “Effects-Based Operations A Command Philosophy” where he says:

“having all components in a joint force working together to achieve common objectives and effects obviously provides a focused sense of direction and unity of effort. We’ve all heard the

story of how different services might interpret a similar order, such as “secure the building.” Although we tell that story in jest, in reality, without explaining our objectives in greater detail, we can expect each component to interpret them differently, based on its own perspective of the situation.”

Lt Gen Elder’s point shows how our senior leaders understand how a service-centric focus can limit our ability to provide capabilities for utilization in a multi-service/multi-agency environment. There in lies the key to JCIDS. Used properly and emphasized by leadership, the system will help staff officers evolve to reduce service-centric blinders. It will allow leaders and staff officers to take a hard look at the tasks and capabilities with respect to cyberspace and build them with a joint flavor and commitment to multi-service/multi-agency interoperability.

Summary

Cyberspace becomes more and more relevant to national security every day. As the United States and the global economy continues to develop rapidly through amazing technological growth and efficiency, the cyberspace threat to national security will grow exponentially. The government leadership has identified the threats in national strategic documents, and the Department of Defense has introduced a new definition for cyberspace. The Air Force, understanding the critical need for a pathfinder in cyberspace, has taken on the burden to build joint capabilities to attain dominance and superiority in cyberspace. The road will be a long one, and there will be lessons learned all along the way.

The JCIDS process has been put in place as a facilitating system to allow service-centric subject matter experts and staff officers to perform analysis from an integrated, joint perspective. If the system is followed correctly it will help place priorities where they need to be place and help press forward in the multi-faceted, complex environment of cyberspace.

IV. The Cyberspace Defense Example

Chapter Overview

The purpose of this chapter is to highlight both a JCD and an ICD developed using the JCIDS process to backup the assertion of this paper that JCIDS strengthens the way ahead for cyberspace operations. The JCD and ICD are related documents focused on cyberspace defense and provide an excellent example of how to perform JCIDS analysis. They also provide a template that will help staff officers and subject matter experts press forward methodically and write JCDs and ICDs for all operational aspects of the cyberspace domain.

Pathfinder versions of both the JCD and ICD are provided in Appendices A and B, respectively. The documents were developed by two subject matter experts in cyberspace operations and two subject matter experts in optimization and analysis. Three of the team members were USAF Majors, while the fourth was a USAF Captain. Across the board, the depth of experience provided by each team member was a significant enabler for successful completion of the document. All members were extremely committed to in-depth analysis of cyberspace defense and how to provide the most relevant and joint focused recommendations possible. The documents are excellent examples of how to perform the JCIDS process and provide an immense amount of solid information to support a joint approach to cyberspace defense capabilities, training, and operations.

To reiterate how JCIDS helps strengthen the way ahead for cyberspace, readers will continue to gain a better understanding of how cyberspace leaders and professionals can leverage JCIDS to be successful in:

- 1) understanding joint cyberspace tasks and activities

- 2) providing a defensible and credible set of prioritized capability gaps
- 3) providing a list of well thought out measures of effectiveness to gauge future success
- 4) offering the best DOTMLPF cyberspace solutions, from both near and long term perspectives

The Cyberspace Defense JCD

As stated in the JCD section of Chapter II, Explanation of JCIDS, the JCD is a fundamental JCIDS document which helps facilitate a capabilities-based analysis to identify what is important to warfighters. The JCD helps organize and prioritize tasks essential to meet warfighters needs from a joint perspective. The document also helps layout a prioritized list of capability gaps that inherently limit the ability of warfighters from performing essential tasks.

The JCD follows a format that is provided in CJCSI 3170.01B, Enclosure D, and the JCD outline is organized as follows:

- 1) Concept of Operations Summary
note: An Operational View (OV-1) is required
 - 2) Joint Functional Area
 - 3) Required Capability
 - 4) Capability Gaps
 - 5) Threat and Operational Environment
 - 6) Recommendations
-
- The diagram shows two horizontal arrows pointing to the left. The top arrow is labeled 'FAA' and points to the right side of a bracket that groups items 2) Joint Functional Area and 3) Required Capability. The bottom arrow is labeled 'FNA' and points to the right side of item 4) Capability Gaps.

As shown in the outline, the FAA is performed in sections 2 and 3, while the FNA results are provided in section 4 of the document. The example in Appendix A follows this format, and it is recommended for readers to review the JCD on cyberspace defense while reading this section. The section discusses the outline of the JCD in order starting with the Concept of Operations Summary and ending with the Recommendations section.

First, the Concept of Operations Summary is used to set the stage of the document and provide a scope to help shape the document for feasibility. It is important to establish scope up

front and keep the team focused on the scope. So many times, these analysis projects get out of hand because no scope was established up front. No matter how much the team wants to address issues outside the scope, it is recommended that a team stick to the original scope while using JCIDS. Otherwise, the whole project can become extremely overwhelming.

A concept of operations is an overall interpretation and Joint Publication 1-02 defines a concept of operations as follows:

“A verbal or graphic statement, in broad outline, of a commander’s assumptions or intent in regard to an operation or series of operations...The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity and purpose.”

With respect to a JCD, remember to setup the overall scene for the concept and describe the operational relationships without getting into too much detail. The use of an Operational View (OV-1) is mandatory to provide a general visual reference. The JCD Concept of Operations Summary needs to set the stage for the operational environment while foreshadowing the types of effects and capabilities-based approaches commanders need to be successful in the environment.

The Draft Cyber Warfare Air Force Operational Concept is a great place to start with respect to a cyberspace concept of operations. The document does a great job to describe operations where the Air Force is concentrating on. I would recommend to Air Staff and Cyberspace Command that staff officers work hard to put out JCDs on Countercyber Operations, Offensive Counter Cyber, Defensive Counter Cyber, and others as described right out of the Draft Cyber Warfare Concept.

As this paper makes its way through how the JCDs and ICDs focus analysis on joint capabilities, it will be easier to see why staff officers should engage using the JCIDS process.

Other great areas for performing JCIDS analysis are the examples discussed in Chapter III, the Air Force and Cyberspace. As the Air Force moves forward, it is critical for cyberspace professionals to pay attention to what the Secretary of the Air Force and the leaders in cyberspace are saying about the direction of cyberspace and the capabilities required for achieving cyberspace superiority. Also, when writing JCIDS documents, it is important for Subject Matter Experts (SMEs) to be included at the outset of writing to help develop the concept of operations summary. Their insight can not be underemphasized and is essential to provide credibility to the overall JCD.

The cyberspace defense team provided the scope of the JCD upfront in Section 1.3 to ensure the effort did not veer from track. This worked well, and the team was successful to press forward through the analysis process well synchronized. The cyberspace defense concept of operations summary was written to provide an overall idea of how cyberspace operators work to defend cyberspace and provide cyberspace defensive capabilities to combatant commanders, services, agencies, and multi-national allies. It was intended to address an ever changing environment where allies change over time depending on different operations, campaigns, world events, etc. The concept even indicates the premise of how a joint commander in charge commands forces and some organizational considerations to help focus the analysis.

There will be disagreements among team members when writing the concept of operations summary. The disagreement is expected and good for the overall effort. The important part of the disagreement is to get advice from leadership and work to find common ground. Remember, the concept is about today's and tomorrow's operations. With respect to cyberspace, creativity and boldness will go a long way. There are political constraints, bureaucracy, and laws that may inhibit cyberspace warfighters from operating in a certain way,

but don't let those issues hold the team back from writing the right concept of operations based on their subject matter expertise. An example of this was realized when the team was trying to include the statement:

“The joint cyberspace commander will have joint personnel attached and collocated with services, combatant commanders, agencies, coalitions, and homeland security...The concept cohesively integrates all military cyberspace defense operations through a fully joint approach where the joint commander can organize, train, provide equipment, and decide what the standards are for cyberspace defense.”

The statement could be interpreted by some as outside current law and political limitations instilled on combatant commanders where the military services are responsible to organize train and equip. So, the team added a reference in the summary stating: “From this description of the cyberspace defense operational view, the roles and responsibilities for cyberspace described contain similarities to the operational missions of United States Special Operations Command and United States Strategic Command.” The annotation was a compromise on the team to show that we felt the constructs of the two combatant commands had aspects that are important to success in cyberspace.

The next big hurdle was Section 2, the Joint Functional Area, which was a significant piece of the FAA in order to show pedigree for the cyberspace defense JCD. The team members dove into national strategy documents, joint doctrine, Joint Capability Areas, JOCs, JICs, JFCs, and looked at how the joint community and services were engaged in cyberspace defense. The reading is straight forward, and the Joint Functional Area section can be updated over time and utilized time and again to support many different JCDs. Ultimately, the section emphasizes the need for cyberspace defense and highlights the overall guidance that exists to support a top-down approach to defining the tasks required for cyberspace defense.

Section 3, Required Capability, wraps up the FAA and tasks that are required with respect to cyberspace defense as well as Measures of Effectiveness (MOEs) to be used to measure the performance of tasks to achieve the intended objectives. First, the team identified four cyberspace defense tasks that need to be performed based on the overall FAA. These tasks were:

- Task 1: Defend Cyberspace Information & Information Systems
- Task 2: Command & Control of Cyberspace Defense
- Task 3: Organize, Train and Equip Cyberspace Personnel
- Task 4: Test and Acquire Information Systems

Then, the team correlated the tasks with the Universal Joint Task List (UJTL) and identified over 200 existing MOEs to support the four tasks. A significant amount of time was spent to consolidate the 200 MOEs into a form to support the four tasks.

Another issue the team faced was the overwhelming number of systems that fall under the cyberspace defense umbrella. To deal with the issue, the team devised an Information Category condition in Section 3.1.2 to help segment systems based on their respective category.

There are four categories listed as follows:

- InfoCAT-A - Information Systems used to operate DoD Weapon Systems
- InfoCAT-B - Information Systems certified to processing Top Secret data
- InfoCAT-C - Information Systems certified to processing Secret data
- InfoCAT-D - Information Systems certified to processing Unclassified data

This approach enabled the team to provide a more detailed breakdown for MOEs based on the criticality of the system. The tasks and associated Information Categories are shown in Table 1 along with the respective MOE standards the team developed.

Task 1: Defend Cyberspace Information & Information Systems			
MEASURE		INFOCAT	STANDARD
M1-1	Percent Of Cyberspace Attacks Successfully Defended	A	99.99%
		B	99.9%
		C	99.5%
		D	99%
M1-2	Time To Investigate & Report Impact, Post-Attack	A	30 Minutes
		B	60 Minutes
		C	120 Minutes
		D	480 Minutes
M1-3	Time To Recover, Post-Attack	A	5 Minutes
		B	15 Minutes
		C	60 Minutes
		D	240 Minutes
Task 2: Command & Control of Cyberspace Defense			
MEASURE		INFOCAT	STANDARD
M2-1	Maintain Cyberspace Situational Awareness	All	99.9%
M2-2	Convene Cyberspace Threat Conference To Direct Attack Response Actions	All	99.9%
M2-3	Time To Notify Users Of New Attacks/Threats/Countermeasures	A	5 Minutes
		B	5 Minutes
		C	10 Minutes
		D	10 Minutes
M2-4	Time To Notify Users Of Known Vulnerabilities/Responses	A	4 Hours
		B	4 Hours
		C	6 Hours
		D	6 Hours
Task 3: Organize, Train and Equip Cyberspace Personnel			
MEASURE		Info Cat	STANDARD
M3-1	Perform Standards Verification	All	Yes/No
M3-2	Percent of Trained Cyber/Information Operations Personnel	A	98%
		B	98%
		C	98%
		D	98%
M3-3	Provide Cyberspace Defense Plans	All	Yes/No
Task 4: Test and Acquire Information Systems			
MEASURE		Info Cat	STANDARD
M4-1	Percent of Information Systems Meeting Availability Standards	A	99.99%
		B	99.9%
		C	99.5%

		D	99%
M4-2	Percent of Information Systems Meeting Interoperability Standards for Cyberspace Defense	A	99.99%

Table 1: Cyberspace Defense Tasks with Associated INFOCATs and MOEs

The emphasis for sound MOEs cannot be understated. A great discussion on MOEs can be found in Chapter 6 of the Air Force Analyst’s Handbook, written by Christopher A. Feuchter. The team spent many hours refining and developing MOEs. The reason MOEs are so important is because they provide future acquisition/test personnel and operators a sound means to measure successful completion of tasks. A few rules of thumb are important here. First, often Boolean measures don’t provide adequate resolution. Percentages, ratios, and quantifiable measures are best. Second, the more details provided with a constraint the better. Also, leaders and SMEs who are familiar with the nature of the operations are the best to establish and validate the MOEs the first time around. So, spend enough time to refine MOEs; they can be changed over time if needed, but they’re critical throughout the entire approval, acquisition, and fielding process to get the right capabilities in the hands of professionals.

Section 4, Capability Gaps, is the FNA. This section takes the tasks required through the JCIDS analysis and identifies capability gaps associated with each task. The team identified eleven capability gaps through the FNA and the gaps are listed Table 2. The section sets up the team for the final JCD recommendations and establishes the final essentials to feed the ICD and perform a formidable FSA and overall recommended way ahead.

Task 1: Defend Cyberspace Information & Information Systems	
MEASURE	IDENTIFIED GAP
M1-1 Defend Against Cyberspace Attacks	There are shortfalls with the capabilities to protect the integrity of information, and information systems from external and internal threats in cyberspace
Task 2: Command & Control of Cyberspace Defense	

MEASURE		IDENTIFIED GAP
T2	C2 of Cyberspace Defense	There is no effective joint standardized Command and Control (C2) tactics process and organization for service, joint, coalition, and national cyberspace defense.
M2-1	Maintain Cyberspace Situational Awareness	There is no centralized ability to obtain or maintain cyberspace situational awareness over joint and national critical defense infrastructure, information, and information systems.
M2-2	Convene Cyberspace Threat Conference to Direct Attack Response Actions	There is a lack of capability to synchronize cyberspace defensive actions and operations in real-time with Combatant Commander (COCOM), National Security, and Homeland Defense operations.
		There is no capability to immediately notify Services, COCOMs, National Security organizations, and Homeland Security organizations of cyberspace emergencies.
M2-4	Notify users of known vulnerabilities/responses	There is no capability to share lessons learned between Service, COCOM, National Security, and Homeland Security cyberspace operators.
Task 3: Organize, Train and Equip Cyberspace		
MEASURE		IDENTIFIED GAP
M3-1	Perform Standards Verification	The standards that exist are very system-specific; there are no overarching joint standards for cyberspace defense evaluation.
M3-2	Systems with Trained Cyber/Information Operations Personnel	There is no joint cyberspace defense school for training personnel to protect and defend cyberspace information and systems in joint and multinational environments.
M3-3	Provide cyberspace defense plans	There is a lack of capability to adequately plan cyberspace defensive actions with wartime, contingency, and disaster plans for COCOMs, National Security organizations, and Homeland Security organizations.
		There are inconsistent policies for protecting end-to-end availability and assured access to cyberspace information, resources, and systems.
Task 4: Test and Acquire Information Systems		
MEASURE		IDENTIFIED GAP
M4-2	Establish Cyberspace Defense Interoperability Standards for Information Systems	There is no structured joint approach for developing standardized and interoperable cyberspace defense qualities, aspects, features, and requirements in information systems.

Table 2: Cyberspace Defense Capability Gaps

Finally, Sections 5 and 6 reiterate the threat emphasizing the need for capabilities identified in the JCD as well as recommendations on how the capability gaps should be prioritized. An ICD, or suite of ICDs, will be developed based on how the gaps are prioritized. This feeds the solutions analysis and helps give credence to the recommended way ahead that comes out of the ICD.

The Cyberspace Defense ICD

Now that a JCD is produced or better, a suite of JCDs, a team can pull together strong ICD(s) to shore up a clear way ahead to support joint warfighting operations. As mentioned earlier in Chapter II, The ICD builds off the JCD(s). For cyberspace defense, we used the JCD recommendations and prioritized capability gaps to press forward with a solutions analysis.

In many respects, the ICD restates what is already written as part of the JCD. The main difference is the FSA. The organizational format for an ICD can be found in CJCSI 3170, Enclosure E, and is provided below:

- 1) Joint Functional Area
 - 2) Required Capability
 - 3) Concept of Operations Summary
 - 4) Capability Gaps
 - 5) Threat and Operational Environment
 - 6) Functional Solutions Analysis
 - a. Ideas for Non-Materiel Approaches (DOTMLPF Analysis)
 - b. Ideas for Materiel Approaches
 - c. Analysis of Materiel/Non-Materiel Approaches (AMA)
 - 7) Final Recommendations
-
- The diagram consists of two large curly braces on the right side of the list. The first brace groups items 1 through 5 and is labeled 'Provided by JCD'. The second brace groups items 6 and 7 and is labeled 'FSA'.

Since Sections 1 thru 5 are provided by the JCD and have already been discussed this section will focus only on the FSA and the DOTMLPF analysis. So, we'll start with Section 6 and finish

up with Section 7 to show how the FSA identifies solutions, performs solutions analysis, and finally provides a recommended way ahead.

At this point, a discussion of what non-materiel versus materiel solutions is helpful. A non-materiel solution is basically using or modifying existing resources and manpower as an approach to the solution. A materiel solution is where a non-existent system, device, weapon, etc needs to be developed or acquired to fill the capability gaps. In the FSA, it is good to have a strong mix of both in order to see the full picture of the required effort and options available. Also, the description of each idea does not need to be in exhaustive detail. An overall description works well for this effort. The details of the idea will be fleshed and detailed in more depth after the ICD is funded further down in the corporate process.

The first effort of the FSA focuses on the DOTMLPF analysis to what existing resources and organizations are available or can be reorganized to fill the capability gaps. For the cyberspace defense example, the team had a number of ideas like reorganizing career fields and standing up a joint cyberspace defense school and warfare center. There were also some ideas on reorganizing some of the joint commands.

The next part of the process is to get ideas for materiel approaches to provide solutions for the capability gaps. The cyberspace defense team came up with some new systems that would be important to push cyberspace defense forward in a joint direction. Throughout the FSA, the team identified many other solutions that were easily weeded out during the solutions analysis portion of the process. For the time being, the team concentrated on identifying solutions to fill the capability gaps identified during JCD development.

The next step, Analysis of Materiel/non-Materiel Approaches (AMA), is critical and having one or two operations analysts to work along side the SMEs will go a long way. The

cyberspace defense team first created a methodology to help assist the overall AMA analysis. The methodology broke out a list of feasibility factors that were given an assigned SME weighting. All factors had written definitions to help the team delineate an overall grade for each solution. The team also analyzed each solution relative to the “Do Nothing” solution. As with any analysis, there were many assumptions the team documented in Section 6.3.1.10. The overall feasibility worksheet is provided at the end of the ICD for review and to help give an understanding of the level of effort required.

The team then struggled with where to go next. None of the solutions was a glaring single solution to answer the cyberspace defense needs. After deliberating for some time the team came up with a way to integrate the solutions that filled certain capability gaps along with a phased implementation approach to take advantage of low hanging fruit and build a foundation for long-term evolution of systems not yet developed or mature enough for implementation. The overall recommended solutions are provided in Table 3. This approach worked well and the team was able to recommend a concentration on near-term capabilities that improved cyberspace defense in many areas. Then, the mid-term and long-term capabilities would be brought on-line on top of a solid foundation to fill all the capability gaps identified in the JCD.

The final approach was a nine-year phased approach and the “Solutions Performance and Capability Gaps” appendix to the ICD is good reference to review. It starts with the “Do Nothing approach” along the top, and then begins with the near-term over the first three years, followed by mid-term, and long term. The approach uses a number of solutions that work together to help fill all the gaps for cyberspace defense.

Remember, this is an example of many ways to perform an AMA. The approach worked well for cyberspace defense, but may not work well for other ICDs. The methodology a

team develops for AMA will depend on the type of capability gaps the team is trying to fill and the solutions recommended. The point is JCIDS can help strengthen the cyberspace way ahead. Cyberspace leaders and staff officers need to start using JCIDS in order to advocate for the complex capabilities and systems to enable our military to dominate cyberspace. The cyberspace defense ICD is a good example, and can be used as a guide to help subject matter experts and analysts work through the process.

GAP Description	Joint C2	Joint SA	Synchronize Ops	Notify of new threats	Share Lessons Learned	Joint Training	Defend against attack	Policy & doctrine	Joint Interoperability	Standards Verification	Adequate Planning
JCD GAP Ranking	1	2	3	4	5	6	7	8	9	10	11
NEAR TERM (0-3 Years) - Establish organizational groundwork & enable expertise needed to dominate the virtual battleground	Red	Red	Yellow	Yellow	Green	Green	Red	Green	Green	Green	Green
US Cyberspace Command (USCYBERCOM)	Red	Red	Red	Yellow	Green	Red	Red	Green	Green	Green	Green
Create Joint Cyberspace Defense School and Warfare Center	Red	Red	Red	Red	Red	Green	Red	Red	Red	Red	Red
Develop Cyberspace Defense career fields (enables development of Cyberspace Professional Cadre)	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red
Modify JTF-GNO mission/organization to include Cyberspace Defense	Red	Red	Yellow	Yellow	Yellow	Red	Red	Red	Red	Red	Red
Each Term Builds on Top of the Previous Term											
MID TERM (3-6 Years) - Adds standard defensive equip & upgrades C2 node	Yellow	Yellow	Yellow	Yellow	Green	Green	Red	Green	Green	Green	Green
Near Term Capabilities	Yellow	Yellow	Yellow	Yellow	Green	Green	Red	Green	Green	Green	Green
IOC of Distributed Cyber Defense System	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red
IOC of Joint Cyber Operations Center – Replaces Modified JTF-GNO	Yellow	Yellow	Yellow	Yellow	Yellow	Red	Red	Red	Red	Red	Red
Each Term Build On Top of the Previous Term											
FAR TERM (6-9 Years) - DCDS & JCOC go FOC	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Mid Term Capabilities	Red	Red	Yellow	Yellow	Green	Green	Red	Green	Green	Green	Green
FOC - Distributed Cyber Defense System	Red	Red	Red	Red	Red	Red	Green	Red	Yellow	Red	Red
FOC - Joint Cyber Operations Center	Green	Green	Green	Green	Yellow	Red	Red	Red	Red	Red	Red

Table 3: Cyberspace Defense Recommended Solution (Phased Approach)

Summary

The cyberspace defense JCD and ICD discussed in this chapter show an example of how JCIDS can help strengthen the cyberspace way ahead. The chapter documented how cyberspace leaders and professionals can leverage JCIDS to be successful in:

- 1) understanding joint cyberspace tasks and activities
- 2) providing a defensible and credible set of prioritized capability gaps
- 3) providing a list of well thought out measures of effectiveness to gauge future success
- 4) offering the best DOTMLPF cyberspace solutions, from both near and long term perspectives

It is important to remember the FSA/AMA portion of the ICD can be performed in many different ways and team leaders should consider having an optimization and analysis professional be a part of the team from the beginning. The professional will significantly help define strong measures of effectiveness and integrate sound analysis/optimization techniques throughout the process.

V. Strengthening the Cyberspace Way Ahead

The JCIDS joint focus on national strategy, tasks, and capabilities ensures a grounded approach to strengthen the cyberspace way ahead. In addition, it helps develop cyberspace doctrine along the lines of priorities and needs of joint warfighters. This approach assists to provide a solid foundation to help navigate through the DoD corporate process, and ultimately provides the cyberspace community an ability to acquire funding through credible arguments. In addition, the analysis of national strategy guidance, doctrine, JFCs, JICs, JOCs, gives essential pedigree to the cyberspace way ahead. The analysis also aligns the tasks and capabilities with UJTLs to provide additional strength when vetting the overall cyberspace way ahead.

With respect to doctrine development a suite of cyberspace JCDs and ICDs provides a new wave of documents to build doctrine from. In reality, it is a new way to build doctrine closely with approaches to DoD 5000 acquisition, funding, and the DoDAF architectural framework. Cyberspace is an extremely complex, changing environment. The JCIDS process provides a method to breakdown the complexity of the cyberspace operational environment in manageable chunks using documents that can evolve along with the changes and challenges of cyberspace.

In addition, the JCIDS capabilities-based approach helps leaders get a better understanding of the overall cyberspace domain as it evolves. The approach helps build experts capable of understanding the broad issues with cyberspace and how their unique experiences in the domain can be leveraged to propel the US military's cyberspace lethality and effectiveness forward in a joint focused manner.

Finally, the JCIDS process helps prioritize capabilities based on joint warfighters needs and national guidance. Many of the capabilities in cyberspace overlap and are critical for other

domains than cyberspace. Effective use of the JCIDS process will help reduce stovepipe acquisitions and maximize how capabilities are used across all operational domains. As the Air Force presses forward, the JCIDS process will help fill in many blanks and effectively use subject matter experts across the entire cyberspace electromagnetic spectrum to build a joint focused lethal force. It will be heavy lifting and it will take time, but if the effort and time are put in, JCIDS will help strengthen the cyberspace way ahead. The efforts will also help Air Force leaders compete for limited funding through joint capabilities based assessments focused on warfighters needs.

The joint aspects of JCIDS helps the Air Force deal with the vast domain of cyberspace. As the Air Force presses forward in cyberspace, leaders need to press staff officers to think jointly. Officers today are getting increased training on joint doctrine, and they are frequently operating in joint environments. This trend continues to be emphasized in the Air Force for good reason, and leaders can use this along with JCIDS to further our progress dramatically in cyberspace. As staff officers continue to learn about their sister services and the priorities of combatant commanders they can help further the military's ability to dominate cyberspace.

In the end, since JCIDS focuses to create joint capabilities from a top-down approach, the Air Force can use the documents to build alliances with combatant commanders and other services to show how we can make forward progress in cyberspace.

VI. Lessons Learned

Measure of Effectiveness (MOE)

The importance of well thought-out MOEs can not be underestimated. A team working on a JCD should not take the MOE development lightly. The SMEs on the team must create MOEs that are sound in order to provide a reference of success. This is a lesson the military has learned time and again. Without solid MOEs, further down the line, the testing and fielding professionals will not be able to provide a true representation of success or failure.

A few rules of thumb are important here. Percentages, ratios, and quantifiable measures are best. Second, the more details provided with a constraint the better. Also, leaders and SMEs who are familiar with the nature of the operations are the best to establish and validate the MOEs the first time around. So, spend time refining MOEs, they can be tweaked over time if needed, but they're critical throughout the entire approval, acquisition, and fielding process to get the right capabilities in the hands of professionals

Team Makeup

The team should be made up of SMEs from across the cyberspace spectrum. They need to have an understanding of JCIDS prior to beginning the analysis and every effort should be taken to keep the team together to foster a strong work environment. As staff officers, the JCIDS document development process should be a high priority on their list of responsibilities and daily work effort. Also, the team should have a couple of experienced analysis and optimization experts. When developing the cyberspace defense documents, the analysis and optimization experts on the team help keep everyone grounded and provide invaluable help to strengthen MOEs and perform the solutions analysis. Also, the team should have someone with expertise in

how the DoDAF framework is organized. The JCIDS documents only require an OV-1, but someone with DoDAF experience will understand how the capabilities will be influenced by joint architectural framework. The understanding will help with analysis of overall systems and maintain a joint systems focus since cyberspace is heavily grounded to joint systems.

Use of Scenarios

One area the cyberspace defense team did not take advantage of was the use of scenarios. However, scenario development and utilization can be extremely helpful when developing the concept of operations summary, developing MOEs, and prioritizing capability gaps. The scenarios can also be useful in gaining a better understanding of joint issues surrounding cyberspace and how different combatant commanders handle cyberspace issues. They're highly recommended and should be considered upfront during JCIDS document development.

Analysis Pitfalls

Just like any other early conceptual initiative, there can be a tendency to over analyze. The team should make a conscious effort to keep analysis relevant and well grounded to the overall effort. The optimization/analysis experts can help facilitate this. There will be times when assumptions will have to be made. The best way to deal with assumptions is to document and keep track of them. Very often, the team will realize the validity of the assumption later on during the analysis and make modifications where required. This is very much an art as it is a process, so keep in mind that creativity will help move the process along and expect the analysis to have holes in it. The holes and assumption come along with the environment and risky business related to the military.

Understand Combatant Commanders, Services, Agencies, etc roles/relationship

The team should take time to understand how combatant commanders, services, agencies, etc operate in cyberspace. The information learned will be valuable throughout the process. It will also help breakdown service-centric blinders that will creep up and weaken the end result of the overall documents. The importance of a top-down, born joint approach is essential when gaining approval to build capabilities and acquire funding in cyberspace. The Air Force way ahead in cyberspace needs to exude joint and combatant commanders' priorities for cyberspace superiority. The DoD continues to press services to think joint and provide capabilities that are joint from the beginning. If the Air Force brings a capability to the table that bleeds blue instead of purple, it will be tougher to gain priority and gain alliances to press forward to field critical cyberspace capabilities.

Conclusion

Air Force leaders and staff officers continue to get exposure and training on how the joint community and other services provide capabilities and go to war. Thus, the JCIDS process is not just a means for the Chairman of the Joint Chiefs of Staff to develop capabilities documents. The process can be used by Air Force leaders and staff officers to create top-down, born joint capabilities documents that aid in:

- 1) understanding joint cyberspace tasks and activities
- 2) providing a defensible and credible set of prioritized capability gaps
- 3) providing a list of well thought out measures of effectiveness to gauge future success
- 4) offering the best DOTMLPF cyberspace solutions, from both near and long term perspectives

Ultimately, the JCIDS process facilitates the Air Force's ability to field joint cyberspace capabilities that are truly analyzed and developed from a top-down approach and not a bottom-up stove-pipe approach. The JCIDS process also helps grow joint thinking leaders for cyberspace that will have a big picture understanding of what all services have to provide combatant commanders in order to achieve cyberspace superiority.

Appendix A. Cyberspace Defense JCD

UNCLASSIFIED

JOINT CAPABILITIES DOCUMENT (JCD)

FOR

CYBERSPACE DEFENSE

By:

Maj Mike Hindley

Maj Nick Kozdras

Maj Tim Treat

Capt Richard Brown

11 February 2007

Table of Contents

1 Concept of Operations (CONOPS) Summary.....47

 1.1 Introduction47

 1.2 General47

 1.3 Scope47

 1.4 Cyberspace Defense Operational View.....48

2 Joint Functional Area.....52

 2.1 Strategic Guidance for Cyberspace Defense52

 2.2 Joint Capability Areas (JCA)54

 2.3 Joint Operating Concepts55

 2.3.1 *Deterrence Operations Joint Operating Concept (DO JOC)* 55

 2.4 Joint Functional Concepts56

 2.4.1 *Protection Joint Functional Concept* 56

 2.4.2 *Focused Logistics Joint Functional Concept* 57

 2.4.3 *Net-Centric Environment Joint Functional Concept* 58

 2.4.4 *Force Management Joint Functional Concept* 58

 2.5 Current Cyberspace Defense Related Operations58

3 Required Capability60

 3.1 Functional Area Analysis (FAA) Report.....60

 3.2 Defend Cyberspace Information and Information Systems60

 3.3 Command and Control of Cyberspace Defense61

 3.4 Organize, Train and Equip Cyberspace Personnel61

 3.5 Test and Acquire Cyberspace Systems:62

4 Capability Gap	62
5 Threat and Operational Environment.....	64
6 Recommendation	65
AppendixA Cyberspace Defense Tasks and Measures of Effectiveness Analysis.....	68

Table of Figures

Figure 1: Command and Control of Joint Forces through Cyberspace	49
Figure 2: Coordination with External Entities through Cyberspace	50
Figure 3: OV-1 Cyberspace Defense Operational View	51

Index of Tables

Table 1: Measures to Defend Cyberspace Information and Information Systems	61
Table 2: Measures for Command & Control of Cyberspace Defense	61
Table 3: Measures to Organize, Train and Equip Cyberspace.....	62
Table 4: Measures to Test and Acquire Information Systems.....	62
Table 5: Capability Gaps	64
Table 6: Prioritized Capability Gaps.....	67

1 Concept of Operations (CONOPS) Summary

1.1 Introduction

1.1.1 As the US military becomes increasingly reliant on cyberspace to achieve and maintain superiority in the traditionally recognized operational/strategic domains (land, sea, air, and space), cyberspace has become an operational domain in its own right. The virtual cyberspace theater has evolved to a strategic high ground instead of just a force enabler or multiplier. This evolution from force enabler to strategic/operational domain requires a dramatic examination of military forces and capabilities to ensure our military force is capable of achieving and maintaining cyberspace superiority. In addition, that superiority must be sustained in a Joint and Coalition environment as well as between military forces and national and local agencies protecting the homeland.

1.2 General

1.2.1 This Cyberspace Defense document contains a Capabilities Based Assessment (CBA) that includes both a Functional Area Analysis (FAA) and a Functional Needs Analysis (FNA). The document identifies core tasks associated with cyberspace defense and identifies capability gaps that need to be addressed in order to achieve cyberspace superiority during military operations.

1.2.2 The Functional Area Analysis (FAA) pulls information from many existing strategic documents, including a review of the Quadrennial Defense Review (QDR) for 2006, the National Security Strategy, the National Defense Strategy, the National Strategy to Secure Cyberspace, the National Military Strategy for Cyberspace, Joint Operational Concepts and Joint Functional Concepts. All consistently identify cyberspace as a new operational/strategic domain that must be defended. The challenge as outlined in these documents is not just retooling our military forces to operate more effectively in cyberspace, but to appropriately ensure our use of all of the instruments of national power; economic, military, political, and information.

1.2.3 One of the biggest challenges for cyberspace is development of a definition. Since the cyberspace theater is asymmetric and virtual, there are multiple working definitions. Recently, the Joint Chiefs of Staff released a definition stating, “Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.”¹ This definition allows us to adequately scope our efforts by providing a foundation to link the required tasks and capability gaps to during the FNA.

1.3 Scope

¹National Military Strategy for Cyberspace

1.3.1 This document focuses on a capabilities-based assessment for cyberspace defense. It does not directly assess cyberspace attack; rather it concentrates on synchronizing cyberspace forces to defend against internal and external attacks and exploitation in the asymmetric cyberspace theater of operations. The document also does not address the physical aspects of information protection in containers, facilities, on individuals, etc... as much of that is already effectively addressed in the functional area of force protection. In order to scope the project to a manageable scale, this document concentrates on the defense of cyberspace information specifically in the cyberspace theater of operations.

1.4 Cyberspace Defense Operational View

1.4.1 The DOD is faced with the evolution of a global system of systems that reside in Cyberspace. Not only are sensors, platforms, systems, and networks becoming more global, they are becoming intertwined and technologically intense. Given this, we have struggled to manage complexity, reduce the risk of compromise, and develop methodologies that affordably increase military capability.

1.4.2 As our military effectiveness develops through cyberspace capabilities, it will be critical to introduce and evolve an effective cyberspace defense operational concept based on an operational view. The concept will have to be executed in a joint environment alongside our technical advances in military capability. The obvious need for the cyberspace defense concept is derived from the realization cyberspace has created a more intense and asymmetric battle front. As the joint community becomes more reliant on technology, and employs smaller numbers of highly capable assets to achieve objectives, the defense of cyberspace must be a priority and executed unambiguously.

1.4.3 The cyberspace defense operational view is based on the joint staff definition of cyberspace stated previously in paragraph 1.2.3. The definition provides a foundation for an overall concept of unambiguous defense of cyberspace and the development of the tactics, people, and systems required. To provide a visual example, Figure 1 shows an overview for command and control of joint forces through joint cyberspace networks. It is not an all encompassing diagram for cyberspace but enables the following paragraphs to accurately outline the overall approach for the cyberspace defense CONOPS.

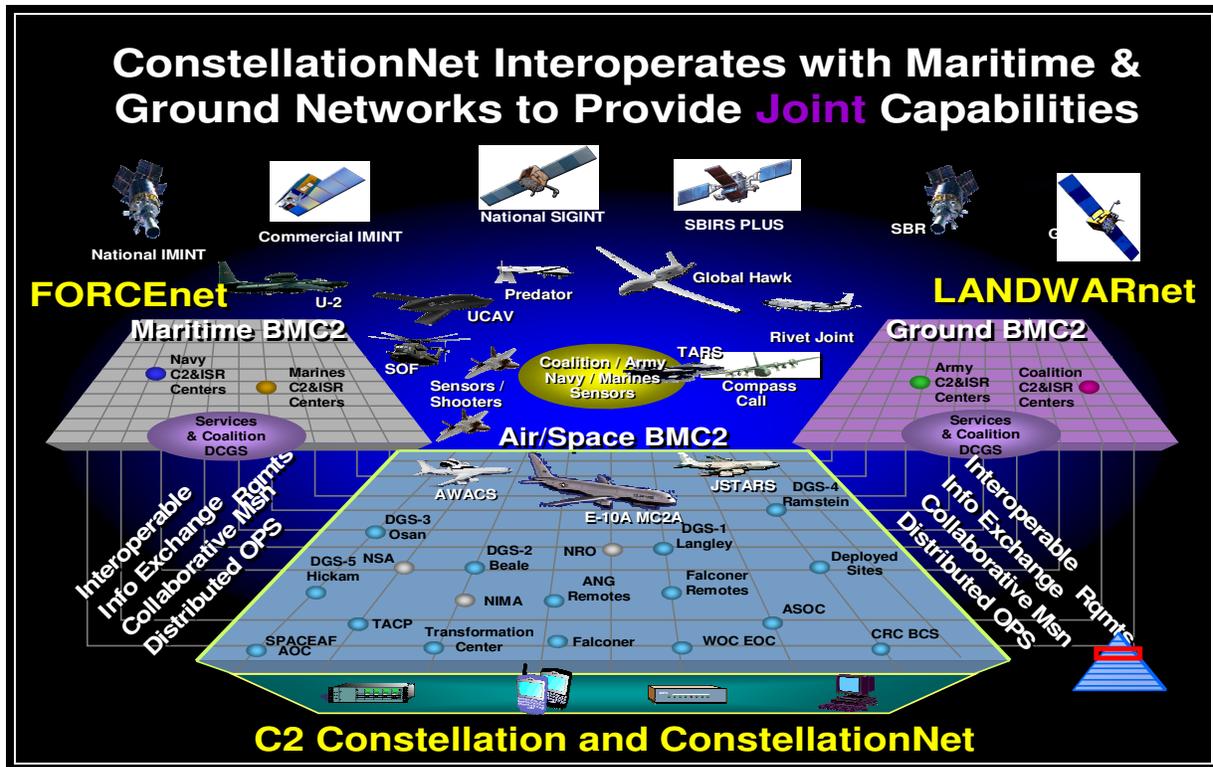


Figure 1: Command and Control of Joint Forces through Cyberspace²

1.4.4 First, the military is evolving from platform-centric operations to net-centric operations connected through cyberspace allowing services, combatant commanders, agencies, and multi-national forces to synchronize operations and work in conjunction with each other. *The level-of-effort to adequately defend the cyberspace battle front from internal and external attack or “unintended fratricide” is the crux of the cyberspace defense operational view.* For our net-centric operations to be reliable, successful, unhindered, and secure, we must be able to protect and verify cyberspace connectivity throughout Figure 1 for all levels of security and weapon systems in the joint environment.

1.4.5 Next, Figure 2 shows how the joint community evolves to synchronize operations through cyberspace. An adequately defended cyberspace theater provides military commanders the critical access to information and systems when operating with combatant commanders, multi-national forces, national agencies, and homeland security. Again, the diagram does not adequately represent the complex environment of cyberspace. Since the environment is virtual, adaptive, and asymmetric, the dynamic nature of cyberspace must be imagined as much as documented on paper.

² Implementing the Constellation Net briefing, Titcombe, Matthew A.

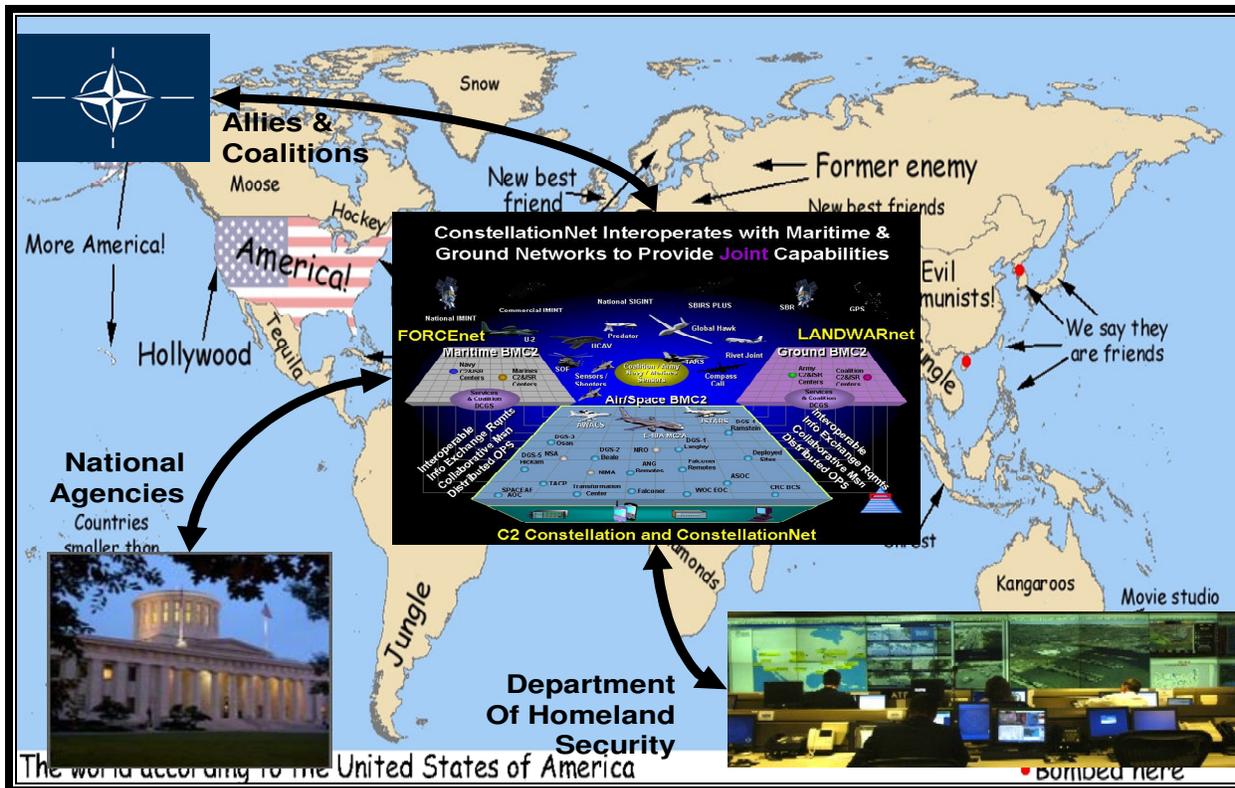


Figure 2: Coordination with External Entities through Cyberspace

1.4.6 As a build to the previous diagrams, Figure 3 includes a dotted line around the cyberspace environment that is intended to be porous to allow authorized personnel access to critical information resources and automated dissemination of trusted and verified information. The figure also shows how we must be able to maintain the strategic cyberspace high ground through fully vetted and effective cyberspace defense. This operational cyberspace defense concept provides the ability to defend, assure, secure, and verify information throughout the cyberspace theater of operations. The concept also provides for the ability for combatant commanders and joint forces to work with agencies, allies, coalitions, and Homeland Security. In this manner, we can defend cyberspace:

1. from attack
2. from unintended loss/compromise of information while providing assured critical information for operational and support use
3. through verification that the information is from trusted sources.

operational missions of United States Special Operations Command and the United States Strategic Command.

2 Joint Functional Area

2.1 Strategic Guidance for Cyberspace Defense

2.1.1 As stated in paragraph 1.2.2, the FAA was initiated by analyzing strategic documents to find references and priorities to cyberspace. The analysis quickly revealed national leaders have identified cyberspace as a new operational domain. The leaders have also increased the priority for cyberspace security and our ability to maintain cyberspace operational superiority. For instance, the 2006 QDR included a new domain, cyberspace, to protect and defend along with air, land, maritime, and space.³ In addition, the National Defense Strategy written in 2005 also highlighted the increased priority of cyberspace by noting:

“Our ability to operate in and from the global commons—space, international waters and airspace, and cyberspace—is important.”⁴

2.1.2 The National Defense Strategy goes on to clearly single out cyberspace as a “new theater of operations.”⁵ Then the strategy directly links cyberspace with Information Operations and indicates:

“Consequently, Information Operations (IO) is becoming a core military competency. Successful military operations depend on the ability to protect information infrastructure and data. Increased dependence on information networks creates new vulnerabilities that adversaries may seek to exploit. At that time, an adversary’s use of information networks and technologies creates opportunities for us to conduct discriminate offensive IO as well. Developing IO as a core military competency requires fundamental shifts in processes, policies, and culture.”⁶

The fundamental shifts mentioned by the National Defense Strategy to reorganize United States assets and operate securely in cyberspace are significant. The shifts will posture our military and federal organizations in order to synchronize operations and ensure our cyberspace defensive capabilities are utilized adequate and effectively.

2.1.3 According to the Joint Chiefs of Staff, “Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.”⁷ This definition describes an incredibly complex domain that crosses multiple organizations, agencies, and institutions. In

³ Quadrennial Defense Review, 2006, pg 37

⁴ National Defense Strategy, March, 2005, pg 13

⁵ National Defense Strategy, March, 2005, pg 13

⁶ National Defense Strategy, March, 2005, pg 13

⁷ National Military Strategy for Cyberspace

addition, not all are military and federal. There are many that are civilian, commercial, medical, etc..., that could cripple our national security if compromised by an adversary. Military organizations must be able to share information as required with trusted federal and national security entities. This information sharing must be defended against compromise or attack for both intended and unintended instances.

2.1.4 The 2006 QDR increased the complexity of the cyberspace domain by including the need to work with our international allies and coalition partners in cyberspace. It directly calls out cyberspace as a multi-national priority along with Weapons of Mass Destruction (WMD) by stating:

“Concepts and constructs enabling unity of effort with more than 70 supporting nations under the Proliferation Security Initiative should be extended to domains other than WMD proliferation, including cyberspace, as a priority.”⁸

The emphasis shows how important cyberspace is from a multi-national perspective and foreshadows how our national leadership will focus on multinational cyberspace operational efforts in the future.

2.1.5 The 2006 QDR continues with more than just identifying cyberspace as a new domain. For instance, it explains that terrorists “exploit the Internet as a cyber-sanctuary, which enables the transfer of funds and the cross-training of geographically isolated cells.”⁹ The QDR also discusses how:

“China is likely to continue making large investments in high-end asymmetric military capabilities, emphasizing electronic and cyber-warfare...for employment by the Chinese military and for global export.”¹⁰

This is not just the Internet; the electronic capabilities China and other countries are creating utilize the entire electronic spectrum. Thus, cyberspace defense must encompass the defense of the entire cyberspace theater of operations.

2.1.6 Another strategic document that discusses the importance for cyberspace defense is The National Strategy to Secure Cyberspace (NSSC). Written in February 2003, it is an implementing component to the National Strategy to Homeland Security.¹¹ It provides the overarching guidance for protecting Cyberspace. The document identifies the Department of Defense as the lead agency for cyberspace defense of the national defense industrial base. In addition, the strategy provide “Critical Priorities for Cyberspace Security” as follows:

⁸ 2006 QDR, pg 88-89

⁹ 2006 QDR, pg 21

¹⁰ 2006 QDR, pg 29-30

¹¹ National Strategy for Homeland Security, July 2002

1. A National Cyberspace Security Response System
2. A National Cyberspace Security Threat and Vulnerability Reduction Program
3. A National Cyberspace Security Awareness and Training Program
4. Securing Governments' Cyberspace
5. National Security and International Security Cooperation¹²

The five priorities provide a glimpse of what is ahead for professionals defending cyberspace. Likewise, the priorities provide a compass for DoD cyberspace defenders to direct their efforts. The strategy is another solid example of many to depict the importance of cyberspace defense and the strategic importance of controlling the cyberspace high ground.

2.1.7 As our adversaries continue to build cyberspace capabilities to achieve strategic military objectives, the United States will have to create an effective counter by fundamentally shifting our military and civilian assets. The shifts must provide for fully integrated synchronization with respect to military operations in support of military objectives and military assistance to federal authorities and agencies when required.

2.1.8 Ultimately, our national leadership realizes the importance of defending the cyberspace operational and strategic high ground. The virtual and asymmetric challenges in cyberspace open up a multitude of holes that can weaken our resolve and national security if not rigorously defended. As a nation, we must develop an overall cyberspace defense capability to include how the military integrates with agencies and departments to protect vital information from enemies abroad and secure our homeland internally.

2.1.9 As the strategic documents show, cyberspace is more than a domain America utilizes to increase efficiency and improve processes; it is a strategic high ground for critical systems and infrastructure. The domain provides a medium where the war can literally impact homes and work places. It can be used to cripple a nation's ability to perform life sustaining functions and topple a nation's ability to maintain stability if not adequately defended.

2.2 Joint Capability Areas (JCA)

2.2.1 There are currently 21 Tier-1 JCAs approved by the Secretary of Defense. Each Tier-1 JCA includes collection of similar capabilities, grouped at a high level to support decision-making, capability delegation, and analysis.¹³ Cyberspace defense is inherent across a number of the Tier 1 JCAs including:

- Joint Access and Access Denial Operations
- Joint Maritime/Littoral Operations
- Joint Space Operations
- Joint Command and Control
- Joint Net-Centric Operations
- Joint Interagency/IGO/MN/NGO Coordination
- Joint Public Affairs Operations
- Joint Information Operations

¹² The National Strategy to Secure Cyberspace, February 2003

¹³ Joint Capability Document for Net-Centric Operational Environment, 10 Jul 2006

Joint Protection
Defensive Support of Civil Authorities
Joint Battlespace Awareness
Joint Force Generation
Joint Force Management
Joint Homeland Defense
Joint Global Deterrence
Joint Shaping
Joint Stability Operations
Joint Special Operations and Irregular Warfare

The fact cyberspace defense impacts such a wide cross section of our JCAs, is eye-opening and makes cyberspace defense increasingly more significant. Our military is evolving to perform all mission aspects through the cyberspace domain and can not afford to lose ground on the cyberspace front. Across the board, a fundamental shift will have to take place over time to embrace cyberspace defense as more than just a support operation. Cyberspace operators will have to become truly joint warriors and directly integrate into all missions.

2.3 Joint Operating Concepts

2.3.1 Deterrence Operations Joint Operating Concept (DO JOC)¹⁴

2.3.1.1 The DO JOC highlights the increasing advantages asymmetric cyberspace threats can utilize against our technology advance systems and capabilities. The document notes:

“The emergence of advanced capabilities and technologies such as computer network attack or directed energy weapons may permit future adversaries to achieve objectives once attainable only via the use of WMD.”¹⁵

Both computer network attack and directed energy threats fall directly in the cyberspace defense realm of operations. As we continue to increase our use of technology advanced capabilities we have to grow highly capable cyberspace defenders trained to utilize cyberspace capabilities in joint operational environments as well as trained on how to defend our joint/coalition operations and information from network attack, energy weapons, or other cyberspace threats. The statement above is staggering, especially over time, the fact that cyberspace attack can achieve the same proportional effect as WMD just cannot be underemphasized. This simple fact makes the need for fundamental shifts in our military to enable unequivocal cyberspace defense essential.

2.3.1.2 The DO JOC goes on to discuss to support the need of a strong cyberspace defense by not only discussing the vulnerabilities to our forces, but also the vulnerabilities to our society:

“*Vulnerabilities of US Society and Forces*: Free and open societies are uniquely vulnerable to terrorist tactics. Both the US economy and

¹⁴ Deterrence Operations Joint Operating Concept, v2., December 2006

¹⁵ Deterrence Operations Joint Operating Concept, v2., December 2006

US military forces are increasingly dependent on advanced technologies for their significant competitive advantages. While this technological superiority yields tremendous capabilities it also creates potential vulnerabilities that adversaries might exploit. Advanced cyberspace warfare capabilities, capabilities to disable space systems, and electromagnetic pulse weapons could all provide adversaries means of undermining potentially decisive US advantages. In addition, both state and non-state actors will have significant abilities to conduct devastating covert attacks on the US population, infrastructure, forces, and overseas interests. US deterrence strategy needs to take these potential US vulnerabilities fully into account, eliminating them where feasible, and compensating for them when necessary.”¹⁶

The text foreshadows the impact of failing to defend the cyberspace domain from terrorists and adversaries. Our ability to maintain national security, sovereignty, economic strength, and freedom will be significantly impacted if we wait too long to fundamentally adjust.

2.4 Joint Functional Concepts

2.4.1 Protection Joint Functional Concept

2.4.1.1 The protection joint functional concept defines force protection as being “composed of a variety of active and passive measures (e.g., weapons, armor, camouflage, stealth, pre-emption, deception, etc.) in the air, land, sea, space and cyberspace domains.” This force protection will be accomplished “through the scaled and tailored selection and application of multi-layered, active and passive, lethal and non-lethal measures, within the air, land, sea, space and cyberspace.”¹⁷ Cyber defense of the joint force’s information, infrastructure, and systems is critical to the protection of the joint force.

2.4.1.2 The functional concept further develops the conduct of protecting information as “the interaction of the force operations activities related to sensing, understanding, deciding, and executing the tasks necessary to ensure that cyberspace attacks are avoided, neutralized or mitigated.”¹⁸ These operations activities and how they relate to computer network defense are:

2.4.1.3 Detect

2.4.1.4 The ability to collect timely and accurate data/information regarding adversary capabilities is a vital capability of protection. Our ability to detect in the future is inextricably tied to predictive intelligence, focusing our detection efforts and optimizing where to look.¹⁹

¹⁶ Deterrence Operations Joint Operating Concept, v2., December 2006

¹⁷ Protection Joint Functional Concept, 30 June 2004

¹⁸ Protection Joint Functional Concept, 30 June 2004

¹⁹ Protection Joint Functional Concept, 30 June 2004

2.4.1.5 Assess

2.4.1.6 Develop an understanding of the situation and accurately identify adversary capabilities that can be used against friendly personnel, physical assets, and information and precisely derive adversary courses of action, planned or employed, with the intent to destroy, or disrupt, operational readiness. Additionally, begin development of a course (or courses) of action, and orders for execution that will allow the JF to react to actionable intelligence regarding adversary plans and actions.²⁰

2.4.1.7 Warn

2.4.1.8 The ability to execute detailed contingency planning and preparation is a fundamental aspect of the protection process. Desired capabilities in 2015 include a robust C2 system that provides the effective means to coordinate the execution of plans, global warning based on focused detection, predictive intelligence and a network of dissemination systems in real time—thus driving the requirement for cyber defense of information, infrastructure and systems.²¹

2.4.1.9 Defend

2.4.1.10 The ability to execute a selected course of action to resist hostile actions directed against friendly personnel, physical assets, and information in order to preserve operational capabilities. Protection is characterized by the execution of those multi-layered, active and passive, measures/actions that resist hostile actions directed against friendly personnel, physical assets, and information in order to preserve operational capabilities.²²

2.4.1.11 Recover

2.4.1.12 Actions taken during, or after a hostile attack to restore friendly personnel, physical assets, and information to full operational readiness. Recovery will span reconstitution efforts for forces deployed, assistance in managing the consequences of an attack at an installation, conducting military support to designated civilian authorities and agencies, and when applicable, recovery of isolated personnel and/or equipment, and rapid repositioning.²³

2.4.1.13 The functional concept continues to describe national cyberspace defense as "all defensive measures of homeland defense taken to detect, deter, defeat, or nullify hostile cyberspace threats against US territory, domestic population, and defense critical infrastructure. Note: only encompasses defensive Information Operations (IO), particularly information protection."²⁴

2.4.2 Focused Logistics Joint Functional Concept

²⁰ Protection Joint Functional Concept, 30 June 2004

²¹ Protection Joint Functional Concept, 30 June 2004

²² Protection Joint Functional Concept, 30 June 2004

²³ Protection Joint Functional Concept, 30 June 2004

²⁴ Protection Joint Functional Concept, 30 June 2004

2.4.2.1 This functional concept notes that the logistics pipeline, from end to end, will be a lucrative target for enemy attack, as deployment and sustainment data are transmitted via cyberspace and will be subject to cyberspace attack.²⁵ The logistics community continues to forge ahead with increasing numbers of cyberspace initiatives, such as radio frequency identification tags on cargo pallets, that place the military's logistics trains at increasing risk to cyberspace attack.

2.4.3 Net-Centric Environment Joint Functional Concept

2.4.3.1 This functional concept highlights the importance of the cyberspace domain's ability to maintain service and survive an attack: "Once deployed, the network must be able to maintain service while under both physical attack and information attack. It should degrade gracefully, that is, continue operations at a gradually reduced capacity in accordance with prioritization plans as systems/equipment are destroyed and/or damaged. The network must be capable of dynamically rerouting services as nodes are incapacitated and/or as information flow requirements change. The network must be capable of obtaining additional resources as required to maintain or increase capacity."²⁶

2.4.3.2 Helpfully, the concept notes that the over-reliance on information and communications technologies may result in forces incapable of operating effectively in the absence of those technologies due to failure or attack. To mitigate this concern, the joint force can increase reliability of new equipment and develop appropriate levels of integrated redundancy in system architectures. Further, training and exercises that realistically simulate conditions of failure and attack are critical to effective joint capability development.²⁷

2.4.4 Force Management Joint Functional Concept

2.4.4.1 This functional concept defines functional modularity to include "human and technical assets fulfilling the same roles while operating in the same primary functional domain and operating to the same standards of practice, proficiency, and lexicon. Primary functional domains include: space, air, land, sea, undersea and cyber environments."²⁸ Cyberspace defense is critical to employing the constellation net's information sharing capabilities.

2.5 Current Cyberspace Defense Related Operations

2.5.1 There are a multitude of current operations being conducted as part of cyberspace defense. At this time, the preponderance of forces and operations is supported by and supporting USSTRATCOM under the Computer Network Defense (CND) mission. As the DoD lead for CND, USSTRATCOM has delegated the responsibility to Joint Task Force Global Network Operations (JTF-GNO). The overall CND operation is directed by JTF-GNO to all other COCOMs and Services. JTF-GNO is the operational interface between DoD and other federal entities and civilian organizations. With respect to defense, JTF-GNO concentrates on CND and

²⁵ Focused Logistics Joint Functional Concept, December 2003

²⁶ Net-Centric Environment Joint Functional Concept, 7 April 2005

²⁷ Net-Centric Environment Joint Functional Concept, 7 April 2005

²⁸ Force Management Joint Functional Concept, 2 June 2005

does not have a full cyberspace defense scope or capabilities to fully defend all of DoD cyberspace.

2.5.2 Each military service and Combatant Command has non-standardized constructs for C2 and defense of cyberspace assets. They concentrate on CND operations separately and report status back to JTF-GNO. The CND tactics are handled by each service independently and the non-standard approach hinders our ability to synchronize cyberspace defense operations. There are joint policies and procedures in place for reporting, and there are processes to follow for nominating joint tactics.

2.5.3 The training of cyberspace professionals is also handled by each individual service and organization. Virtually all cyberspace professionals are trained by their respective organization on how to operate, maintain, and secure the cyberspace infrastructure. However, there are no joint schools for training professionals on cyberspace defense. The DoD currently addresses cyberspace like all other domains where each respective service is responsible for organizing, training, and equipping themselves to operate.

2.5.4 Other than tools and systems for cyberspace reporting, the joint community has not identified joint tools and systems that are mandated for cyberspace defense. Each service and COCOM monitors their respective portions of the cyberspace theater independently. This makes correlation of attacks and outages difficult and hinders our ability to identify coordinated attacks then recover.

2.5.5 Currently, there is no traffic monitoring service for Cyberspace. If a joint entity is under a cyberspace attack, coordination of response activities is very ad hoc, where the level of perceived impact determines the methodology. Additionally, there is currently no process for informing other entities as to the integrity of systems. A relevant example would be AFIT & AFRL communications, where for instance AFIT's e-mail is down, the NetOps center at WPAFB is informed that the system is down, however there is no communication to AFRL that AFIT's e-mail is down.

2.5.6 There are many other organizations throughout the DoD working independently to secure cyberspace assets. They rely on different standards, capabilities, knowledge, training, etc. The cyberspace defense concept will help overcome this significant problem and allow our cyberspace defense capabilities to evolve along with our technology advanced systems.

2.5.7 As we continue to become more technology advance and reliant, the impact of cyberspace attacks and problems will impact our ability to operate more and more. As the United States military, agencies, civilian companies, etc continue to develop architectures and

integrated systems, it will be more and more important for us to have an evolving cyberspace defense force. In addition, we are faced with many pressures which have changed how we fight:

We fight joint, and we are still trying to figure out what that means
We fight coalition, and we make that happen on a case by case basis
Our adversaries tactics and target profiles are changing more and more²⁹

3 Required Capability

3.1 Functional Area Analysis (FAA) Report

3.1.1 Cyberspace is an emerging strategic domain and documentation of Required Capabilities is neither well defined nor standardized. The team identified five tasks during FAA and, using the Universal Joint Task List (UJTL) as a reference, identified over 200 existing Measures of Effectiveness (MOE) to support these tasks. These UJTL MOEs have been consolidated into MOEs supporting four of these tasks listed in the tables below. The linkages between these measures and the UJTL are provided in the Correlation Matrix in Appendix A. The fifth task, Defend Critical Cyberspace Infrastructure, is not covered in the scope of this document.

3.1.2 The team identified four categories of information systems and data, dubbed Information Categories (InfoCAT), used as a condition to appropriately tailor specific Cyberspace Defense measures. The InfoCAT definitions are as follows:

InfoCAT-A - Information Systems used to operate DoD Weapon Systems
InfoCAT-B - Information Systems certified to processing Top Secret data
InfoCAT-C - Information Systems certified to processing Secret data
InfoCAT-D - Information Systems certified to processing Unclassified data

3.1.3 As noted previously, there is no standardized DoD-wide construct for Cyberspace. Likewise, there is no standard set of metrics that can be used to determine current performance or be used as a baseline to set standards for the measures identified below. Thus, the standards of performance listed in this document are based on initial SME judgment with any ambiguity clarified in the MOE summary in Appendix A.

3.2 Defend Cyberspace Information and Information Systems

3.2.1 This task quantifies the ability to detect and defend against Cyberspace attacks, investigate and report on their impacts, and to accomplish recovery actions. The Cyberspace domain is unique in its definition of 'attack'. Attacks include any attempt to disrupt, damage, or

²⁹ Architecture 101 briefing, Titcombe, Matthew A.

destroy information systems or data. Attacks can be launched from anywhere in the world and range from criminal activity to acts of war.

Task 1: Defend Cyberspace Information & Information Systems			
MEASURE		INFOCAT	STANDARD
M1-1	Percent Of Cyberspace Attacks Successfully Defended	A	99.99%
		B	99.9%
		C	99.5%
		D	99%
M1-2	Time To Investigate & Report Impact, Post-Attack	A	30 Minutes
		B	60 Minutes
		C	120 Minutes
		D	480 Minutes
M1-3	Time To Recover, Post-Attack	A	5 Minutes
		B	15 Minutes
		C	60 Minutes
		D	240 Minutes

Table 1: Measures to Defend Cyberspace Information and Information Systems

3.3 Command and Control of Cyberspace Defense

3.3.1 This task defines the need to maintain real-time Command & Control of the entire Cyberspace Domain (joint, allied, critical defense infrastructure, etc). This includes maintaining situational awareness of DoD network status worldwide, identifying and responding to major attacks, directing response actions, coordinating with external agencies, etc.

Task 2: Command & Control of Cyberspace Defense			
MEASURE		INFOCAT	STANDARD
M2-1	Maintain Cyberspace Situational Awareness	All	Yes/No
M2-2	Convene Cyberspace Threat Conference To Direct Attack Response Actions	All	Yes/No
M2-3	Time To Notify Users Of New Attacks/Threats/Countermeasures	A	5 Minutes
		B	5 Minutes
		C	10 Minutes
		D	10 Minutes
M2-4	Time To Notify Users Of Known Vulnerabilities/Responses	A	4 Hours
		B	4 Hours
		C	6 Hours
		D	6 Hours

Table 2: Measures for Command & Control of Cyberspace Defense

3.4 Organize, Train and Equip Cyberspace Personnel

3.4.1 This task defines those core activities that personnel must perform to ensure that the cyberspace defense concept is executed appropriately. Organize, train and equip cyberspace personnel is necessary as the information systems being defended do not always have the capability to automatically respond to an attack, and that in addition the human in the loop creates the environment in which these systems are used. The essence of this task is to develop and execute joint standards and processes for defensive measures while providing the required personnel.

Task 3: Organize, Train and Equip Cyberspace			
MEASURE		Info Cat	STANDARD
M3-1	Perform Standards Verification	All	Yes/No
M3-2	Percent of Trained Cyber/Information Operations Personnel	A	98%
		B	98%
		C	98%
		D	98%
M3-3	Provide Cyberspace Defense Plans	All	Yes/No

Table 3: Measures to Organize, Train and Equip Cyberspace

3.5 Test and Acquire Cyberspace Systems:

3.5.1 As a capability, test and acquire cyberspace systems defines those activities related to the assurance that the information systems being used by all members of the joint community will meet current and/or future cyberspace defense standards. This task includes such activities as establishing baseline defensive requirements like availability and interoperability into new information systems before they become operational.

Task 4: Test and Acquire Information Systems			
MEASURE		Info Cat	STANDARD
M4-1	Percent of Information Systems Meeting Availability Standards	A	99.99%
		B	99.9%
		C	99.5%
		D	99%
M4-2	Percent of Information Systems Meeting Interoperability Standards for Cyberspace Defense	A	99.99%

Table 4: Measures to Test and Acquire Information Systems

4 Capability Gap

4.1 As noted previously, there is no standardized, DoD-wide construct for cyberspace defense. Thus, a comprehensive and quantitative analysis of current cyberspace defense capabilities is required to adequately assess our current performance. Current documentation, however, does reveal numerous qualitative capability gaps. The team ended identifying eleven capability gaps listed in Table 5. For a prioritized list of these gaps, refer to Table 6 in the Recommendations section of this document.

Task 1: Defend Cyberspace Information & Information Systems		
MEASURE		IDENTIFIED GAP
M1-1	Defend Against Cyberspace Attacks	There are shortfalls with the capabilities to protect the integrity of information, and information systems from external and internal threats in cyberspace
Task 2: Command & Control of Cyberspace Defense		
MEASURE		IDENTIFIED GAP
T2	C2 of Cyberspace Defense	There is no effective joint standardized Command and Control (C2) tactics process and organization for service, joint, coalition, and national cyberspace defense.
M2-1	Maintain Cyberspace Situational Awareness	There is no centralized ability to obtain or maintain cyberspace situational awareness over joint and national critical defense infrastructure, information, and information systems.
M2-2 and M2-3	Convene Cyberspace Threat Conference to Direct Attack Response Actions	There is a lack of capability to synchronize cyberspace defensive actions and operations in real-time with Combatant Commander (COCOM), National Security, and Homeland Defense operations.
M2-4	Notify users of known vulnerabilities/responses	There is no capability to immediately notify Services, COCOMs, National Security organizations, and Homeland Security organizations of cyberspace emergencies.
M2-4	Notify users of known vulnerabilities/responses	There is no capability to share lessons learned between Service, COCOM, National Security, and Homeland Security cyberspace operators.
Task 3: Organize, Train and Equip Cyberspace		
MEASURE		IDENTIFIED GAP
M3-1	Perform Standards Verification	The standards that exist are very system-specific; there are no overarching joint standards for cyberspace defense evaluation.
M3-2	Systems with Trained Cyber/Information Operations Personnel	There is no joint cyberspace defense school for training personnel to protect and defend cyberspace information and systems in joint and multinational environments.

M3-3 and M3-4	Provide cyberspace defense plans	There is a lack of capability to adequately plan cyberspace defensive actions with wartime, contingency, and disaster plans for COCOMs, National Security organizations, and Homeland Security organizations.
		There are inconsistent policies for protecting end-to-end availability and assured access to cyberspace information, resources, and systems.
Task 4: Test and Acquire Information Systems		
MEASURE		IDENTIFIED GAP
M4-2	Establish Cyberspace Defense Interoperability Standards for Information Systems	There is no structured joint approach for developing standardized and interoperable cyberspace defense qualities, aspects, features, and requirements in information systems.

Table 5: Capability Gaps

5 Threat and Operational Environment

5.1 The DoD’s reliance on technology has dramatically changed the way we fight wars, work with allies, coalitions, agencies, and homeland security. Cyberspace technology has literally allowed us to reduce the size of our forces to the point that we bring overwhelming technological might to bear on our adversaries instead of overwhelming manpower might. Our focus in cyberspace has primarily been on making us capable of doing more with smaller forces and more advanced equipment. Doing so continues to make us more and more vulnerable in the cyberspace theater of operations. As we evolve, it can be reasonably stated that an adversary could bring our country to its knees if they take control of cyberspace and dominate the cyberspace domain.

5.2 The cyberspace domain continues to become a more relevant operational and strategic high ground. Therefore it is critical that cyberspace defense is a priority to allow us to maintain the cyberspace high ground and adequately defend our information and information systems. The threat is real and our national leaders are engaging to make sure we are ready. To quote The National Strategy to Secure Cyberspace (NSSC):

“Our economy and national security are fully dependent upon information technology and the information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same Internet that today connects millions of other computer networks making most of the nation’s essential services and infrastructures work. These computer networks also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars, and stock

markets, all of which exist beyond cyberspace. A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security.

The required technical sophistication to carry out such an attack is high—and partially explains the lack of a debilitating attack to date. We should not, however, be too sanguine. There have been instances where organized attackers have exploited vulnerabilities that may be indicative of more destructive capabilities. Uncertainties exist as to the intent and full technical capabilities of several observed attacks. Enhanced cyber threat analysis is needed to address long-term trends related to threats and vulnerabilities.

What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving. In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping U.S. information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access.

In wartime or crisis, adversaries may seek to intimidate the Nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems. Cyber attacks on United States information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life.”

Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures.³⁰

The citation is a sobering reality for how failing to ensure superiority over the cyberspace domain can cripple our ability to maintain national security and the welfare of Americans. The note that “the required technical sophistication to carry out such an attack is high—and partially explains the lack of a debilitating attack to date”³¹ shows that as our adversaries increase their technical sophistication, we too must increase our cyberspace defense readiness and capability.

6 Recommendation

³⁰ The National Strategy to Secure Cyberspace, February 2003

6.1 It is critical to examine a deeper analysis of existing cyberspace capabilities, standards, tactics, techniques and procedures to develop a better set of measures of effectiveness and performance. We examined the capability gaps and priorities in the NSSC, and based our capability prioritization on the NSSC strategic priorities to secure cyberspace. The prioritized capability gap list is shown in Table 6 below.

6.2 Furthermore, we looked at our own experiences, came up with an overall prioritized capability gap list for the DoD cyberspace community. The FINAL column of Table 6 shows our final priority for each capability gap. These capability gaps should act as a catalyst to execute a DOTMLPF analysis and an overall analysis of alternatives to determine if a number of Initial Capabilities Document and/or DCRs are appropriate meet NSSC priorities.

Prioritized Capability Gaps				
FINAL	NSSC	MEASURE		IDENTIFIED GAP
1	1	T2	C2 of Cyberspace Defense	There is no effective joint standardized Command and Control (C2) tactics process and organization for service, joint, coalition, and national cyberspace defense.
2	1	M2-1	Maintain Cyberspace Situational Awareness	There is no centralized ability to obtain or maintain cyberspace situational awareness over joint and national critical defense infrastructure, information, and information systems.
3	1	M2-2	Convene Cyberspace Threat Conference to Direct Attack Response Actions	There is a lack of capability to synchronize cyberspace defensive actions and operations in real-time with Combatant Commander (COCOM), National Security, and Homeland Defense operations.
4	1	M2-3	Time To Notify Users Of New Attacks/Threats/Countermeasures	There is no capability to immediately notify Services, COCOMs, National Security organizations, and Homeland Security organizations of cyberspace emergencies.
5	2	M2-4	Notify users of known vulnerabilities/responses	There is no capability to share lessons learned between Service, COCOM, National Security, and Homeland Security cyberspace operators.
6	3	M3-2	Systems with Trained Cyber/Information Operations Personnel	There is no joint cyberspace defense school for training personnel to protect and defend cyberspace information and systems in joint and multinational

³¹ The National Strategy to Secure Cyberspace, February 2003

				environments.
7	4	M1-1	Defend Against Cyberspace Attacks	There are shortfalls with the capabilities to protect the integrity of information, and information systems from external and internal threats in cyberspace
8	4	M3-3	Provide cyberspace defense plans	There are inconsistent policies for protecting end-to-end availability and assured access to cyberspace information, resources, and systems.
9	5	M4-2	Establish Cyberspace Defense Interoperability Standards for Information Systems	There is no structured joint approach for developing standardized and interoperable cyberspace defense qualities, aspects, features, and requirements in information systems.
10	5	M3-1	Perform Standards Verification	The standards that exist are very system-specific; there are no overarching joint standards for cyberspace defense evaluation.
11	5	M3-3	Provide cyberspace defense plans	There is a lack of capability to adequately plan cyberspace defensive actions with wartime, contingency, and disaster plans for COCOMs, National Security organizations, and Homeland Security organizations.

Table 6: Prioritized Capability Gaps

6.3 The Functional Solutions Analysis (FSA) and Analysis of Alternatives should complete a review of the prioritized capability gaps and tasks. Then, a broad review of military organizations performing these tasks should be performed. The review would ensure we understood the operational domain better and allow us to make a better determination of how to effectively defend cyberspace. After the review of the military organizations, efforts should focus on how to bring these organizations together to work cohesively and in synchronization to defend cyberspace. It is just a matter of time before our enemies are able to use cyberspace in a way that can tremendously degrade our ability to maintain our dominant force in the world. The US military must press now and push forward to establish a fully capable cyberspace defense force.

AppendixA Cyberspace Defense Tasks and Measures of Effectiveness Analysis

Rolled-up Cyber Defense Measures and suggested corresponding units.
 Generic Conditions for each measure are provided in section 3.1.2

Task 1. Defend Cyberspace Information & Systems

MOE	MOE Title	Description	Unit
M1-1	Percent of Cyberspace attacks successfully defended	# of defended attacks/# of total attacks	Percent
M1-2	Time to Investigate & Report Impact, Post-Attack	Interval is time from the completion of the attack, to the successful release of post-attack report	Minutes
M1-3	Time to Recover, Post-Attack	Interval is time from the completion of the attack, to reestablishment of fully operational capability	Minutes

Task 2. Command and Control of Cyber Defense

MOE	MOE Title	Description	Unit
M2-1	Maintain Cyberspace Situational Awareness	Yes/No criteria applies to each IS in each condition, resulting in an individual system comply/non-comply for awareness	Yes/No
M2-2	Convene Cyberspace Threat Conference to Direct Attack Response Actions	Compliance unit, only appropriate if specific threat warrants	Yes/No
M2-3	Time to notify users of known Attacks/Threats/Countermeasures	Interval is time of awareness of threat by central authority to time of distribution of information to users	Minutes
M2-4	Time to notify users of known vulnerabilities/Responses	Interval is time of awareness of vulnerability by central authority to time of distribution of information to users	Hours

Task 3. Organize, Train, and Equip Cyberspace

MOE	MOE Title	Description	Unit
M3-1	Perform Standards Verification	Yes/No criteria applies to each IS in each condition, resulting in an individual system comply/non-comply	Yes/No
M3-2	Percent of Trained Cyber/Information Operations Personnel	# trained and available personnel/ # of needed personnel	Percent
M3-3	Provide Cyberspace Defense Plans		Yes/No

Task 4. Test and Acquire Secure Information Systems

MOE	MOE Title	Description	Unit
M4-1	Percent of Information Systems meeting Availability Standards	# meeting availability standards/# total IS	Percent
M4-2	Percent of Information Systems meeting Interoperability Standards for Cyberspace Defense	# meeting interoperability standards/ # total IS	Percent

Tasks and Measures on this sheet Support the "Defend Cyber Information Systems" master Task					
UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure
SN 2.5.3	Provide Sensitive Compartmentalized Information (SCI) Networks for the Intelligence Community	Provide Joint Worldwide Intelligence Communications System (JWICS).	System is fully operational.	Percent/Time	M4-1
SN 3.4.6	Coordinate Protection of National Strategic Information, Information-Based Processes, and Information Systems	To coordinate the protection of information, information-based processes, and information systems by planning and implementing comprehensive defensive information operations (IO) measures.	Of confirmed loss of classified data from penetrations.	Instances	M1-2
			Of detected penetrations of command information systems.	Instances	M1-1
			Of time, command joint information systems down.	Percent	M4-1
			To switch to an alternate system after attack on major information system.	Minutes	M1-3
			To restore major information system after attack.	Minutes	M1-3
			To detect attempted penetration of information system.	Minutes	M1-1
			Of penetrations of multiple command information systems.	Instances	M1-1

SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Of operational C4 networks and nodes available.	Percent	M4-1
			Of operational C4 networks and nodes reliable.	Percent	M4-1
			To restore information systems to fully operational status after a successful penetration and attack.	Percent	M1-3
			Of time available for nuclear command control (NC2) C4I systems to transmit situation monitoring tactical warning and attack assessment (TW/AA) messages within established guidelines.	Percent	M3-1
SN 5.1.2.1.3	Provide Global Internet Protocol (IP)-Based Networks for Classified and Unclassified Information	To provide interoperable, secure IP data communications services.	Of access circuit availability.	Percent	M4-1
			Of access circuit quality of service - latency.	Percent	M4-1
			Of access circuit quality of service - packet loss rate.	Percent	M4-1
			To provision/implement services.	Days	M4-1
			Of satellite constellation availability.	Percent	M4-1

SN 5.1.2.1.4	Provide Global Communications and Networks for Video Services	To provide global video service capabilities, ranging from network delivery of video of live events and real time video communications sessions among people who are geographically dispersed to delivery of video from prerecorded video files.	Of video services network availability.	Percent	M4-1
			Outages of video services network that impact a general/flag officer-level video teleconferencing session.	Yes/No	M4-1
SN 5.1.2.1.7	Provide Community of Interest Global Networks for the Department of Defense	Provide community of interest (COI) networks to select users. COI are sets of users who have shared goals, shared interests, shared mission or business processes, and agreed-upon terms of behavior.	Of community of interest access circuit availability.	Percent	M4-1
			Of community of interest access circuit quality of service - latency.	Percent	M4-1
			Of community of interest access circuit quality of service - packet loss rate.	Percent	M4-1
			Community of interest bandwidth available.	Yes/No	M4-1
			To provision/implement services.	Days	M4-1
SN 5.5	Coordinate Worldwide Information Operations	To coordinate the elements of offensive and defensive IO	Of US national-level IO plans or objectives being delayed, defeated, or disrupted due to adversary offensive IO actions.	Instances	M1-2

SN 5.5.2	Conduct Defensive Information Operations	To perform authorized actions to protect, monitor, analyze, detect, and respond to unauthorized activity within national security information systems and computer networks	To identify qualified personnel, determine availability of equipment, and initiate technical surveillance service of customers.	Days	M3-2
			To identify analysis team required to perform network evaluations.	Days	M3-2
			To complete network evaluations after team identification.	Days	M2-1
			To assess customer network security posture.	Days	M2-1
			To provide network security assessment to customer.	Days	M3-1
SN 5.5.3	Provide Regional NetOps to Support the Global Information Grid (GIG)	Execute GIG NetOps and defense.	Capabilities measured in subtasks linked to selected combatant command OPLANS	Yes/No	M1-1
SN 5.5.3.1	Provide Network Management for the Theater Information Grid (TIG) Transport and Computer Network Infrastructures	Equip, train, maintain, and sustain the theater-level NetOps centers to enable them to manage and control the command, control, communications, computer systems, and networks, including space systems that define the TIG transport infrastructure within their AOR.	Heating and air conditioning systems are available/operational to enable the TNC to accomplish NETOPS S&NM missions.	Yes/No	Infrastructure
			Power, generators, and grounding systems are available/operational to enable the TNC to accomplish NETOPS S&NM tasks.	Yes/No	Infrastructure

SN 5.5.3.2	Protect and Defend the Theater Information Grid (TIG)	To collect and consolidate TIG intrusion detection reports and data, assessing the compiled data, and reporting the results to the appropriate command authorities.	To alert TIG users and the Global NetOps Center (GNC) to presence of critical information assurance Information Assurance/Computer Network Defense (IA/CND) events that affect the TIG.	Minutes	M2-3
			Of Information Assurance Vulnerability Alert (IAVA) compliance distribution process for notifying Theater combatant commanders, the Services, and Defense agencies about vulnerability alerts and countermeasures information.	Percent	M2-4
			Of TIG computer assets that are compliant or operating with approved extensions and mitigation plans with negligible risk on information systems capability to perform required theater missions	Percent	M3-1
			Of TIG networks compliant or operating with approved extensions and mitigation plans with negligible risk on information systems capability to perform required theater missions.	Percent	M3-1
			Of TIG IA/CND status information currently available.	Percent	M4-1
ST 5.5	Conduct Theater-Wide Information Operations (IO)	To conduct information operations for implementing the Secretary of Defense's national military strategy, policy, objectives and operations at the theater level.	Are appropriate allied and coalition IO resources and capabilities factored into theater IO plans?	Yes/No	M3-3

			Of mission essential US command, control, communications, computers, and intelligence surveillance and reconnaissance (C4ISR) systems remaining after enemy command and control (C2) attack.	Percent	M1-2
			Of information systems capable of instantaneous detection of hostile attack and incorporating fully automated defend/repair/restore capabilities.	Percent	M1-1
			Of enemy operations disrupted, cancelled, or modified, attributable to IO plan.	Percent	M1-1
ST 6.3.5	Protect Theater Information Systems	To coordinate theater-wide activities to protect and defend information and information systems. This task includes integrating and synchronizing indigenous and joint force capabilities for defensive IO, ranging from technical security measures (such as INFOSEC) to procedural measures (such as counterintelligence, physical security, and hardening of communications nodes).	Do commands responsible for design, operation and maintenance of information systems perform risk assessments of potential IO threats and take appropriate action to respond to those risks that meet the appropriate criteria?	Yes/No	M3-1
			Do commands responsible for design, operation and maintenance of information systems have IA or defensive IO memorandums of understanding with commercial communications providers who support information systems?	Yes/No	M3-1

			Do commands responsible for design, operation and maintenance of information systems use "Red Teams" to identify vulnerabilities in those systems?	Yes/No	M3-1
			Of theater strategic C4I systems not protected by firewalls, virus detection software and other appropriate defensive IO measures.	Percent	M3-1
			Of information system hardware and software components that have backup components to replace them if they fail or are corrupted.	Percent	M3-1
			Of redundant communications paths available to connect information systems.	Number	Solution
			Of information systems being disabled, corrupted or compromised through identified adversary IO actions or criminal mischief.	Instances	M2-1
			For appropriate Computer Emergency Response Teams (CERTs) to respond, identify and correct information system failures attributed to adversary IO action or criminal mischief.	Hours	M3-1
			To restore primary local area network (LAN) in command center.	Hours	M1-3
			Of allies with which joint information security agreements exist.	Percent	M2-1

			Of information systems within high security area.		M2-1
			Of adversary trusted sources (systems and personnel) under friendly control.	Percent	M2-1
			Of adversary penetrations of friendly information systems are identified and targeted	Percent	M2-1
			For Computer Emergency Response Team (CERT) to respond and report attack to the information operations officer (IOO), from notification of attack.	Time	M2-1
			For CERT to implement Information Conditions (INFOCON) Updates, and disseminate information to the command and TFs, from IOO determines INFOCON.	Time	M1-1
			For task forces to implement INFOCON change and report completion status.	Time	M2-1, M3-1
OP 6.3	Protect Systems and Capabilities in the Joint Operations Area	To identify critical information and subsequently analyze friendly actions attendant to planning and conducting campaigns and major operations to identify those actions that can be observed by adversary intelligence systems	Of attempted adversary penetrations of friendly information systems successful.	Percent	M1-1
			Of enemy's sensor coverage known.	Percent	M2-1
			Of information systems within high security area.	Percent	M3-1
			Of command net secured.	Percent	M2-1, M3-1

OP 6	Provide Operational Force Protection	To conserve the force's fighting potential so that it can be applied at the decisive time and place. This activity includes actions taken to counter the enemy's forces by making friendly forces (including operational formations, personnel, etc.), systems, and operational facilities difficult to locate, strike, and destroy.	Of friendly communications hardened or redundant.	Percent	M3-1
			Reduction in friendly LOC capacity.	Percent	M1-2
OP 6.5.3	Protect/Secure Operationally Critical Installations, Facilities, and Systems	To protect operationally critical installations, facilities, and systems from attack in the operational area.	For internal/external reaction force to reach installation or facility under attack.	Hours	M1-3
			Of operations delayed, disrupted, canceled or modified.	Instances	M1-2
			Of terrorists acts against coalition forces in OA.	Instances	M1-2
			Of terrorists acts against US forces in OA.	Instances	M1-2
			Of communications in operational area supporting operation hardened.	Percent	M3-1
			Of communications in operational area supporting operation with alternate paths.	Percent	M3-1
			Of critical friendly facilities (e.g., PODs, command posts) destroyed, damaged, or rendered inoperable by sabotage or insurgents or terrorist actions.	Percent	M1-2
			Of critical friendly facilities hardened or protected against hostile acts.	Percent	M3-1

			Of terrorist attacks penetrate security in operational area.	Percent	M1-2
			Reduction in LOC capacity resulting from enemy attacks.	Percent	M1-2
			To coordinate for additional assets for theater LOCs.	Hours	Solution
			Of threat assessments passed within established criteria.	Percent	M3-1
			Command has established executable antiterrorism program.	Yes/No	M3-1
			Command has established procedures to change force protection conditions.	Yes/No	M3-1
			Command has procedures to respond to terrorist use of CBRNE weapons.	Yes/No	M3-1
			Antiterrorism/security plan is coordinated, approved, and executable.	Yes/No	M3-1
			Compliance with DOD antiterrorism standard.	Yes/No	M3-1

Tasks and Measures on this sheet Support the "Defend Cyber Information****" master Task					
*** After analysis this task was combined with Defend Information Systems Task ***					
UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure

SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Of traffic sent on nondedicated or non-DOD lines or channels.	Percent	M4-1
SN 5.5	Coordinate Worldwide Information Operations	To coordinate the elements of offensive and defensive IO	To modify national-level IO plans and actions due to operational contingencies.	Hours	M3-3
			Of national-level IO cell nominated "targets" struck with lethal or nonlethal means during the timeframe planned for in the IO appendix or other planning document	Percent	Offensive Measure
SN 5.5.1	Conduct Strategic Information Operations	To conduct offensive and defensive IO for implementing Presidential and SecDef national military strategy, policy, objectives, and operations at the strategic level.	To implement measures for full spectrum IO in support of global computer network defense (CND) mission.	Hours	M1-1
SN 5.5.3.2	Protect and Defend the Theater Information Grid (TIG)	To collect and consolidate TIG intrusion detection reports and data, assessing the compiled data, and reporting the results to the appropriate command authorities.	Of unauthorized access (root, user, privileged) to Mission Assurance Category (MAC) I, MAC II, and MAC III systems and networks within the TIG since last reporting period.	Percent	M1-1

ST 1.6.4	Gain and Maintain Information Superiority in Theater	To achieve information superiority by affecting an adversary's information, information-based processes, and information systems, while defending one's own information, information-based processes, and information systems.	Of friendly communications traffic delayed, disrupted, or corrupted by adversary IW/C2W.	Percent	M2-1
			Without significant security breach.	Weeks	M3-1
ST 5.5	Conduct Theater-Wide Information Operations (IO)	To conduct information operations for implementing the Secretary of Defense's national military strategy, policy, objectives and operations at the theater level.	Of US or allied plans or objectives in theater being delayed, defeated, or disrupted due to adversary offensive IO actions.	Instances	M2-1
			To conduct battle damage assessment of IO "targets" struck with lethal and nonlethal means after receipt of information.	Days	M1-2
			Of theater level IO objectives verifiably achieved.	Percent	M2-1
			Delay to operations because of the lack of information security.	Days	M1-2
			To achieve information superiority after crisis onset.	Days	M2-1
ST 5.5.2	Control Theater Information Operations (IO)	To monitor and adjust the theater IO efforts during execution.	To achieve information superiority after crisis onset.	Days	M2-1
OP 6.2.14	Employ Operations Security (OPSEC) in the Joint Operations Area	To employ OPSEC measures to deny critical information necessary by an adversary commander to accurately estimate the military situation.	Before joint force knows of possible compromise of EEFI.	Hours	M2-1
			To develop critical info list from EEFI.	Hours	M2-1

			Of identified friendly vulnerabilities exploited by enemy action.	Percent	M1-2
			Of joint operations disrupted as result of enemy detection and response.	Percent	M1-2
OP 6.3.2	Supervise Communications Security (COMSEC)	To supervise the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.	Of frequency allocation or frequency management failing to prevent signal fratricide.	Instances	M1-2
			Of interceptions of friendly communications during planning and execution.	Instances	M1-2
			Of communications encrypted.	Percent	M3-1
			Of communications sent by secure means.	Percent	M3-1
OP 6.4	Conduct Military Deception in Support of Subordinate Campaigns and Major Operations	To manipulate enemy operational level commander's perceptions and expectations into a false picture of reality that conceals friendly actions and intentions until it is too late for enemy forces to react effectively within the context of the geographic combatant commander's deception plan.	Of EEFI/Critical Information addressed in deception plan.	Percent	M3-3
			Of enemy forces deployed to deal with deception threat.	Percent	M2-1
			Of deception plans not including smoke and obscurants.	Instances	M3-3

TA 5.6	Employ Tactical Information Operations	Tactical Information Operations (TIO) employed by joint services produce tactical information and gain, exploit, defend, or attack information or information systems.	Identified processes have fully integrated all available capabilities to ensure a defense in depth. Should be integrated in all military operations, to include activities by other government and nongovernment agencies or organizations.	Percent	M3-3
			Of friendly operations delayed, disrupted, or degraded due to ineffective tactical information operations.	Percent	M1-2
SN 3.4.4.1	Support Force Protection	To provide assessments which ensure mission survivability to critical facilities by determining single point vulnerabilities, mitigation techniques and/or enhanced force protection postures.	To provide written report of observations/vulnerabilities to the combatant commander with mitigating options.	Days	M2-4
			Of identified defensive measures validated by installation / unit commander to ensure the physical security of personnel, facilities, and equipment.	Percent	Infrastructure
			Of the time Force Protection (FP) enhancement recommendations have been taken to reduce risk from threats to acceptable levels based on FP operational risk assessment.	Percent	M4-2
			To determine FP enhancement processes/procedures/facility modifications, etc and provide "answer" to the combatant commander.	Days	M2-4

			Of required installations receive periodic Force Protection Assistance Visits.	Percent	M3-1
			To respond to combatant command request; complete plans review process.	Months	M3-1
			Of Research and Development (R&D) funding used to meet Defense Technology Objectives (DTOs) in the Scientific and Technical (S&T) Reliance Process to meet current and future requirements.	Percent	M4-1

Tasks and Measures on this sheet Support the "C2 of Cyber Defense" master Task					
UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure
SN 3.4.6	Coordinate Protection of National Strategic Information, Information-Based Processes, and Information Systems	To coordinate the protection of information, information-based processes, and information systems by planning and implementing comprehensive defensive information operations (IO) measures.	Of commands have adequate information processing hardware and software.	Percent	M3-1
			Of commands have current processes and programs to protect information systems, processes, and networks.	Percent	M3-1
			Of commands have fully trained and manned information systems management and operating personnel.	Percent	M3-2

			Of time, command joint information systems down.	Percent	M4-1
			Organization applies resources to protect against IO, detect and react to offensive IO, and restore capabilities should defensive measurers fail.	Yes/No	M1-1, M1-2, M1-3
			To implement countermeasures in response to a confirmed intrusion.	Minutes	M1-1
			To activate a change in information condition (INFOCON) in response to increased threats or actual activity.	Minutes	M2-3
			To switch to an alternate system after attack on major information system.	Minutes	M1-3
			Of penetrations of multiple command information systems.		M1-2
SN 5.1	Operate and Manage Global Strategic Communications and Information Systems	To receive information and data on the strategic situation worldwide, including: combatant command, theater component command, and operational level command missions, disposition of friendly and enemy forces, strategic centers of gravity, and characteristics of the theater areas (worldwide).	To begin transmitting force direction (FD) emergency action message (EAM) to bombers, tankers (positive control launch (PCL) only) (availability of individual Nuclear Command and Control System (NCCS) command, control, communications, computers, and intelligence (C4I) systems).	Minutes	M3-1
			To begin transmitting force management (FM) messages to bombers/tankers/intercontinental ballistic missile('s) (ICBM's) (availability of National Military Command System (NMCS) and combatant commander C4I systems).	Minutes	M3-1

			To begin transmitting FM messages to bombers/tankers/ICBMs (availability of bomber/tanker/ICBM NCCS C4I systems).	Minutes	M3-1
			To begin transmitting situation monitoring (SM), threat warning (TW), and attack assessment (AA) messages (availability of NCCS C4I systems).	Minutes	M3-1
			To begin decision-making conference.	Minutes	M2-2
SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Interact with the NMCS network and nodes to obtain or send strategic information.	Hours	
SN 5.5	Coordinate Worldwide Information Operations	To coordinate the elements of offensive and defensive IO	National-level IO coordination policies and procedures exist.	Yes/No	M3-1
			To identify qualified personnel from various elements and activities and augment national-level IO planning cell after onset of planning requirement.	Hours	M3-3
			To identify required national-level IO information necessary for IO planning after onset of planning.	Hours	M3-3
			To task intelligence community and other national-level support organizations and agencies to fill information requirements for IO planning.	Hours	M3-3

			Of identified national-level IO information requirements unfilled at time-critical points in planning process.	Percent	M3-3
			To get interagency approval for proposed national or subordinate level IO plans and actions.	Days	M3-3
			Of uncoordinated IO actions at different levels (national, theater, AOR) or different theaters causing disruption or delay of US plans and objectives.	Instances	M3-3, M2-1
			Of national-level IO objectives verifiably achieved.	Percent	M2-1
SN 5.5.1	Conduct Strategic Information Operations	To conduct offensive and defensive IO for implementing Presidential and SecDef national military strategy, policy, objectives, and operations at the strategic level.	Of planners with access to the information operations (IO) plan within 12 hours of plan initiation message.	Percent	M3-3
SN 5.5.3.3	Provide a Common Operational Picture (COP)	To provide an integrated capability to receive, correlate, and display, functional and operational pictures of systems and networks and the integrated view(s) of networks that display network health, security status, and information sources.	Of availability of the TIG integrated COP delivery to the GNC.	Percent	M4-1
			Of ESM/NM operations information integrated into the TIG COP.	Percent	M3-3
			Of IA/CND information integrated into the TIG COP.	Percent	M3-3

SN 8.3.5	Coordinate DOD/Government Information Operations (IO)	To work with the Services, combatant commands, and civil/military agencies on issues involving offensive and defensive IO.	Development and approval of information operations.	Yes/No	M4-2
ST 5.5	Conduct Theater-Wide Information Operations (IO)	To conduct information operations for implementing the Secretary of Defense's national military strategy, policy, objectives and operations at the theater level.	To task intelligence community and other theater level support organizations and agencies (including those of allies where appropriate) to fill information requirements for IO planning.	Hours	M3-3
			Of identified theater level IO information requirements unfilled at time-critical points in planning process.	Percent	M3-3
			To get theater level approval for proposed IO plan.	Hours	M3-3
			To respond to subordinate command requests for IO support or coordination.	Hours	M3-3
			Of uncoordinated IO element or activity actions within theater causing disruption or delay of US or allied plans and objectives.	Instances	M3-3
			To modify theater level IO plans and actions due to operational contingencies.	Hours	M3-3
			Of planners with access to the IO plan within 12 hours of plan initiation message.	Percent	M2-3
ST 5.5.1	Plan and Integrate Theater-Wide Information Operation (IO)	To plan theater-wide IOs, integrating military operations and non-DOD USG activities.	Does a theater level IO cell exist?	Yes/No	M3-1

			To task intelligence community and other theater level support organizations and agencies (including those of allies where appropriate) to fill information requirements for IO planning.	Hours	M3-3
			Of identified theater level IO information requirements unfilled at time-critical points in planning process.	Percent	M3-1
			Are appropriate allied and coalition IO resources and capabilities factored into theater IO plans?	Yes/No	M3-3
			To get theater level approval for proposed IO plan.	Hours	M3-3
			To respond to subordinate command requests for IO support or coordination.	Hours	M3-3
ST 5.5.2	Control Theater Information Operations (IO)	To monitor and adjust the theater IO efforts during execution.	Of uncoordinated IO element or activity actions within theater causing disruption or delay of US or allied plans and objectives.	Instances	M1-2
			To modify theater level IO plans and actions due to operational contingencies.	Hours	M1-1, M2-1, M3-3
			Of US or allied plans or objectives in theater being delayed, defeated, or disrupted due to adversary offensive IO actions.	Hours	M1-2
			To conduct battle damage assessment of IO "targets" struck with lethal and nonlethal means after receipt of information.	Days	M2-1
			Of theater level IO objectives verifiably achieved.	Percent	M2-1

			To change IO plan upon receiving status updates to ensure supporting elements of IO plan coordinate actions.	Hours	M3-3
OP 5.6	Coordinate Operational Information Operations (IO)	To coordinate the use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, in order to deny information, influence, degrade, or destroy adversary information, information-based processes, and information systems, and to protect one's own against such actions.	To get JFC approval for proposed operational IO plans and actions.	Hours	M3-3
OP 6.2.14	Employ Operations Security (OPSEC) in the Joint Operations Area	To employ OPSEC measures to deny critical information necessary by an adversary commander to accurately estimate the military situation.	Of information (pieces or types) commander needs to make decision listed as FFIR.	Items	n/a
			Of information (pieces or types) commander needs to make decision listed as PIR.	Items	n/a
			Of information (pieces or types) joint force needed to protect itself listed as EEFI.	Items	n/a
TA 5.6	Employ Tactical Information Operations	Tactical Information Operations (TIO) employed by joint services produce tactical information and gain, exploit, defend, or attack information or information systems.	Actions taken must be appropriate to the situation and consistent with US objectives. They must be permissible under the law of armed conflict, consistent with applicable domestic and international law, and in accordance with applicable rules of engagement.	Percent	M3-1

Tasks and Measures on this sheet Support the "Organize, Train, and Equip" master Task					
UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure
SN 3.4.6	Coordinate Protection of National Strategic Information, Information-Based Processes, and Information Systems	To coordinate the protection of information, information-based processes, and information systems by planning and implementing comprehensive defensive information operations (IO) measures.	Organization applies resources to protect against IO, detect and react to offensive IO, and restore capabilities should defensive measurers fail.	Yes/No	M1-1,M1-2, M1-3
			To detect attempted penetration of information system.	Minutes	M1-2
SN 5.1.1.1	Provide Information Assurance Products and Services	To provide products, services, infrastructure, and capability to assure availability and appropriate application of evaluated/validated products and solutions.	Of fully qualified Information Systems Security Engineers as a percentage of required.	Percent	M3-2
			Of quick response requirements met by existing inventory of equipment and parts stockpiles.	Percent	M3-1
SN 5.1.1.3	Provide Information Assurance Education and Awareness	To prepare individuals, leaders, and organizations to accomplish mission activities in coordination with multination, interagency, nongovernmental, private voluntary and United Nations (UN) agencies/forces/organizations. This task applies to providing guidance on national information assurance (IA) policy and foreign information exchange.	To identify knowledgeable personnel to research and interpret policy or procedural solutions.	Days	M3-2
			To provide policy interpretation/information to the customer.	Days	

			To publish validated/evaluated information assurance security issues.	Days	M2-3, M3-4
SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Of communications systems provide access by intelligence personnel to consumers.	Percent	M4-1
SN 5.5	Coordinate Worldwide Information Operations	To coordinate the elements of offensive and defensive IO	National-level IO planning/coordination cell exists.	Yes/No	M3-3
			National-level IO planners from all appropriate US departments, agencies and organizations are involved in development and coordination of national IO plans and actions.	Yes/No	M3-3
			To conduct combat assessment of national IO "targets" struck with lethal and nonlethal means.	Hours	M2-1
			Of national IO cell nominated "targets" attacked when called for after combat assessment of initial strike.	Percent	offensive measure
SN 5.5.1	Conduct Strategic Information Operations	To conduct offensive and defensive IO for implementing Presidential and SecDef national military strategy, policy, objectives, and operations at the strategic level.	To provide assistance in the preparation and legal review of a request for supplemental ROE.	Hours	M3-3

			To provide assistance in the preparation and legal review of a review and approval package (RAP) in connection with computer network operations (CNO).	Hours	M3-3
SN 5.5.3.1	Provide Network Management for the Theater Information Grid (TIG) Transport and Computer Network Infrastructures	Equip, train, maintain, and sustain the theater-level NetOps centers to enable them to manage and control the command, control, communications, computer systems, and networks, including space systems that define the TIG transport infrastructure within their AOR.	Of authorized personnel on hand.	Percent	M3-2
			Of theater-level network operations center (TNC) personnel trained/certified to perform network operations (NETOPS) systems and network management (S&NM) tasks.	Percent	M3-2
			TNC is organized under the NETOPS CONOPS.	Yes/No	M3-1
SN 8.3.5	Coordinate DOD/Government Information Operations (IO)	To work with the Services, combatant commands, and civil/military agencies on issues involving offensive and defensive IO.	Identifications and organization of appropriate agencies and organizations to support interagency process.	Yes/No	M4-2
			Recommended versus approved DOD capabilities and activities employed in support of information operations tasks.	Percent	M3-3

ST 5.1.6	Establish Information Assurance (IA) Procedures	To establish information assurance procedures for deployed operations.	Do commands responsible for design, operation, and maintenance of theater strategic C4 systems have IA and defensive IO policies and procedures?	Yes/No	M3-1
			IA included in the command's plans and orders.	Yes/No	M3-1
			To appropriately respond to indications of hostile (domestic or foreign) information attack.	Minutes	M1-1
ST 5.5	Conduct Theater-Wide Information Operations (IO)	To conduct information operations for implementing the Secretary of Defense's national military strategy, policy, objectives and operations at the theater level.	Do theater level IO coordination policies and procedures exist?	Yes/No	M3-1, M3-3
			Does a theater level IO cell exist?	Yes/No	M3-1
			Are theater IO planners involved in identifying IO targets, deconflicting with conventional and other targeting efforts, and coordinating with conventional targeting efforts for enhanced effects-based operations within all plans?	Yes/No	M3-1
			To identify qualified personnel from various elements and activities and augment theater level IO planning cell after onset of planning requirement.	Hours	M3-3
			To identify required theater level IO information necessary for IO planning after onset of planning.	Hours	M3-3

ST 6.3.5	Protect Theater Information Systems	To coordinate theater-wide activities to protect and defend information and information systems. This task includes integrating and synchronizing indigenous and joint force capabilities for defensive IO, ranging from technical security measures (such as INFOSEC) to procedural measures (such as counterintelligence, physical security, and hardening of communications nodes).	Of licensed system administrators for critical C4I systems.	Percent	M3-2
			Of system administrators with full OPSEC training.	Percent	M3-2
			Of system administrators with full information system security training.	Percent	M3-2
			Of personnel familiar with command policies on information security.	Percent	M3-2
OP 6.2.14	Employ Operations Security (OPSEC) in the Joint Operations Area	To employ OPSEC measures to deny critical information necessary by an adversary commander to accurately estimate the military situation.	Of units equipped with antisurveillance sensor and sensor jamming devices.	Percent	M4-1
OP 6.3	Protect Systems and Capabilities in the Joint Operations Area	To identify critical information and subsequently analyze friendly actions attendant to planning and conducting campaigns and major operations to identify those actions that can be observed by adversary intelligence systems	Of system administrators with full OPSEC training.	Percent	M3-2
			Of licensed system administrators.	Percent	M3-2

SN 3.4.7	Coordinate Force Protection for Strategic Forces and Means	To coordinate force protection for strategic forces and means to enhance freedom of strategic action by reducing friendly vulnerability to hostile acts, influence, or surprise.	Of personnel who receive level one antiterrorism/force protection (AT/FP) training prior to deployment or travel overseas.	Percent	M3-2
			Of personnel who receive annual security awareness training.	Percent	M3-2
			Of strategic forces able to execute mission operations in an nuclear, biological, and chemical (NBC) environment	Percent	M3-2
ST 6	Coordinate Theater Force Protection	To conserve the fighting potential of a joint force, including actions taken to counter the enemy taking strategic action against that force.	Of forces operate in areas under control of friendly ground forces (during execution).	Percent	M2-1
			Of forces operate under air superiority umbrella (during execution).	Percent	M2-1
			Of forces operate within maritime superiority area (during execution).	Percent	M2-1
			In-place theater-wide system for tracking status of US personnel vaccines, antidotes, chemical/biological protective training.	Yes/No	M2-1

Tasks and Measures on this sheet Support the "Test & Acquire Secure Information Systems" master Task					
UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure

SN 5.1	Operate and Manage Global Strategic Communications and Information Systems	To receive information and data on the strategic situation worldwide, including: combatant command, theater component command, and operational level command missions, disposition of friendly and enemy forces, strategic centers of gravity, and characteristics of the theater areas (worldwide).	To process and authenticate EAM for execution of preplanned options against fixed Single Integrated Operational Plan (SIOP) targets (ICBM/fleet ballistic missile submarine (SSBN)/Bomber crews).	Minutes	M3-1
			To process RECORD COPY emergency action message (EAM) for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			To process VOICE emergency action message (EAM) for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			To transmit EAM to bombers for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			To transmit EAM to intercontinental ballistic missile(s) (ICBMs) for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			To transmit EAM to SSBNs for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			Of addressees received messages.		M2-3, M2-4
SN 5.1.1.1	Provide Information Assurance Products and Services	To provide products, services, infrastructure, and capability to assure availability and appropriate application of evaluated/validated products and solutions.	To complete information assurance product evaluations.	Months	M3-1

			To develop a secure interoperable Communications Security (COMSEC) solution to be submitted for approval from the Committee for National Security Systems in support of a validated customer requirement.	Weeks	M3-3
			Of National Security Agency (NSA) information assurance solutions that have full lifecycle support plans as a percentage of total.	Percent	M3-3
			To respond to validated customer requirements.	Days	M3-3
			Of microelectronics stockpile inventories maintained.	Percent	M4-1
SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Of articles on netted system available in heavy demand environment.	Percent	M4-1
			Of essential command and control (C2) nodes have redundant communication paths for minimum required communication capabilities to ensure timely receipt of all record traffic.	Percent	M4-1
			Of communications networks critical to operations fully operational.	Percent	M2-1

			Of communications outages equipped with adequate redundant communications paths to ensure timely receipt of record traffic.	Percent	M4-1
			Of DOD long-haul communications channels saturated.	Percent	M4-1
			Of information system interfaces require information scanning, retyping, reformatting, or other nondirect translation methods.	Percent	M4-2
			Of surge capacity available in DOD long-haul communications.	Percent	M4-1
			Each NC2 node can communicate by voice and record copy in a locally degraded environment.	Yes/No	M3-1
SN 5.1.2.1.1	Provide Global, Secure, Interoperable Communications and Networks for the Department of Defense	Provide global classified and unclassified voice, data, video, network, and transport backbone and access services through a combination of terrestrial and satellite assets.	Outages of any Defense Information System Network (DISN) global classified or unclassified voice, data, video, network, or transport backbone or access service that support a command and control network that isolates any combatant command headquarters.	Yes/No	M4-1
SN 5.1.2.1.2	Provide Global Information Grid Transport Backbone Networks for Data Communications	To provide the long-haul telecommunications infrastructure segment including the communication systems and services between the fixed environment and the deployed Joint Task Force (JTF) and/or Coalition Task Force (CTF) warfighter.	Of circuit or network availability.	Percent	M4-1

			Outages of the Defense Information System Network (DISN) that support a command and control network that isolate any combatant command headquarters.	Yes/No	M4-1
SN 5.5.3.1	Provide Network Management for the Theater Information Grid (TIG) Transport and Computer Network Infrastructures	Equip, train, maintain, and sustain the theater-level NetOps centers to enable them to manage and control the command, control, communications, computer systems, and networks, including space systems that define the TIG transport infrastructure within their AOR.	TNC has required facilities to conduct NETOPS S&NM tasks.	Yes/No	M3-1
SN 5.5.3.2	Protect and Defend the Theater Information Grid (TIG)	To collect and consolidate TIG intrusion detection reports and data, assessing the compiled data, and reporting the results to the appropriate command authorities.	Of TIG computer assets that are compliant or operating with approved extensions and mitigation plans with negligible risk on information systems capability to perform required theater missions	Percent	M2-1
OP 6.3.2	Supervise Communications Security (COMSEC)	To supervise the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.	Of multinational units operating from a common JCEOI.	Percent	M4-2
			Of US joint force units operating from common JCEOI.	Percent	M4-2

Appendix B. Cyberspace Defense ICD

UNCLASSIFIED

INITIAL CAPABILITIES DOCUMENT (ICD)

FOR

CYBERSPACE DEFENSE

By:

Maj Mike Hindley

Maj Nick Kozdras

Maj Tim Treat

Capt Richard Brown

6 March 2007

Table of Contents

1 Joint Functional Area105

 1.1 Strategic Guidance for Cyberspace Defense105

 1.2 Joint Capability Areas (JCA)107

 1.3 Joint Operating Concepts108

 1.3.1 *Deterrence Operations Joint Operating Concept (DO JOC)* 108

 1.4 Joint Functional Concepts109

 1.4.1 *Protection Joint Functional Concept* 109

 1.4.2 *Focused Logistics Joint Functional Concept* 110

 1.4.3 *Net-Centric Environment Joint Functional Concept* 111

 1.4.4 *Force Management Joint Functional Concept* 111

 1.5 Current Cyberspace Defense Related Operations111

2 Required Capability.....113

 2.1 Functional Area Analysis (FAA) Report.....113

 2.2 Defend Cyberspace Information and Information Systems113

 2.3 Command and Control of Cyberspace Defense114

 2.4 Organize, Train and Equip Cyberspace Personnel.....114

 2.5 Test and Acquire Cyberspace Systems:115

3 Concept of Operations (CONOPS) Summary.....115

 3.1 Introduction115

 3.2 General115

 3.3 Scope116

 3.4 Cyberspace Defense Operational View.....116

4	Capability Gaps	120
5	Threat and Operational Environment	121
6	Functional Solution Analysis	123
6.1	Ideas for Non-Materiel Approaches (DOTMLPF Analysis).....	123
6.2	Ideas for Materiel Approaches	125
6.3	Analysis of Materiel/Non-Materiel Approaches (AMA)	126
6.3.1	<i>Methodology</i>	<i>126</i>
6.3.2	<i>Today’s Cyberspace Defense Capability</i>	<i>128</i>
6.3.4	<i>Near Term (0-3 years)</i>	<i>129</i>
6.3.5	<i>Mid Term (3-6 years)</i>	<i>130</i>
6.3.6	<i>Far Term (6-9 years)</i>	<i>131</i>
7	Final Recommendation.....	131
AppendixA	Feasibility Worksheet	133
AppendixB	Solutions Performance and Capability Gaps	134
AppendixC	Cyberspace Defense Tasks and Measures of Effectiveness Analysis	135

Table of Figures

Figure 1: Command and Control of Joint Forces through Cyberspace	49
Figure 2: Coordination with External Entities through Cyberspace	50
Figure 3: OV-1 Cyberspace Defense Operational View	51

Index of Tables

Table 1: Measures to Defend Cyberspace Information and Information Systems	114
Table 2: Measures for Command & Control of Cyberspace Defense	114
Table 3: Measures to Organize, Train and Equip Cyberspace.....	115
Table 4: Measures to Test and Acquire Information Systems	115
Table 5: Prioritized Capability Gaps.....	121
Table 6: Today's Cyberspace Defense Capability (Gap Fulfillment)	129
Table 7: Near Term Cyberspace Defense Capabilities (Gap Fulfillment).....	130
Table 8: Mid Term Cyberspace Defense Capabilities (Gap Fulfillment).....	131
Table 9: Far Term Cyberspace Defense Capabilities (Gap Fulfillment)	131

1 Joint Functional Area

1.1 Strategic Guidance for Cyberspace Defense

1.1.1 The FAA was initiated by analyzing strategic documents to find references and priorities to cyberspace. The analysis quickly revealed national leaders have identified cyberspace as a new operational domain. The leaders have also increased the priority for cyberspace security and our ability to maintain cyberspace operational superiority. For instance, the 2006 QDR included as new domain, cyberspace, to protect and defend along with air, land, maritime, and space.³² In addition, the National Defense Strategy written in 2005 also highlighted the increased priority of cyberspace by noting:

“Our ability to operate in and from the global commons—space, international waters and airspace, and cyberspace—is important.”³³

1.1.2 The National Defense Strategy goes on to clearly single out cyberspace as a “new theater of operations.”³⁴ Then the strategy directly links cyberspace with Information Operations and indicates:

“Consequently, Information Operations (IO) is becoming a core military competency. Successful military operations depend on the ability to protect information infrastructure and data. Increased dependence on information networks creates new vulnerabilities that adversaries may seek to exploit. At that time, an adversary’s use of information networks and technologies creates opportunities for us to conduct discriminate offensive IO as well. Developing IO as a core military competency requires fundamental shifts in processes, policies, and culture.”³⁵

The fundamental shifts mentioned by the National Defense Strategy to reorganize United States assets and operate securely in cyberspace are significant. The shifts will posture our military and federal organizations in order to synchronize operations and ensure our cyberspace defense capabilities are utilized adequately and effectively. Ultimately, the shifts must provide for fully integrated synchronization with respect to military operations in support of military objectives and military assistance to federal authorities and agencies when required.

1.1.3 According to the Joint Chiefs of Staff, “Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.”³⁶ This definition describes an incredibly complex domain that crosses multiple organizations, agencies, and institutions. In

³² Quadrennial Defense Review, 2006, pg 37

³³ National Defense Strategy, March, 2005, pg 13

³⁴ National Defense Strategy, March, 2005, pg 13

³⁵ National Defense Strategy, March, 2005, pg 13

³⁶ National Military Strategy for Cyberspace

addition, not all are military and federal. There are many that are civilian, commercial, medical, etc..., that could cripple our national security if compromised by an adversary. Military organizations must be able to share information as required with trusted federal and national security entities. This information sharing must be defended against compromise or attack for both intended and unintended instances.

1.1.4 The 2006 QDR increased the complexity of the cyberspace domain by including the need to work with our international allies and coalition partners in cyberspace. It directly calls out cyberspace as a multi-national priority along with Weapons of Mass Destruction (WMD) by stating:

“Concepts and constructs enabling unity of effort with more than 70 supporting nations under the Proliferation Security Initiative should be extended to domains other than WMD proliferation, including cyberspace, as a priority.”³⁷

The emphasis shows how important cyberspace is from a multi-national perspective and foreshadows how our national leadership will focus on multinational cyberspace operational efforts in the future.

1.1.5 The 2006 QDR continues with more than just identifying cyberspace as a new domain. For instance, it explains that terrorists “exploit the Internet as a cyber-sanctuary, which enables the transfer of funds and the cross-training of geographically isolated cells.”³⁸ The QDR also discusses how:

“China is likely to continue making large investments in high-end asymmetric military capabilities, emphasizing electronic and cyber-warfare...for employment by the Chinese military and for global export.”³⁹

This is not just the Internet; the electronic capabilities China and other countries are creating utilize the entire electronic spectrum. Thus, cyberspace defense must encompass the defense of the entire cyberspace theater of operations.

1.1.6 Another strategic document that discusses the importance for cyberspace defense is The National Strategy to Secure Cyberspace (NSSC). Written in February 2003, it is an implementing component to the National Strategy to Homeland Security.⁴⁰ It provides the overarching guidance for protecting Cyberspace. The document identifies the Department of Defense as the lead agency for cyberspace defense of itself and the national defense industrial base. In addition, the strategy provide “Critical Priorities for Cyberspace Security” as follows:

1. A National Cyberspace Security Response System

³⁷ 2006 QDR, pg 88-89

³⁸ 2006 QDR, pg 21

³⁹ 2006 QDR, pg 29-30

⁴⁰ National Strategy for Homeland Security, July 2002

2. A National Cyberspace Security Threat and Vulnerability Reduction Program
3. A National Cyberspace Security Awareness and Training Program
4. Securing Governments' Cyberspace
5. National Security and International Security Cooperation⁴¹

The five priorities provide a glimpse of what is ahead for professionals defending cyberspace. Likewise, the priorities provide a compass for DoD cyberspace defenders to direct their efforts. The strategy is another solid example of many to depict the importance of cyberspace defense and the strategic importance of controlling the cyberspace high ground.

1.1.7 Ultimately, our national leadership realizes the importance of defending the cyberspace operational and strategic high ground. The virtual and asymmetric challenges in cyberspace open up a multitude of holes that can weaken our resolve and national security if not rigorously defended. As a nation, we must develop an overall cyberspace defense capability to include how the military integrates with agencies and departments to protect vital information from enemies abroad and secure our homeland internally.

1.1.8 As the strategic documents show, cyberspace is more than a domain America utilizes to increase efficiency and improve processes; it is a strategic high ground for critical systems and infrastructure. The domain provides a medium where the war can literally impact homes and work places. It can be used to cripple a nation's ability to perform life sustaining functions and topple a nation's ability to maintain stability if not adequately defended.

1.2 Joint Capability Areas (JCA)

1.2.1 There are currently 21 Tier-1 JCAs approved by the Secretary of Defense. Each Tier-1 JCA includes collection of similar capabilities, grouped at a high level to support decision-making, capability delegation, and analysis.⁴² Cyberspace defense is inherent across a number of the Tier 1 JCAs including:

- Joint Access and Access Denial Operations
- Joint Maritime/Littoral Operations
- Joint Space Operations
- Joint Command and Control
- Joint Net-Centric Operations
- Joint Interagency/IGO/MN/NGO Coordination
- Joint Public Affairs Operations
- Joint Information Operations
- Joint Protection
- Defensive Support of Civil Authorities
- Joint Battlespace Awareness
- Joint Force Generation
- Joint Force Management
- Joint Homeland Defense

⁴¹ The National Strategy to Secure Cyberspace, February 2003

⁴² Joint Capability Document for Net-Centric Operational Environment, 10 Jul 2006

Joint Global Deterrence
Joint Shaping
Joint Stability Operations
Joint Special Operations and Irregular Warfare

The fact cyberspace defense impacts such a wide cross section of our JCAs, is eye-opening and makes cyberspace defense increasingly more significant. Our military is evolving to perform all mission aspects through the cyberspace domain and can not afford to lose ground on the cyberspace front. Across the board, a fundamental shift will have to take place over time to embrace cyberspace defense as more than just a support operation. Cyberspace operators will have to become truly joint warriors and directly integrate into all missions.

1.3 Joint Operating Concepts

1.3.1 Deterrence Operations Joint Operating Concept (DO JOC)⁴³

1.3.1.1 The DO JOC highlights the increasing advantages asymmetric cyberspace threats can utilize against our technology advance systems and capabilities. The document notes:

“The emergence of advanced capabilities and technologies such as computer network attack or directed energy weapons may permit future adversaries to achieve objectives once attainable only via the use of WMD.”⁴⁴

Both computer network attack and directed energy threats fall directly in the cyberspace defense realm of operations. As we continue to increase our use of technology advanced capabilities we have to grow highly capable cyberspace defenders trained to utilize cyberspace capabilities in joint operational environments as well as trained on how to defend our joint/coalition operations and information from network attack, energy weapons, or other cyberspace threats. The statement above is staggering, especially over time, the fact that cyberspace attack can achieve the same proportional effect as WMD just cannot be underemphasized. This simple fact makes the need for fundamental shifts in our military to enable unequivocal cyberspace defense essential.

1.3.1.2 The DO JOC goes on to discuss supporting the need of a strong cyberspace defense by not only addressing the vulnerabilities to our forces, but also the vulnerabilities to our society:

“Vulnerabilities of US Society and Forces: Free and open societies are uniquely vulnerable to terrorist tactics. Both the US economy and US military forces are increasingly dependent on advanced technologies for their significant competitive advantages. While this technological superiority yields tremendous capabilities it also creates potential vulnerabilities that adversaries might exploit. Advanced

⁴³ Deterrence Operations Joint Operating Concept, v2., December 2006

⁴⁴ Deterrence Operations Joint Operating Concept, v2., December 2006

cyberspace warfare capabilities, capabilities to disable space systems, and electromagnetic pulse weapons could all provide adversaries means of undermining potentially decisive US advantages. In addition, both state and non-state actors will have significant abilities to conduct devastating covert attacks on the US population, infrastructure, forces, and overseas interests. US deterrence strategy needs to take these potential US vulnerabilities fully into account, eliminating them where feasible, and compensating for them when necessary.”⁴⁵

The text foreshadows the impact of failing to defend the cyberspace domain from terrorists and adversaries. Our ability to maintain national security, sovereignty, economic strength, and freedom will be significantly impacted if we wait too long to fundamentally adjust.

1.4 Joint Functional Concepts

1.4.1 Protection Joint Functional Concept

1.4.1.1 The protection joint functional concept defines force protection as being “composed of a variety of active and passive measures (e.g., weapons, armor, camouflage, stealth, pre-emption, deception, etc.) in the air, land, sea, space and cyberspace domains.” This force protection will be accomplished “through the scaled and tailored selection and application of multi-layered, active and passive, lethal and non-lethal measures, within the air, land, sea, space and cyberspace.”⁴⁶ Cyber defense of the joint force’s information, infrastructure, and systems is critical to the protection of the joint force.

1.4.1.2 The functional concept further develops the conduct of protecting information as “the interaction of the force operations activities related to sensing, understanding, deciding, and executing the tasks necessary to ensure that cyberspace attacks are avoided, neutralized or mitigated.”⁴⁷ These operations activities and how they relate to computer network defense are:

1.4.1.3 Detect

1.4.1.4 The ability to collect timely and accurate data/information regarding adversary capabilities is a vital capability of protection. Our ability to detect in the future is inextricably tied to predictive intelligence, focusing our detection efforts and optimizing where to look.⁴⁸

1.4.1.5 Assess

1.4.1.6 Develop an understanding of the situation and accurately identify adversary capabilities that can be used against friendly personnel, physical assets, and information and precisely derive adversary courses of action, planned or employed, with the intent to destroy, or disrupt,

⁴⁵ Deterrence Operations Joint Operating Concept, v2., December 2006

⁴⁶ Protection Joint Functional Concept, 30 June 2004

⁴⁷ Protection Joint Functional Concept, 30 June 2004

⁴⁸ Protection Joint Functional Concept, 30 June 2004

operational readiness. Additionally, begin development of a course (or courses) of action, and orders for execution that will allow the JF to react to actionable intelligence regarding adversary plans and actions.⁴⁹

1.4.1.7 Warn

1.4.1.8 The ability to execute detailed contingency planning and preparation is a fundamental aspect of the protection process. Desired capabilities in 2015 include a robust C2 system that provides the effective means to coordinate the execution of plans, global warning based on focused detection, predictive intelligence and a network of dissemination systems in real time—thus driving the requirement for cyber defense of information, infrastructure and systems.⁵⁰

1.4.1.9 Defend

1.4.1.10 The ability to execute a selected course of action to resist hostile actions directed against friendly personnel, physical assets, and information in order to preserve operational capabilities. Protection is characterized by the execution of those multi-layered, active and passive, measures/actions that resist hostile actions directed against friendly personnel, physical assets, and information in order to preserve operational capabilities.⁵¹

1.4.1.11 Recover

1.4.1.12 Actions taken during, or after a hostile attack to restore friendly personnel, physical assets, and information to full operational readiness. Recovery will span reconstitution efforts for forces deployed, assistance in managing the consequences of an attack at an installation, conducting military support to designated civilian authorities and agencies, and when applicable, recovery of isolated personnel and/or equipment, and rapid repositioning.⁵²

1.4.1.13 The functional concept continues to describe national cyberspace defense as "all defensive measures of homeland defense taken to detect, deter, defeat, or nullify hostile cyberspace threats against US territory, domestic population, and defense critical infrastructure. Note: only encompasses defensive Information Operations (IO), particularly information protection."⁵³

1.4.2 Focused Logistics Joint Functional Concept

1.4.2.1 This functional concept notes that the logistics pipeline, from end to end, will be a lucrative target for enemy attack, as deployment and sustainment data are transmitted via cyberspace and will be subject to cyberspace attack.⁵⁴ The logistics community continues to forge ahead with increasing numbers of cyberspace initiatives, such as radio frequency

⁴⁹ Protection Joint Functional Concept, 30 June 2004

⁵⁰ Protection Joint Functional Concept, 30 June 2004

⁵¹ Protection Joint Functional Concept, 30 June 2004

⁵² Protection Joint Functional Concept, 30 June 2004

⁵³ Protection Joint Functional Concept, 30 June 2004

⁵⁴ Focused Logistics Joint Functional Concept, December 2003

identification tags on cargo pallets, that place the military's logistics trains at increasing risk to cyberspace attack.

1.4.3 Net-Centric Environment Joint Functional Concept

1.4.3.1 This functional concept highlights the importance of the cyberspace domain's ability to maintain service and survive an attack: "Once deployed, the network must be able to maintain service while under both physical attack and information attack. It should degrade gracefully, that is, continue operations at a gradually reduced capacity in accordance with prioritization plans as systems/equipment are destroyed and/or damaged. The network must be capable of dynamically rerouting services as nodes are incapacitated and/or as information flow requirements change. The network must be capable of obtaining additional resources as required to maintain or increase capacity."⁵⁵

1.4.3.2 Helpfully, the concept notes that the over-reliance on information and communications technologies may result in forces incapable of operating effectively in the absence of those technologies due to failure or attack. To mitigate this concern, the joint force can increase reliability of new equipment and develop appropriate levels of integrated redundancy in system architectures. Further, training and exercises that realistically simulate conditions of failure and attack are critical to effective joint capability development.⁵⁶

1.4.4 Force Management Joint Functional Concept

1.4.4.1 This functional concept defines functional modularity to include "human and technical assets fulfilling the same roles while operating in the same primary functional domain and operating to the same standards of practice, proficiency, and lexicon. Primary functional domains include: space, air, land, sea, undersea and cyber environments."⁵⁷ Cyberspace defense is critical to employing the constellation net's information sharing capabilities.

1.5 Current Cyberspace Defense Related Operations

1.5.1 There are a multitude of current operations being conducted as part of cyberspace defense. At this time, the preponderance of forces and operations is supported by and supporting USSTRATCOM under the Computer Network Defense (CND) mission. As the DoD lead for CND, USSTRATCOM has delegated the responsibility to Joint Task Force Global Network Operations (JTF-GNO). The overall CND operation is directed by JTF-GNO to all other COCOMs and Services. JTF-GNO is the operational interface between DoD and other federal entities and civilian organizations. With respect to defense, JTF-GNO concentrates on CND and does not have a full cyberspace defense scope or capabilities to fully defend all of DoD cyberspace.

⁵⁵ Net-Centric Environment Joint Functional Concept, 7 April 2005

⁵⁶ Net-Centric Environment Joint Functional Concept, 7 April 2005

1.5.2 Each military service and Combatant Command has non-standardized constructs for C2 and defense of cyberspace assets. They concentrate on CND operations separately and report status back to JTF-GNO. The CND tactics are handled by each service independently and the non-standard approach hinders our ability to synchronize cyberspace defense operations. There are joint policies and procedures in place for reporting, and there are processes to follow for nominating joint tactics.

1.5.3 The training of cyberspace professionals is also handled by each individual service and organization. Virtually all cyberspace professionals are trained by their respective organization on how to operate, maintain, and secure the cyberspace infrastructure. However, there are no joint schools for training professionals on cyberspace defense. The DoD currently addresses cyberspace like all other domains where each respective service is responsible for organizing, training, and equipping themselves to operate.

1.5.4 Other than tools and systems for cyberspace reporting, the joint community has not identified joint tools and systems that are mandated for cyberspace defense. Each service and COCOM monitors their respective portions of the cyberspace theater independently. This makes correlation of attacks and outages difficult and hinders our ability to identify coordinated attacks and quickly recover.

1.5.5 Currently, there is no traffic monitoring service for cyberspace. If a joint entity is under a cyberspace attack, coordination of response activities is very ad hoc, where the level of perceived impact determines the methodology. Additionally, there is currently no process for informing other entities as to the integrity of systems. A relevant example would be AFIT & AFRL communications, where for instance AFIT's e-mail is down, the NetOps center at WPAFB is informed that the system is down, however there is no communication to AFRL that AFIT's e-mail is down.

1.5.6 There are many other organizations throughout the DoD working independently to secure cyberspace assets. They rely on different standards, capabilities, knowledge, training, etc. The cyberspace defense concept will help overcome this significant problem and allow our cyberspace defense capabilities to evolve along with our technology advanced systems.

1.5.7 As we continue to become more technologically advanced and reliant, the impact of cyberspace attacks and problems will impact our ability to operate more and more. As the United States military, agencies, civilian companies, etc... continue to develop architectures and integrated systems, it will be more and more important for us to have an evolving cyberspace defense force. In addition, we are faced with many pressures which have changed how we fight:

We fight joint, and we are still trying to figure out what that means
 We fight coalition, and we make that happen on a case by case basis
 Our adversaries' tactics and target profiles are changing more and more⁵⁸

2 Required Capability

2.1 Functional Area Analysis (FAA) Report

2.1.1 Cyberspace is an emerging strategic domain and documentation of Required Capabilities is neither well defined nor standardized. The team identified five tasks during FAA and, using the Universal Joint Task List (UJTL) as a reference, identified over 200 existing Measures of Effectiveness (MOE) to support these tasks. These UJTL MOEs have been consolidated into MOEs supporting four of these tasks listed in the tables below. The linkages between these measures and the UJTL are provided in the Correlation Matrix in Appendix C. The fifth task, Defend Critical Cyberspace Infrastructure, is not covered in the scope of this document.

2.1.2 The team identified four categories of information systems and data, dubbed Information Categories (InfoCAT), used as a condition to appropriately tailor specific Cyberspace Defense measures. The InfoCAT definitions are as follows:

- InfoCAT-A - Information Systems used to operate DoD Weapon Systems
- InfoCAT-B - Information Systems certified to processing Top Secret data
- InfoCAT-C - Information Systems certified to processing Secret data
- InfoCAT-D - Information Systems certified to processing Unclassified data

2.1.3 As noted previously, there is no standardized DoD-wide construct for Cyberspace. Likewise, there is no standard set of metrics that can be used to determine current performance or be used as a baseline to set standards for the measures identified below. Thus, the standards of performance listed in this document are a based on initial SME judgment with any ambiguity clarified in the MOE summary in Appendix C.

2.2 Defend Cyberspace Information and Information Systems

2.2.1 This task quantifies the ability to detect and defend against Cyberspace attacks, investigate and report on their impacts, and to accomplish recovery actions. The Cyberspace domain is unique in its definition of 'attack'. Attacks include any attempt to disrupt, damage, or destroy information systems or data. Attacks can be launched from anywhere in the world and range from criminal activity to acts of war.

Task 1: Defend Cyberspace Information & Information Systems			
MEASURE		INFOCAT	STANDARD
M1-1	Percent Of Cyberspace Attacks Successfully Defended	A	99.99%
		B	99.9%

⁵⁸ Architecture 101 briefing, Titcombe, Matthew A.

		C	99.5%
		D	99%
M1-2	Time To Investigate & Report Impact, Post-Attack	A	30 Minutes
		B	60 Minutes
		C	120 Minutes
		D	480 Minutes
M1-3	Time To Recover, Post-Attack	A	5 Minutes
		B	15 Minutes
		C	60 Minutes
		D	240 Minutes

Table 7: Measures to Defend Cyberspace Information and Information Systems

2.3 Command and Control of Cyberspace Defense

2.3.1 This task defines the need to maintain real-time Command & Control of the entire Cyberspace Domain (joint, allied, critical defense infrastructure, etc). This includes maintaining situational awareness of DoD network status worldwide, identifying and responding to major attacks, directing response actions, coordinating with external agencies, etc.

Task 2: Command & Control of Cyberspace Defense			
MEASURE		INFOCAT	STANDARD
M2-1	Maintain Cyberspace Situational Awareness	All	99.9%
M2-2	Convene Cyberspace Threat Conference To Direct Attack Response Actions	All	99.9%
M2-3	Time To Notify Users Of New Attacks/Threats/Countermeasures	A	5 Minutes
		B	5 Minutes
		C	10 Minutes
		D	10 Minutes
M2-4	Time To Notify Users Of Known Vulnerabilities/Responses	A	4 Hours
		B	4 Hours
		C	6 Hours
		D	6 Hours

Table 8: Measures for Command & Control of Cyberspace Defense

2.4 Organize, Train and Equip Cyberspace Personnel

2.4.1 This task defines those core activities that personnel must perform to ensure that the cyberspace defense concept is executed appropriately. Organize, train and equip cyberspace personnel is necessary as the information systems being defended do not always have the capability to automatically respond to an attack, and recognizes that the human in the loop creates the environment in which these systems are used. The essence of this task is to develop and execute joint standards and processes for defensive measures while providing the required personnel.

Task 3: Organize, Train and Equip Cyberspace

MEASURE		INFO CAT	STANDARD
M3-1	Perform Standards Verification	All	98%
M3-2	Percent of Trained Cyber/Information Operations Personnel	All	98%
M3-3	Provide Cyberspace Defense Plans	All	Yes/No

Table 9: Measures to Organize, Train and Equip Cyberspace

2.5 Test and Acquire Cyberspace Systems:

2.5.1 As a capability, test and acquire cyberspace systems defines those activities related to the assurance that the information systems being used by all members of the joint community will meet current and/or future cyberspace defense standards. This task includes such activities as establishing baseline defensive requirements like availability and interoperability into new information systems before they become operational.

Task 4: Test and Acquire Information Systems			
MEASURE		INFO CAT	STANDARD
M4-1	Percent of Information Systems Meeting Availability Standards	A	99.99%
		B	99.9%
		C	99.5%
		D	99%
M4-2	Percent of Information Systems Meeting Interoperability Standards for Cyberspace Defense	All	99.99%

Table 10: Measures to Test and Acquire Information Systems

3 Concept of Operations (CONOPS) Summary

3.1 Introduction

3.1.1 As the US military becomes increasingly reliant on cyberspace to achieve and maintain superiority in the traditionally recognized operational/strategic domains (land, sea, air, and space), cyberspace has become an operational domain in its own right. The virtual cyberspace theater has evolved to a strategic high ground instead of just a force enabler or multiplier. This evolution from force enabler to strategic/operational domain requires a dramatic examination of military forces and capabilities to ensure our military force is capable of achieving and maintaining cyberspace superiority. In addition, that superiority must be sustained in a Joint and Coalition environment as well as between military forces and national and local agencies protecting the homeland.

3.2 General

3.2.1 This Cyberspace Defense document contains a Capabilities Based Assessment (CBA) that includes a Functional Solutions Analysis (FSA) based on the results and recommendations of The Cyberspace Defense Joint Capabilities Document⁵⁹.

3.2.2 The Functional Area Analysis (FAA) pulled information from many existing strategic documents, including a review of the Quadrennial Defense Review (QDR) for 2006, the National Security Strategy, the National Defense Strategy, the National Strategy to Secure Cyberspace, the National Military Strategy for Cyberspace, Joint Operational Concepts and Joint Functional Concepts. All consistently identify cyberspace as a new operational/strategic domain that must be defended. The challenge as outlined in these documents is not just retooling our military forces to operate more effectively in cyberspace, but to appropriately ensure our use of all of the instruments of national power; economic, military, political, and information.

3.2.3 One of the biggest challenges for cyberspace is development of a definition. Since the cyberspace theater is asymmetric and virtual, there are multiple working definitions. Recently, the Joint Chiefs of Staff released a definition stating, “Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.”⁶⁰ This definition allows us to adequately scope our efforts by providing a foundation to link the required tasks and capability gaps to during the FNA.

3.3 Scope

3.3.1 This document focuses on a capabilities-based assessment for cyberspace defense. It does not directly assess cyberspace attack; rather it concentrates on synchronizing cyberspace forces to defend against internal and external attacks and exploitation in the asymmetric cyberspace theater of operations. The document also does not address the physical aspects of information protection in containers, facilities, on individuals, etc., as much of that is already effectively addressed in the functional area of force protection. In order to scope the project to a manageable scale, this document concentrates on the defense of cyberspace information specifically in the cyberspace theater of operations.

3.4 Cyberspace Defense Operational View

3.4.1 The DOD is faced with the evolution of a global system of systems that reside in Cyberspace. Not only are sensors, platforms, systems, and networks becoming more global, they are becoming intertwined and technologically intense. Given this, we have struggled to manage complexity, reduce the risk of compromise, and develop methodologies that affordably increase military capability.

3.4.2 As our military effectiveness develops through cyberspace capabilities, it will be critical to introduce and evolve an effective cyberspace defense operational concept based on an operational view. The concept will have to be executed in a joint environment alongside our technical advances in military capability. The obvious need for the cyberspace defense concept

⁵⁹ Joint Capabilities Document for Cyberspace Defense, Hindley, Kozdras, Treat, Brown, 11 February 2007

⁶⁰National Military Strategy for Cyberspace

is derived from the realization cyberspace has created a more intense and asymmetric battle front. As the joint community becomes more reliant on technology, and employs smaller numbers of highly capable assets to achieve objectives, the defense of cyberspace must be a priority and executed unambiguously.

3.4.3 The cyberspace defense operational view is based on the joint staff definition of cyberspace stated previously in paragraph 1.2.3. The definition provides a foundation for an overall concept of unambiguous defense of cyberspace and the development of the tactics, people, and systems required. To provide a visual example, Figure 1 shows an overview for command and control of joint forces through joint cyberspace networks. It is not an all encompassing diagram for cyberspace but enables the following paragraphs to accurately outline the overall approach for the cyberspace defense CONOPS.

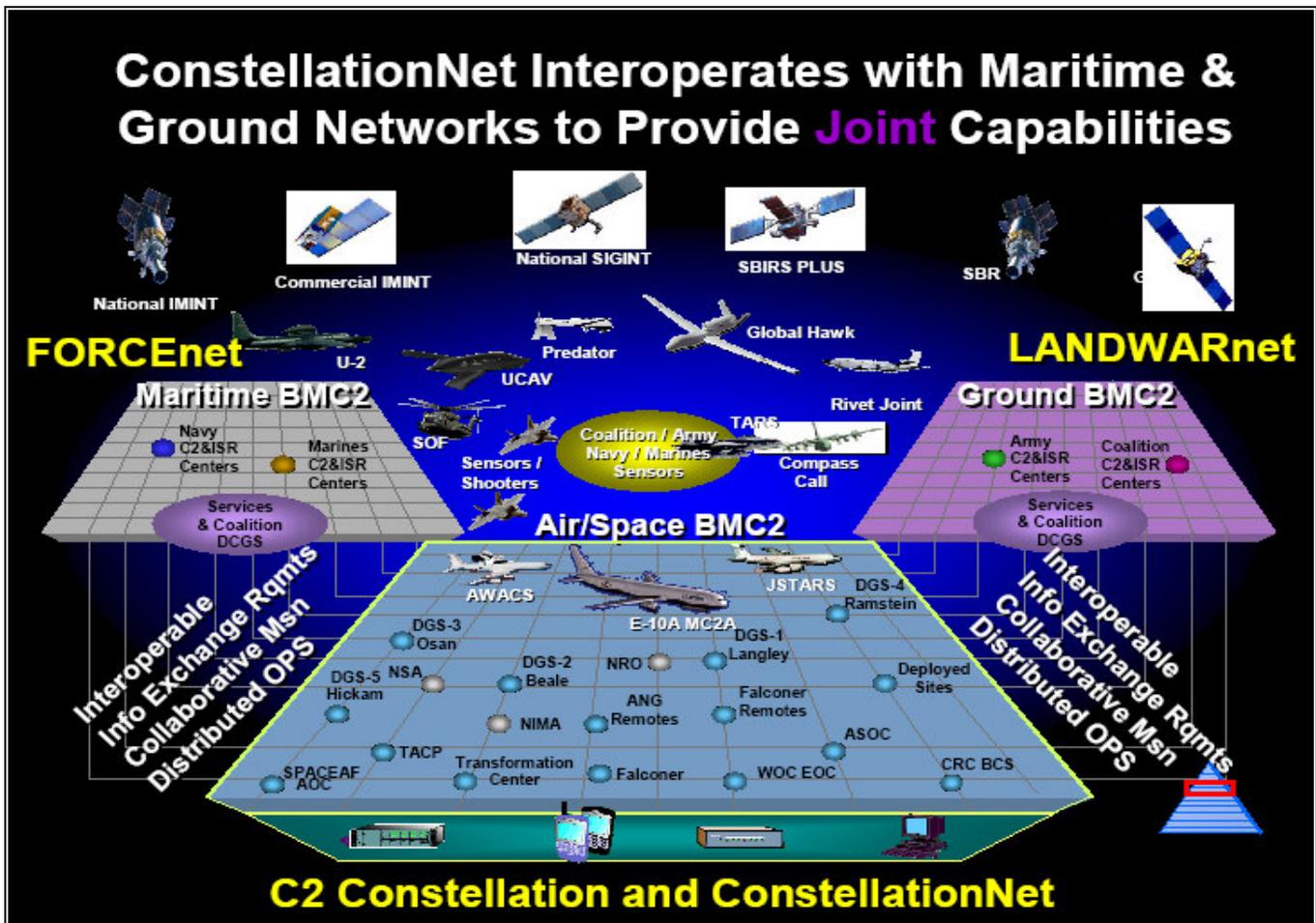


Figure 4: Command and Control of Joint Forces through Cyberspace⁶¹

3.4.4 First, the military is evolving from platform-centric operations to net-centric operations connected through cyberspace allowing services, combatant commanders, agencies, and multinational forces to synchronize operations and work in conjunction with each other. *The level-of-*

⁶¹ Implementing the Constellation Net briefing, Titcombe, Matthew A.

effort to adequately defend the cyberspace battle front from internal and external attack or “unintended fratricide” is the crux of the cyberspace defense operational view. For our net-centric operations to be reliable, successful, unhindered, and secure, we must be able to protect and verify cyberspace connectivity throughout Figure 1 for all levels of security and weapon systems in the joint environment.

3.4.5 Next, Figure 2 shows how the joint community evolves to synchronize operations through cyberspace. An adequately defended cyberspace theater provides military commanders the critical access to information and systems when operating with combatant commanders, multi-national forces, national agencies, and homeland security. Again, the diagram does not adequately represent the complex environment of cyberspace. Since the environment is virtual, adaptive, and asymmetric, the dynamic nature of cyberspace must be imagined as much as documented on paper.

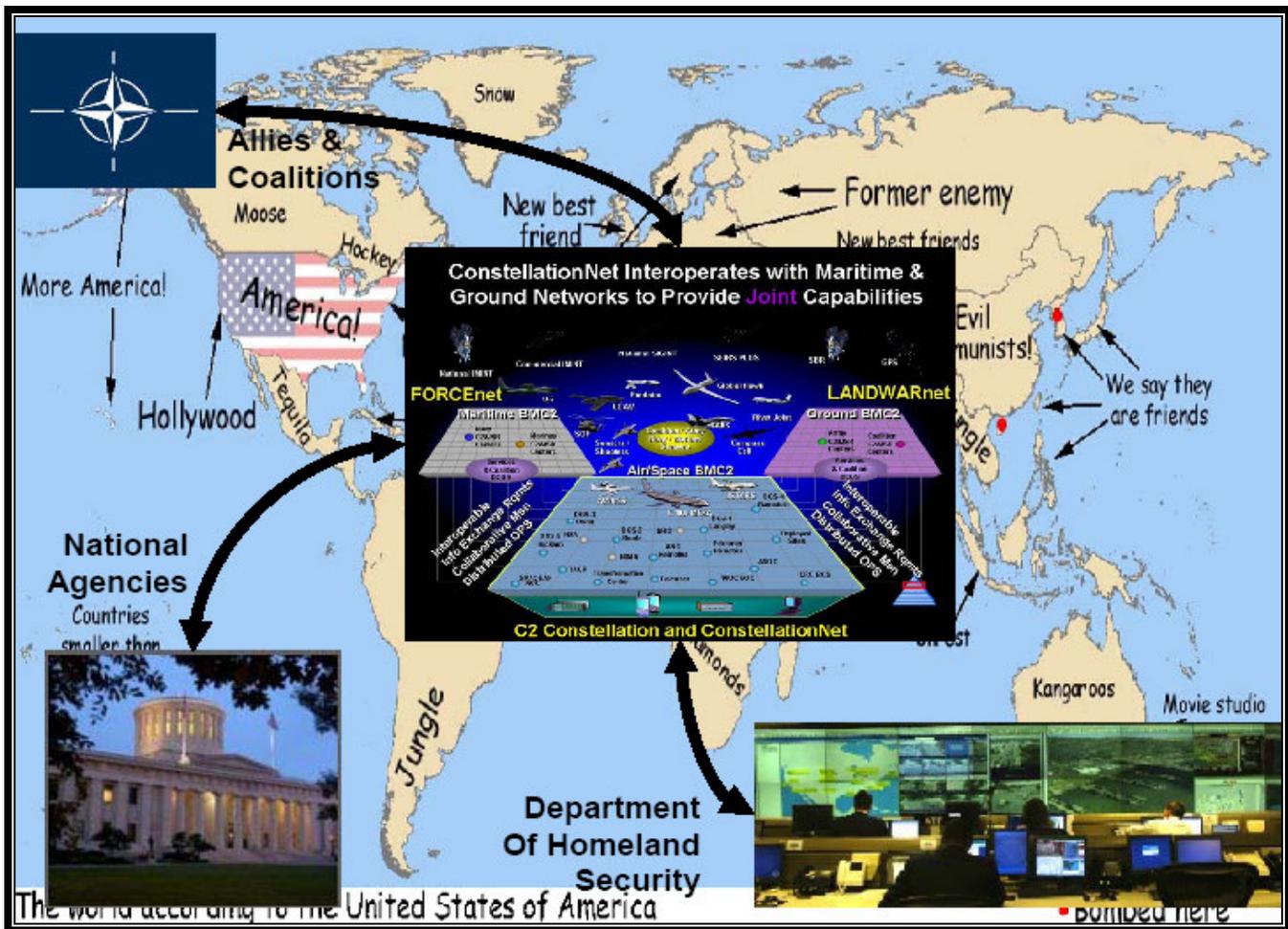


Figure 5: Coordination with External Entities through Cyberspace

3.4.6 As a build to the previous diagrams, Figure 3 includes a dotted line around the cyberspace environment that is intended to be porous to allow authorized personnel access to critical information resources and automated dissemination of trusted and verified information. The figure also shows how we must be able to maintain the strategic cyberspace high ground

through fully vetted and effective cyberspace defense. This operational cyberspace defense concept provides the ability to defend, assure, secure, and verify information throughout the cyberspace theater of operations. The concept also provides for the ability for combatant commanders and joint forces to work with agencies, allies, coalitions, and Homeland Security. In this manner, we can defend cyberspace:

1. from attack
2. from unintended loss/compromise of information while providing assured critical information for operational and support use.
3. through verification that the information is from trusted sources.

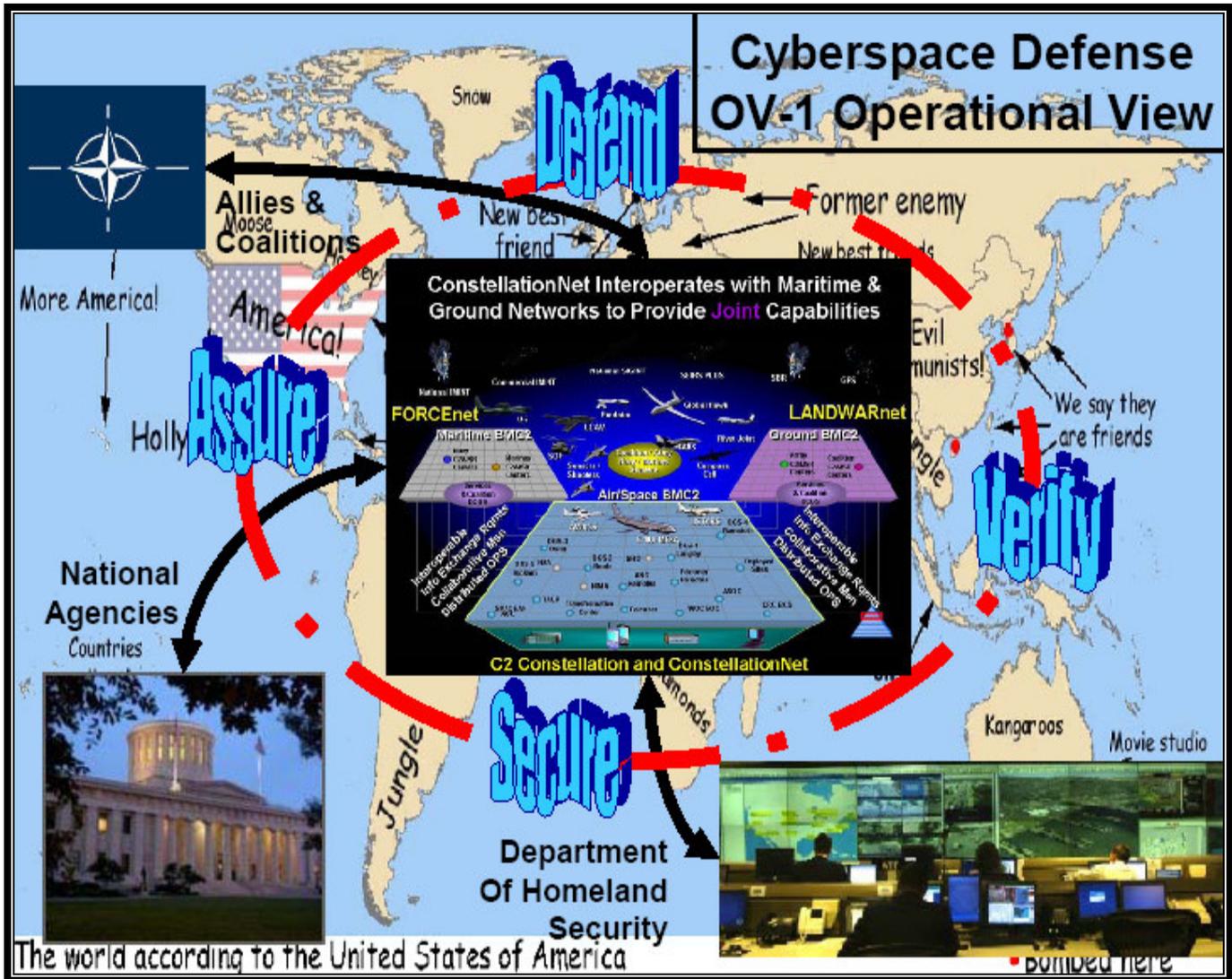


Figure 6: OV-1 Cyberspace Defense Operational View

3.4.7 The means to defend cyberspace under the cyberspace defense concept are nebulous at this time. There are a number of best practices that include positioning sensors strategically throughout cyberspace for immediate feedback about activity on electromagnetic mediums. The sensors identify suspicious or malicious activity and provide situational awareness to cyberspace professionals. We also have intrusion detection systems in place that automatically sift through

log files and report to personnel monitoring different cyberspace systems. However, we do not have the joint standardization of equipment, processes, systems, personnel and training necessary to effectively defend cyberspace. To effectively defend cyberspace, we will need the same capabilities of any force fighting a war. The capabilities include joint commanders overseeing joint personnel working together using joint standardized capabilities to fight in a synchronized environment. The joint cyberspace commander in charge will have joint personnel attached and collocated with services, combatant commanders, agencies, coalitions, and homeland security. The personnel will have the skills to execute cyberspace defense capabilities using the tactics, training, and procedures directed as they execute supporting and supported roles for the joint community. They will be able to perform cyberspace patrols throughout all of cyberspace and call for support from the joint cyberspace commander's attack elements when needed. The concept cohesively integrates all military cyberspace defense operations through a fully joint approach where the joint commander can organize, train, provide equipment and decide what the standards are for cyberspace defense. From this description of the cyberspace defense operational view, the roles and responsibilities of cyberspace described contain similarities to the operational missions of United States Special Operations Command and the United States Strategic Command.

4 Capability Gaps

4.1 As noted previously, there is no standardized, DoD-wide construct for cyberspace defense. Thus, a comprehensive and quantitative analysis of current cyberspace defense capabilities is required to adequately assess our current performance. Current documentation, however, does reveal numerous qualitative capability gaps. The Joint Capabilities Document for Cyberspace Defense⁶² identified eleven capability gaps that are shown in Table 5. The gaps are prioritized based SME experience.

Prioritized Capability Gaps				
FINAL	NSSC	MEASURE		IDENTIFIED GAP
1	1	T2	C2 of Cyberspace Defense	There is no effective joint standardized Command and Control (C2) tactics process and organization for service, joint, coalition, and national cyberspace defense.
2	1	M2-1	Maintain Cyberspace Situational Awareness	There is no centralized ability to obtain or maintain cyberspace situational awareness over joint and national critical defense infrastructure, information, and information systems.
3	1	M2-2	Convene Cyberspace Threat Conference to Direct Attack Response Actions	There is a lack of capability to synchronize cyberspace defensive actions and operations in real-time with Combatant Commander (COCOM), National Security,

⁶² Joint Capabilities Document for Cyberspace Defense, Feb 2007

				and Homeland Defense operations.
4	1	M2-3	Time To Notify Users Of New Attacks/Threats/Countermeasures	There is no capability to immediately notify Services, COCOMs, National Security organizations, and Homeland Security organizations of cyberspace emergencies.
5	2	M2-4	Notify users of known vulnerabilities/responses	There is no capability to share lessons learned between Service, COCOM, National Security, and Homeland Security cyberspace operators.
6	3	M3-2	Systems with Trained Cyber/Information Operations Personnel	There is no joint cyberspace defense school for training personnel to protect and defend cyberspace information and systems in joint and multinational environments.
7	4	M1-1	Defend Against Cyberspace Attacks	There are shortfalls with the capabilities to protect the integrity of information, and information systems from external and internal threats in cyberspace
8	4	M3-3	Provide cyberspace defense plans	There are inconsistent policies for protecting end-to-end availability and assured access to cyberspace information, resources, and systems.
9	5	M4-2	Establish Cyberspace Defense Interoperability Standards for Information Systems	There is no structured joint approach for developing standardized and interoperable cyberspace defense qualities, aspects, features, and requirements in information systems.
10	5	M3-1	Perform Standards Verification	The standards that exist are very system-specific; there are no overarching joint standards for cyberspace defense evaluation.
11	5	M3-3	Provide cyberspace defense plans	There is a lack of capability to adequately plan cyberspace defensive actions with wartime, contingency, and disaster plans for COCOMs, National Security organizations, and Homeland Security organizations.

Table 11: Prioritized Capability Gaps

5.1 The DoD's reliance on technology has dramatically changed the way we fight wars, work with allies, coalitions, agencies, and protect our homeland. Cyberspace technology has literally allowed us to reduce the size of our forces to the point that we bring overwhelming technological might to bear on our adversaries instead of overwhelming manpower might. Our focus in cyberspace has primarily been on making us capable of doing more with smaller forces and more advanced equipment. Doing so continues to make us more and more vulnerable in the cyberspace domain. As we evolve, it can be reasonably stated that an adversary could bring our country to its knees if they take control of cyberspace and dominate the cyberspace domain.

5.2 The cyberspace domain continues to become a more relevant operational and strategic high ground. Therefore it is critical that cyberspace defense is a priority to allow us to maintain the cyberspace high ground and adequately defend our information and information systems. The threat is real and our national leaders are engaging to make sure we are ready. To quote The National Strategy to Secure Cyberspace (NSSC):

“Our economy and national security are fully dependent upon information technology and the information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same Internet that today connects millions of other computer networks making most of the nation's essential services and infrastructures work. These computer networks also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars, and stock markets, all of which exist beyond cyberspace. A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security.

The required technical sophistication to carry out such an attack is high—and partially explains the lack of a debilitating attack to date. We should not, however, be too sanguine. There have been instances where organized attackers have exploited vulnerabilities that may be indicative of more destructive capabilities. Uncertainties exist as to the intent and full technical capabilities of several observed attacks. Enhanced cyber threat analysis is needed to address long-term trends related to threats and vulnerabilities.

What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving. In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping U.S.

information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access.

In wartime or crisis, adversaries may seek to intimidate the Nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems. Cyber attacks on United States information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life.”

Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures.⁶³

The citation is a sobering reality for how failing to ensure superiority over the cyberspace domain can cripple our ability to maintain national security and the welfare of Americans. The note that “the required technical sophistication to carry out such an attack is high—and partially explains the lack of a debilitating attack to date”⁶⁴ shows that as our adversaries increase their technical sophistication, we too must increase our cyberspace defense readiness and capability.

6 Functional Solution Analysis

6.1 Ideas for Non-Materiel Approaches (DOTMLPF Analysis)

6.1.1 Do Nothing

6.1.1.1 The do nothing solution is the status quo option. That is, we continue pressing forward with current cyberspace defense constructs in place for each individual military service. The option continues to build on USSTRATCOM's supporting/supported relationships with each military service and the other combatant commanders. This solution, while not actually addressing any of our capability gaps effectively, is the baseline against which all other solutions are to be evaluated

6.1.2 Outsource Cyberspace Defense

6.1.2.1 The outsource cyberspace defense solution intuitively adheres to the Navy's approach for computer networks implemented to provide standard desktop services and support. The solution rolls up all cyberspace defense operations and support under one commercial contract administered by a joint entity.

6.1.3 Create Joint Cyberspace Defense School and Warfare Center

⁶³ The National Strategy to Secure Cyberspace, February 2003

⁶⁴ The National Strategy to Secure Cyberspace, February 2003

6.1.3.1 A Joint Cyberspace Defense School and Warfare Center will train cyberspace military personnel and develop joint cyberspace doctrine. The school would also ensure cyberspace personnel from all services get in-depth training in cyberspace tactics, operations, support, and deployment of cyberspace defense capabilities.

6.1.3.2 The stand-up and activation of a Joint Cyberspace Defense School and Warfare Center will provide a significant capability to make progress for defense of cyberspace. The combined school and warfare center would bring personnel from all services together to create a combined approach for defending cyberspace in a joint manner throughout the entire domain.

6.1.3.3 The school will also maintain active relationships and liaisons with other national cyberspace defense institutions as well as cyberspace defense institutions of our allies. This part of the solution is necessary to develop sound doctrine that will guide the nation's cyberspace defense current and future operations and capabilities. The approach will normalize and standardize operational and support tactics, techniques, and procedures across all DoD organizations. In addition, the combined school and center provides a joint atmosphere where senior cyberspace defense leaders can mold the future of cyberspace from a joint perspective, in a joint environment, to grow joint cyberspace defense personnel.

6.1.4 Develop Joint Cyberspace Defense Career Field

6.1.4.1 It is important for the DoD community to adequately align itself to make sure the strategic goals for cyberspace superiority are achieved. The significance of the cyberspace domain is well documented. The development of a joint cyberspace career field will allow the military to take highly qualified cyberspace personnel from all services to address the daunting tasks for defending cyberspace.

6.1.4.2 This approach does not include standing up a new cyberspace service. Creating joint cyberspace defense career fields is a broad approach to identify personnel across all services to be a part of a joint organized, trained, and equipped career field. Each member maintains their respective service relationship in much the same way as special operations personnel. Yet, they are given a joint cyberspace career field specialty, certification, or code and aligned in operational and staffing positions to defend cyberspace.

6.1.5 Modify Air Operations Center (AOC) for Cyberspace Defense C2

6.1.5.1 The existing AOC construct was developed for air and space operations, but could be modified for joint cyberspace defense operations. Since the AOC currently operates as a joint operations solution in peace and wartime environments, a modification to include the cyberspace defense mission is possible.

6.1.5.2 A center already exists to work on evolution of the AOC baseline. A modification of the AOC baseline would need to include an object oriented approach to allow the cyberspace defense capability to be employed across all services in an effort to enhance joint cyberspace defense operations.

6.1.6 Modify JTF-GNO mission/organization

6.1.6.1 The intent of this solution is to have JTF-GNO direct and command all joint cyberspace defense operations and support. The current organization only has joint oversight of computer network defense. A modification of the organization to align joint cyberspace personnel and capabilities directly under JTF-GNO would provide needed command direction over cyberspace defense operations.

6.1.6.2 The modification to the organization would include organize, train, and equip relationship between JTF-GNO and the service cyberspace defense personnel. The construct would allow JTF-GNO to work directly with the services to take a best of breed approach for capabilities and then field them quickly. The solution would allow the operational JTF-GNO commander to make final decisions that will ensure the services the joint community have a unified front and way ahead for cyberspace defense.

6.1.6.3 Ultimately, the relationship would allow JTF-GNO and the services to organize train and equip cyberspace personnel. However, JTF-GNO would have the ultimate say in how the joint force integrates to support combatant commanders, services and agencies.

6.1.7 Create a Joint Cyberspace Combatant Command

6.1.7.1 There are two options with respect to this solution. The first option is to follow a USSTRATCOM model where the supporting/supported relationships have virtual implementations and only the services have responsibility to organize, train, and equip.

6.1.7.2 The second option follows a USSOCOM model that does not include virtual relationships. Instead, joint trained cyberspace defense personnel are embedded with all COCOMs, services, and agencies. The embed personnel work for the Joint Cyberspace Combatant Commander and synchronize operations and planning by supporting the organizations where they're embedded. In this model the Joint Cyberspace Combatant Commander and the services both have responsibility to organize, train, and equip. In addition, the commander has overall decision making authority on standards and capabilities that are fielded for cyberspace defense.

6.2 Ideas for Materiel Approaches

6.2.1 Distributed Cyberspace Defense System (DCDS)

6.2.1.1 Development of a distributed cyberspace defense system is a materiel solution to being successful at cyberspace defense. The system would be scalable and integrated into DoD networks at all InfoCat levels. It would be able to watch all traffic both internal and external as well as logs on cyberspace information systems. The system would be able to correlate internal and external activity in cyberspace to identify coordinated attacks, attempted intrusions, suspicious activity, outages, etc...

6.2.1.2 The system is envisioned as a joint system and a deployment plan would be provided for the system throughout cyberspace. The distributed deployment of the system would provide cyberspace personnel the ability to see real-time events and activity to adequately defend cyberspace. The system should be developed to provide cyberspace personnel the ability to perform cyberspace defense patrols throughout DoD networks identifying vulnerabilities and suspicious activity.

6.2.1.3 The success of the system is how it is utilized to help synchronize operations in support of joint and service operations and support. Personnel must be adequately trained to utilize and operate the system. The training should include exercises to test the validity and effectiveness of the overall system.

6.2.1.4 The joint cyberspace community should be responsible for maintenance oversight of the system. In much the same way DISA provides infrastructure and access to the Global Information Grid, it appears that a joint cyberspace commander and their community should operate and maintain this system solution.

6.2.2 Joint Cyberspace Operations Center (J-COC)

6.2.2.1 Develop a dedicated cyberspace defense operations center. The operations center would enable command and control of all joint cyberspace defense operations across the globe.

6.2.2.2 The J-COC needs to have an overall joint role for all cyberspace defense operations and personnel. It is envisioned that the command operations for the cyberspace defense system described in section 6.2.1.

6.2.3 DoD-developed Operating System

6.2.3.1 This solution would provide for a DoD sourced and developed operating system for InfoCat C and higher systems. All information systems that are InfoCat C and higher would be required to operate on this system. The potential benefit of this solution is an expected decrease in operating system attacks on DoD secure systems, since the operating system would be less familiar to the entity executing the attack.

6.2.4 Paper DoD

6.2.4.1 A paper DoD solution would require all DoD action to be accomplished on paper. Paper infrastructure would need to be implemented DoD wide.

6.3 Analysis of Materiel/Non-Materiel Approaches (AMA)

6.3.1 Methodology

6.3.1.1 The Analysis of Materiel/Non-Materiel Approaches (AMA) necessarily considers the following feasibility factors against the solutions described in 6.2. For the cyberspace defense potential solutions we categorized the factors and assigned a SME weighting for each:

1. Technical Maturity – 0.2
2. Risk – 0.3
3. Supportability – 0.15
4. Survivability – 0.15
5. Affordability – 0.2

6.3.1.2 In addition, our rating scale w/in each feasibility factor was defined as 1-3 for each area, relative to the “do-nothing” approach, as specifics were impossible to discover without more subject matter experience. See Appendix A for the feasibility worksheet.

6.3.1.3 Technical maturity is defined as the result of answering the question “Can we achieve successful implementation of our solution with today’s technology?” For instance with the J-COC solution, the rating is a 2, as RDT&E is required to implement any solution. Similarly, with the Joint Cyberspace Combatant Commander solutions, a 1 was assigned as developing a new cyberspace command does not necessarily require new technology.

6.3.1.4 Risk is the intangible factor for including cost, schedule, performance, and political risk for each solution. Political and cost risk will be a significant barrier to any implementation, as the joint community may take a very long time to agree on and/or implement a formal solution set, even though the operational risk will only increase over time. In this sense, creating a joint cyberspace defense training school has less risk (1) than the creation of a new Cyberspace Defense Combatant Command (2).

6.3.1.5 Supportability is the answer to the question, “Do we have the ability to support the solution over the timeline to implement?” This question focuses on such items as estimates for manpower, equipment, etc... required for implementation of the solution. Almost all of the solutions are somewhat more difficult to support than the current structure, however, such things as creating a cyberspace defense school and warfare center were equally easy to implement relative to the “do-nothing” solution.

6.3.1.6 Survivability is defined as the long-term stability of the solution and how well the solution can be executed within the current threat environment. For instance, the “do-nothing” solution cannot be considered survivable given today’s threat environment; however outsourcing cyberspace defense can be considered a survivable strategy.

6.3.1.7 Affordability is simply the question of whether we afford to implement the solution within the timeline outlined at a cost that is reasonable. Estimates were gathered for what we expect each solution to cost. In this sense, outsourcing cyberspace defense appears very unaffordable with a cost of \$2B/yr (double what we think it should cost); whereas a cyberspace defense school and warfare center has an expected cost of around \$80M/yr (AFIT’s budget).

6.3.1.8 In addition to the formal AMA factors outlined above, the FSA must also address how well the solutions perform in successfully addressing the capability gaps. The full solutions performance matrix is in Appendix B. In addition, our analysis led to a roadmap for optimal implementation of the solution set.

6.3.1.9 Solution performance was rated based on how well the solution fills gaps, as identified and prioritized in the Cyberspace Defense JCD⁶⁵. We scored the expected performance of each solution against a “do-nothing” baseline. This activity led to an overall performance score for each solution. Next, each solution was analyzed using the AMA factors of technical maturity, risk, supportability, survivability, and affordability. Again these ratings were scored relative to the do-nothing baseline. Finally, each solution was given a timeliness factor, used to evaluate any order of precedence in determining which gaps were easiest to achieve. Our end result is a roadmap for implementation of a solution set that will result in all 11 capability gaps being adequately addressed within 9 years.

6.3.1.10 There were multiple assumptions that went into the analysis. 1) The prioritized Cyberspace Defense gaps from the JCD are the only capabilities being considered for improvement. Many of our solutions could be utilized to provide other Cyberspace capabilities, but those factors were not considered. 2) The weightings for the performance, feasibility factors and overall roll-up are appropriate. While we did perform some sensitivity analysis, all of our scores are on a relative scale to the do-nothing solution. 3) The prioritized gaps represent the value curve for desirability of effective solutions. If this were not true, the utility matrix developed is not representative of the actual utility of the solution space. Sensitivity analysis was accomplished comparing the JCD prioritized gap ranking and the NSSC gap ranking, and the analysis showed no change in the resulting solution set.

6.3.1.11 The DOTMLPF solution space was examined when developing our potential solutions. As a summary, capability gaps 1-4 concerned Command and Control, gaps 5 & 8-11 addressed organizational and administrative gaps, Cyberspace Defense was outlined in gap 7, and training shortfalls were captured in gap 6. As a result, our roadmap includes solutions that cross the entire DOTMLPF spectrum, with emphasis on organizational, training, and material solutions that adequately address all 11 prioritized gaps within 9 years.

6.3.2 Today’s Cyberspace Defense Capability

6.3.3 The baseline do-nothing solution contains the necessary descriptors for today’s methodology of addressing cyberspace defense (see section 6.1.1). In order to delineate our assessment of today’s capability, Table 6-1 is provided. All of the tables in section 6 show colors within the tables correspond to Fulfilled (Green), Yellow (Partially Fulfilled), and Red (Not Fulfilled) with respect to each capability gap listed.

⁶⁵ Joint Capabilities Document for Cyberspace Defense, Feb 07

GAP Description	Joint C2	Joint SA	Synchronize Ops	Notify of new threats	Share Lessons Learned	Joint Training	Defend against attack	Policy & doctrine	Joint Interoperability	Standards Verification	Adequate Planning
JCD GAP Ranking	1	2	3	4	5	6	7	8	9	10	11
TODAY – The ‘Do-Nothing’ approach											

Table 12: Today's Cyberspace Defense Capability (Gap Fulfillment)

6.3.4 Near Term (0-3 years)

6.3.4.1 Our roadmap for the near-term quickly addresses problems relating to organizational and administrative capability gaps. Through this implementation, we will have the best positioning to reach our end suite of capabilities.

6.3.4.2 In the near-term, the best solution evaluated for cyberspace defense is to establish the joint United States Cyberspace Combatant Command (USCYBERCOM). In addition, USCYBERCOM should be organized based on the USSOCOM model, where the new joint combatant command takes responsibility for organizing, training, and equipping personnel from all services and forming a uniformly capable joint Cyberspace force. This organizational solution resolves gaps 5 & 8-11 and enables the resolution of the remaining gaps. The organizational construct also still enables services to organize, train, and equip for cyberspace defense, but the services take their lead from the joint cyberspace combatant commander for everything cyberspace defense-related. Our sensitivity analysis determined that there are no reasonable analysis scenarios that would suggest a joint command based on the USSTRATCOM model, or a separate service for cyberspace would better address our cyberspace defense capability gaps, except to say that both alternatives were better than the baseline do-nothing approach. The reasoning behind this is that each service has personnel who are critical to successful cyberspace defense, but a single service lacks the breadth and joint focus to successfully defend DoD’s entire cyberspace.

6.3.4.3 In addition, the next two near-term solutions would enable the new USCYBERCOM to build and develop a cyberspace professional cadre of trained experts. Establishment of a joint Cyberspace Defense School and Warfare Center directly fulfills current training gaps, and would serve as the entry point for new cyberspace professionals that would be tracked and managed by distinct Cyberspace Operations career field managers. A cyberspace professional cadre composed of trained and experienced personnel in a unique career field is a critical enabler to fulfilling all capability gaps. Another plus is the school and warfare center will create a joint environment to develop doctrine that enhances our ability to form sound policies for cyberspace defense.

6.3.4.4 Finally, in order to begin addressing Command and Control gaps, another successful near-term solution would be to modify the existing JTF-GNO mission and organization to

encompass all of cyberspace defense. Table 6-2 addresses the resulting near-term phase of the roadmap.

GAP Description	Joint C2	Joint SA	Synchronize Ops	Notify of new threats	Share Lessons Learned	Joint Training	Defend against attack	Policy & doctrine	Joint Interoperability	Standards Verification	Adequate Planning
JCD GAP Ranking	1	2	3	4	5	6	7	8	9	10	11
NEAR TERM (0-3 Years) - Establish organizational groundwork & enable expertise needed to dominate the virtual battleground	Red	Red	Yellow	Yellow	Green	Green	Red	Green	Green	Green	Green
US Cyberspace Command (USCYBERCOM)	Red	Red	Red	Yellow	Green	Red	Red	Green	Green	Green	Green
Create Joint Cyberspace Defense School and Warfare Center	Red	Red	Red	Red	Red	Green	Red	Red	Red	Red	Red
Develop Cyberspace Defense career fields (enables development of Cyberspace Professional Cadre)	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red
Modify JTF-GNO mission/organization to include Cyberspace Defense	Red	Red	Yellow	Yellow	Yellow	Red	Red	Red	Red	Red	Red

Table 13: Near Term Cyberspace Defense Capabilities (Gap Fulfillment)

6.3.4.5 Furthermore, in order to achieve the long-term goals of cyberspace defense capabilities, the near-term requires RDT&E dollars to develop a Distributed Cyberspace Defense System (DCDS) and the weapon system for a Joint Cyberspace Operations Center (J-COC) (both solutions are outlined in sections 6.2.1 and 6.2.2).

6.3.5 Mid Term (3-6 years)

6.3.5.1 The mid-term solution set includes all of the solutions outlined in the near-term. Refinement of those solutions will be crucial to narrowing the capability gaps for cyberspace defense. For instance, the appointment of JTF-GNO to the mission and organization that is responsible for cyberspace defense may have to be revised under the new joint Cyberspace Combatant Command. The major activities in addition to solution refinement during this time period include deployment (IOC) of the DCDS & J-COC.

6.3.5.2 In the mid-term, the DCDS and J-COC will reach IOC. At which point, the JTF-GNO can hand over Cyberspace Defense operations to the J-COC. Table 6-3 illustrates the resulting mid-term phase of the roadmap.

GAP Description	Joint C2	Joint SA	Synchronize Ops	Notify of new threats	Share Lessons Learned	Joint Training	Defend against attack	Policy & doctrine	Joint Interoperability	Standards Verification	Adequate Planning
JCD GAP Ranking	1	2	3	4	5	6	7	8	9	10	11
MID TERM (3-6 Years) - Adds standard defensive equip & upgrades C2 node	Yellow	Yellow	Yellow	Yellow	Green	Green	Red	Green	Green	Green	Green
Near Term Capabilities	Yellow	Yellow	Yellow	Yellow	Green	Green	Red	Green	Green	Green	Green
IOC of Distributed Cyber Defense System	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red
IOC of Joint Cyber Operations Center – Replaces Modified JTF-GNO	Yellow	Yellow	Yellow	Yellow	Yellow	Red	Red	Red	Red	Red	Red

Table 14: Mid Term Cyberspace Defense Capabilities (Gap Fulfillment)

6.3.6 Far Term (6-9 years)

6.3.6.1 The far-term solution set involves finalizing deployment of the DCDS & J-COC. At the end of this time period the current capability gaps for Cyberspace Defense would be completely addressed (see Table 6-4).

GAP Description	Joint C2	Joint SA	Synchronize Ops	Notify of new threats	Share Lessons Learned	Joint Training	Defend against attack	Policy & doctrine	Joint Interoperability	Standards Verification	Adequate Planning
JCD GAP Ranking	1	2	3	4	5	6	7	8	9	10	11
FAR TERM (6-9 Years) - DCDS & JCOG go FOC	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Mid Term Capabilities	Red	Red	Yellow	Yellow	Green	Green	Red	Green	Green	Green	Green
FOC - Distributed Cyber Defense System	Red	Red	Red	Red	Red	Red	Green	Red	Yellow	Red	Red
FOC - Joint Cyber Operations Center	Green	Green	Green	Green	Yellow	Red	Red	Red	Red	Red	Red

Table 15: Far Term Cyberspace Defense Capabilities (Gap Fulfillment)

7 Final Recommendation

7.1 The FSA has provided a reasonable solution set for achieving baseline capabilities in cyberspace defense. The outcome of the FSA suggests that the new capabilities to be developed include development of a joint USCYBERCOM for DoD, creation of a Joint Cyberspace

Defense School and Warfare Center along with joint cyberspace career fields. In addition, the material solutions of a Distributed Cyberspace Defense System (DCDS) should be developed along with a Joint Cyberspace Operations Center (J-COC). As such, we recommend that DOTMLPF Change Recommendations (DCR's) be executed ASAP for the near-term organizational, training, and personnel actions necessary to achieve these solutions, and that Analysis of Alternatives (AOA's) be performed for the DCDS and J-COC material solutions. Additional ICDs are required to identify solutions for cyberspace attack and other aspects for cyberspace that will compliment cyberspace defense.

7.2 The solutions are presented as a roadmap, in order to quickly achieve a reasonable capability for cyberspace defense. Our information and information technologies are under constant attack, but we must first organize, train, and equip ourselves with the correct capabilities to execute cyberspace defense in joint and multi-national environments. Under the aggressive timeline proposed, the US would be light years ahead of other countries in creating an operational construct for effective defense of cyberspace.

Appendix B Feasibility Worksheet

Normalize 'do nothing' to 7's... set other options to 7 unless clearly improves the category
 3-4: Performs OK 5-6: Enablers 7: Same as doing nothing 8-9: Performs worse than today

Proposed Solutions:	Description:	On a Scale of 1-9, how much does the solution contribute to providing the capability desired? (1 is highest, 9 is lowest)											Performance Quantifiers				Time to implement			Feasibility Factors													
		GAP RANKING GAP VALUE		11	10	9	8	7	6	5	4	3	2	1	Gap Rank Solutions Analysis	NSSC Weighted Solution Analysis	Gap Rank Normalized to do nothing approach	NSSC Normalized to do nothing approach	1-3 yr	3-6 yr	6-9 yrs	Timeliness Factor	Tech Maturity	Risk	Supportability	Survivability	Affordability	Net Cost per year	Factor Feasibility	Normalized Factor Feasibility			
		Joint C2	Joint SA	Synchronize Ops	Notify of new threats	Share Lessons Learned	Joint Training	Defend against attack	Inconsistent Policy & doctrine	Joint Cyber defense interoperability	Perform Standards Verification	Provide adequate Planning																					
Priority/Weight assigned to value	NSSC RANKING VALUE	5	5	5	5	5	5	5	5	5	5	5																					
Do Nothing	Maintains Status Quo. Couched under Information Assurance and Operations. JTF-GNO sort of owns Cyberspace for DoD	7	7	7	7	7	7	7	7	7	7	7	462	231	1.00	1.00	N/A	N/A	N/A	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Material:	IOC	5	5	6	6	7	7	4	7	5	7	7	382	193	0.83	0.84				IOC			2	2	2	2	2	2	2	\$200M	2	0.98	
Distributed Cyber Defense System	FOC - Development, Acquisition, and implementation of new hardware and software for Cyberspace Defense. Would necessarily be designed to feed C2 structure.	5	5	6	6	7	7	1	7	5	7	7	361	185	0.78	0.80				RDT&E	FOC		2	2	2	2	2	2	2	\$50M	2	0.98	
Joint Cyber Operations Center	IOC	3	3	3	3	3	3	7	6	6	7	6	272	131	0.59	0.57				Build from JTF/GNO	IOC	FOC	2	2	2	2	2	2	2	\$80M	2	0.98	
DoD-developed Operating System (InfoCat C or better)	FOC - C2 system for Cyberspace. Create unique DoD operating environment so that defense is well-planned	7	7	7	7	7	7	6	4	6	6	7	186	87	0.40	0.38				RDT&E	IOC	FOC	2	1	2	2	2	2	2	\$20M	2	0.98	
Paper DoD	Acquisition of less technology-dependent DoD. Acknowledges that improved technology is making things harder to do.	7	7	7	7	7	7	6	4	6	6	7	434	220	0.94	0.95				RDT&E	IOC	FOC	2	1	2	2	2	2	2	\$200M	1.8	0.88	
		9	9	9	9	9	9	4	9	9	9	9	569	287	1.23	1.24				Not going to happen			1	3	3	3	1	3	3	\$1B	2.3	1.12	
Joint Cyberspace Commander Solutions:	Organization solution creating a formal hierarchy for Cyberspace implies C2 of both attack and defense																																
USSOCOM Model	Hierarchy founded on doctrinal understanding of tactics, releases embedded groups of personnel to other COCOM's in a supporting role. Cyber COCOM org, train, and equip.	4	4	5	3	1	5	5	1	1	1	1	225	113	0.49	0.49				Implement USSOCOM model, Org, train & equip.			1	1	2	2	2	2	2	\$300M	1.8	0.88	
USSTRATCOM Model	Hierarchy founded on centralized control of LD/HV assets, releases unique capabilities to COCOM's on demand while maintaining STRAT control. Services Org, Train, and equip.	4	4	5	3	3	6	5	3	2	2	2	259	129	0.56	0.56				Services Org, Train, And equip			1	1	2	2	2	2	2	\$300M	1.8	0.88	
New "Cyberspace Force"	Creation of new Service level agency. Operational Control of assets would be left to interpretation for new service. New Service would have to create their own DOTMLPF structure for Cyberspace	4	4	5	3	2	6	6	4	4	4	4	273	134	0.59	0.58				Use STRAT model	Cyber Service org, train, and equip		2	1	2	2	2	2	2	\$1.3B	2	0.98	
Other Non-Material Solutions:																																	
Realign Cyberspace Defense under the NSA	NSA presumed to have the infrastructure for creating and maintaining Cyberspace Defense Situational Awareness												0	0	0.00	0.00				Consolidate under STRAT model	Realign under NSA, FOC		2	1	2	2	2	2	2		1.8	0.88	
Outsource Cyberspace Defense	Hire an outside organization to create a secure environment for DoD cyberspace defense	4	4	3	4	4	6	5	1	1	1	1	242	123	0.52	0.53				Source Selection	FOC		2	1	2	2	2	2	2	\$2B	2	0.98	
Create Joint Cyberspace Defense School	School communicates new Cyberspace Defense concepts to affected AFSC's, MOS's, etc.	5	5	5	6	6	7	5	5	5	6	5	323	163	0.70	0.71				FOC			1	1	1	1	1	1	2	\$80M	1.2	0.59	
Develop Cyberspace Defense career fields	Creates Dedicated personnel for Cyberspace defense	6	6	6	6	6	6	6	6	6	6	6	396	198	0.86	0.86				FOC			1	1	1	1	1	1	1	\$1M	1	0.49	
Modify AOC to include Cyberspace Defense C2		4	4	4	4	4	7	6	6	7	7	6	317	155	0.69	0.67				IOC	FOC		2	1	3	3	2	1	1	\$30M	2.05	1.00	
Modify JTF-GNO mission/organization to include Cyberspace Defense		4	4	3	3	3	7	5	5	7	7	5	283	137	0.61	0.59				FOC			1	1	2	2	2	2	1	\$20M	1.6	0.78	
Gap Rank Sums:		72	72	75	71	72	94	74	78	77	85	78																					
Tech Maturity Definition:	Can we achieve success with today's technology																																
Risk Definition:	What is the risk of success within the time to implement																																
Supportability Definition:	Can we successfully support within the timeline to implement																																
Survivability Definition:	Will the solution survive in the current threat environment																																
Affordability Definition:	Will the solution be affordable within the timeline to implement																																

AppendixC Solutions Performance and Capability Gaps

Proposed Solutions: Priority/Weight assigned to value	On a Scale of 1-9, how much does the solution contribute to providing the capability desired? (1 is highest, 9 is lowest)											
GAP Description	Joint C2	Joint SA	Synchronize Cps	Notify of new threats	Share Lessons Learned	Joint Training	Defend against attack	Policy & doctrine	Joint Interoperability	Standards Verification	Adequate Planning	
JCD GAP Ranking	1	2	3	4	5	6	7	8	9	10	11	
Do Nothing	7	7	7	7	7	7	7	7	7	7	7	
TODAY	7	7	7	7	7	7	7	7	7	7	7	
NEAR TERM (+3 Years) - Establish organizational groundwork & enable expertise needed to dominate the virtual battleground	4	4	3	3	1	1	5	1	1	1	1	
US Cyberspace Command (USCYBERCOM)	4	4	5	3	1	5	5	1	1	1	1	Strat evolves into USCYCOM, based on SOCOM model.
Create Joint Cyberspace Defense School	5	5	5	6	6	1	5	5	5	6	5	Stands up schoolhouse to prepare cyber-experts
Develop Cyberspace Defense career fields	6	6	6	6	6	6	6	6	6	6	6	Manage career field... grandfather current experts & produce newbies through school
Modify JTF-GNO mission/organization to include Cyberspace Defense	4	4	3	3	3	7	5	5	7	7	5	
MID TERM (+6 Years) - Adds standard defensive equip & upgrades C2 node	3	3	3	3	1	1	4	1	1	1	1	
Near Term Capabilities	4	4	3	3	1	1	5	1	1	1	1	
IOC - Distributed Cyber Defense System	5	5	6	6	7	7	4	7	5	7	7	IOC - Say... critical assets covered...
IOC - Joint Cyber Operations Center	3	3	3	3	3	7	6	6	7	7	6	IOC - Receives SA data on criticals
FAR TERM (+9 Years) - DCDS & JCOC go FOC	1	1	1	1	1	1	1	1	1	1	1	
Mid Term Capabilities	4	4	3	3	1	1	5	1	1	1	1	
FOC - Distributed Cyber Defense System	5	5	6	6	7	7	1	7	3	7	7	FOC - All assets covered...
FOC - Joint Cyber Operations Center	1	1	1	1	3	7	5	5	7	7	5	FOC - SA data on all

AppendixD Cyberspace Defense Tasks and Measures of Effectiveness Analysis

Rolled-up Cyber Defense Measures and suggested corresponding units.
 Generic Conditions for each measure are provided in section 3.1.2

Task 1. Defend Cyberspace Information & Systems

MOE	MOE Title	Description	Unit
M1-1	Percent of Cyberspace attacks successfully defended	# of defended attacks / # of total attacks	Percent
M1-2	Time to Investigate & Report Impact, Post-Attack	Interval is time from the completion of the attack, to the successful release of post-attack report	Minutes
M1-3	Time to Recover, Post-Attack	Interval is time from the completion of the attack, to reestablishment of fully operational capability	Minutes

Task 2. Command and Control of Cyber Defense

MOE	MOE Title	Description	Unit
M2-1	Maintain Cyberspace Situational Awareness	# of critical nodes effectively monitored / # of total critical nodes	Percent
M2-2	Convene Cyberspace Threat Conference to Direct Attack Response Actions	# of CTCs convened when required / # of CTCs required	Percent
M2-3	Time to notify users of known Attacks/Threats/Countermeasures	Interval is time of awareness of threat by central authority to time of distribution of information to users	Minutes
M2-4	Time to notify users of known vulnerabilities/Responses	Interval is time of awareness of vulnerability by central authority to time of distribution of information to users	Hours

Task 3. Organize, Train, and Equip Cyberspace

MOE	MOE Title	Description	Unit
M3-1	Perform Standards Verification	# of information systems with current standards verification / total # of information systems	Percent
M3-2	Percent of Trained Cyber/Information Operations Personnel	# trained and available personnel / # of needed personnel	Percent
M3-3	Provide Cyberspace Defense Plans		Yes/No

Task 4. Test and Acquire Secure Information Systems

MOE	MOE Title	Description	Unit
M4-1	Percent of Information Systems meeting Availability Standards	# meeting availability standards / # total IS	Percent
M4-2	Percent of Information Systems meeting Interoperability Standards for Cyberspace Defense	# meeting interoperability standards / # total IS	Percent

Tasks and Measures on this sheet Support the "Defend Cyber Information Systems" master Task					
UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure
SN 2.5.3	Provide Sensitive Compartmentalized Information (SCI) Networks for the Intelligence Community	Provide Joint Worldwide Intelligence Communications System (JWICS).	System is fully operational.	Percent/Time	M4-1
SN 3.4.6	Coordinate Protection of National Strategic Information, Information-Based Processes, and Information Systems	To coordinate the protection of information, information-based processes, and information systems by planning and implementing comprehensive defensive information operations (IO) measures.	Of confirmed loss of classified data from penetrations.	Instances	M1-2
			Of detected penetrations of command information systems.	Instances	M1-1
			Of time, command joint information systems down.	Percent	M4-1
			To switch to an alternate system after attack on major information system.	Minutes	M1-3
			To restore major information system after attack.	Minutes	M1-3
			To detect attempted penetration of information system.	Minutes	M1-1
			Of penetrations of multiple command information systems.	Instances	M1-1

SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Of operational C4 networks and nodes available.	Percent	M4-1
			Of operational C4 networks and nodes reliable.	Percent	M4-1
			To restore information systems to fully operational status after a successful penetration and attack.	Percent	M1-3
			Of time available for nuclear command control (NC2) C4I systems to transmit situation monitoring tactical warning and attack assessment (TW/AA) messages within established guidelines.	Percent	M3-1
SN 5.1.2.1.3	Provide Global Internet Protocol (IP)-Based Networks for Classified and Unclassified Information	To provide interoperable, secure IP data communications services.	Of access circuit availability.	Percent	M4-1
			Of access circuit quality of service - latency.	Percent	M4-1
			Of access circuit quality of service - packet loss rate.	Percent	M4-1
			To provision/implement services.	Days	M4-1
			Of satellite constellation availability.	Percent	M4-1

SN 5.1.2.1.4	Provide Global Communications and Networks for Video Services	To provide global video service capabilities, ranging from network delivery of video of live events and real time video communications sessions among people who are geographically dispersed to delivery of video from prerecorded video files.	Of video services network availability.	Percent	M4-1
			Outages of video services network that impact a general/flag officer-level video teleconferencing session.	Yes/No	M4-1
SN 5.1.2.1.7	Provide Community of Interest Global Networks for the Department of Defense	Provide community of interest (COI) networks to select users. COI are sets of users who have shared goals, shared interests, shared mission or business processes, and agreed-upon terms of behavior.	Of community of interest access circuit availability.	Percent	M4-1
			Of community of interest access circuit quality of service - latency.	Percent	M4-1
			Of community of interest access circuit quality of service - packet loss rate.	Percent	M4-1
			Community of interest bandwidth available.	Yes/No	M4-1
			To provision/implement services.	Days	M4-1
SN 5.5	Coordinate Worldwide Information Operations	To coordinate the elements of offensive and defensive IO	Of US national-level IO plans or objectives being delayed, defeated, or disrupted due to adversary offensive IO actions.	Instances	M1-2

SN 5.5.2	Conduct Defensive Information Operations	To perform authorized actions to protect, monitor, analyze, detect, and respond to unauthorized activity within national security information systems and computer networks	To identify qualified personnel, determine availability of equipment, and initiate technical surveillance service of customers.	Days	M3-2
			To identify analysis team required to perform network evaluations.	Days	M3-2
			To complete network evaluations after team identification.	Days	M2-1
			To assess customer network security posture.	Days	M2-1
			To provide network security assessment to customer.	Days	M3-1
SN 5.5.3	Provide Regional NetOps to Support the Global Information Grid (GIG)	Execute GIG NetOps and defense.	Capabilities measured in subtasks linked to selected combatant command OPLANS	Yes/No	M1-1
SN 5.5.3.1	Provide Network Management for the Theater Information Grid (TIG) Transport and Computer Network Infrastructures	Equip, train, maintain, and sustain the theater-level NetOps centers to enable them to manage and control the command, control, communications, computer systems, and networks, including space systems that define the TIG transport infrastructure within their AOR.	Heating and air conditioning systems are available/operational to enable the TNC to accomplish NETOPS S&NM missions.	Yes/No	Infrastructure
			Power, generators, and grounding systems are available/operational to enable the TNC to accomplish NETOPS S&NM tasks.	Yes/No	Infrastructure

SN 5.5.3.2	Protect and Defend the Theater Information Grid (TIG)	To collect and consolidate TIG intrusion detection reports and data, assessing the compiled data, and reporting the results to the appropriate command authorities.	To alert TIG users and the Global NetOps Center (GNC) to presence of critical information assurance Information Assurance/Computer Network Defense (IA/CND) events that affect the TIG.	Minutes	M2-3
			Of Information Assurance Vulnerability Alert (IAVA) compliance distribution process for notifying Theater combatant commanders, the Services, and Defense agencies about vulnerability alerts and countermeasures information.	Percent	M2-4
			Of TIG computer assets that are compliant or operating with approved extensions and mitigation plans with negligible risk on information systems capability to perform required theater missions	Percent	M3-1
			Of TIG networks compliant or operating with approved extensions and mitigation plans with negligible risk on information systems capability to perform required theater missions.	Percent	M3-1
			Of TIG IA/CND status information currently available.	Percent	M4-1
ST 5.5	Conduct Theater-Wide Information Operations (IO)	To conduct information operations for implementing the Secretary of Defense's national military strategy, policy, objectives and operations at the theater level.	Are appropriate allied and coalition IO resources and capabilities factored into theater IO plans?	Yes/No	M3-3

			Of mission essential US command, control, communications, computers, and intelligence surveillance and reconnaissance (C4ISR) systems remaining after enemy command and control (C2) attack.	Percent	M1-2
			Of information systems capable of instantaneous detection of hostile attack and incorporating fully automated defend/repair/restore capabilities.	Percent	M1-1
			Of enemy operations disrupted, cancelled, or modified, attributable to IO plan.	Percent	M1-1
ST 6.3.5	Protect Theater Information Systems	To coordinate theater-wide activities to protect and defend information and information systems. This task includes integrating and synchronizing indigenous and joint force capabilities for defensive IO, ranging from technical security measures (such as INFOSEC) to procedural measures (such as counterintelligence, physical security, and hardening of communications nodes).	Do commands responsible for design, operation and maintenance of information systems perform risk assessments of potential IO threats and take appropriate action to respond to those risks that meet the appropriate criteria?	Yes/No	M3-1

			Do commands responsible for design, operation and maintenance of information systems have IA or defensive IO memorandums of understanding with commercial communications providers who support information systems?	Yes/No	M3-1
			Do commands responsible for design, operation and maintenance of information systems use "Red Teams" to identify vulnerabilities in those systems?	Yes/No	M3-1
			Of theater strategic C4I systems not protected by firewalls, virus detection software and other appropriate defensive IO measures.	Percent	M3-1
			Of information system hardware and software components that have backup components to replace them if they fail or are corrupted.	Percent	M3-1
			Of redundant communications paths available to connect information systems.	Number	Solution
			Of information systems being disabled, corrupted or compromised through identified adversary IO actions or criminal mischief.	Instances	M2-1

			For appropriate Computer Emergency Response Teams (CERTs) to respond, identify and correct information system failures attributed to adversary IO action or criminal mischief.	Hours	M3-1
			To restore primary local area network (LAN) in command center.	Hours	M1-3
			Of allies with which joint information security agreements exist.	Percent	M2-1
			Of information systems within high security area.		M2-1
			Of adversary trusted sources (systems and personnel) under friendly control.	Percent	M2-1
			Of adversary penetrations of friendly information systems are identified and targeted	Percent	M2-1
			For Computer Emergency Response Team (CERT) to respond and report attack to the information operations officer (IOO), from notification of attack.	Time	M2-1
			For CERT to implement Information Conditions (INFOCON) Updates, and disseminate information to the command and TFs, from IOO determines INFOCON.	Time	M1-1
			For task forces to implement INFOCON change and report completion status.	Time	M2-1, M3-1

OP 6.3	Protect Systems and Capabilities in the Joint Operations Area	To identify critical information and subsequently analyze friendly actions attendant to planning and conducting campaigns and major operations to identify those actions that can be observed by adversary intelligence systems	Of attempted adversary penetrations of friendly information systems successful.	Percent	M1-1
			Of enemy's sensor coverage known.	Percent	M2-1
			Of information systems within high security area.	Percent	M3-1
			Of command net secured.	Percent	M2-1, M3-1
OP 6	Provide Operational Force Protection	To conserve the force's fighting potential so that it can be applied at the decisive time and place. This activity includes actions taken to counter the enemy's forces by making friendly forces (including operational formations, personnel, etc.), systems, and operational facilities difficult to locate, strike, and destroy.	Of friendly communications hardened or redundant.	Percent	M3-1
			Reduction in friendly LOC capacity.	Percent	M1-2
OP 6.5.3	Protect/Secure Operationally Critical Installations, Facilities, and Systems	To protect operationally critical installations, facilities, and systems from attack in the operational area.	For internal/external reaction force to reach installation or facility under attack.	Hours	M1-3
			Of operations delayed, disrupted, canceled or modified.	Instances	M1-2
			Of terrorists acts against coalition forces in OA.	Instances	M1-2
			Of terrorists acts against US forces in OA.	Instances	M1-2

			Of communications in operational area supporting operation hardened.	Percent	M3-1
			Of communications in operational area supporting operation with alternate paths.	Percent	M3-1
			Of critical friendly facilities (e.g., PODs, command posts) destroyed, damaged, or rendered inoperable by sabotage or insurgents or terrorist actions.	Percent	M1-2
			Of critical friendly facilities hardened or protected against hostile acts.	Percent	M3-1
			Of terrorist attacks penetrate security in operational area.	Percent	M1-2
			Reduction in LOC capacity resulting from enemy attacks.	Percent	M1-2
			To coordinate for additional assets for theater LOCs.	Hours	Solution
			Of threat assessments passed within established criteria.	Percent	M3-1
			Command has established executable antiterrorism program.	Yes/No	M3-1
			Command has established procedures to change force protection conditions.	Yes/No	M3-1
			Command has procedures to respond to terrorist use of CBRNE weapons.	Yes/No	M3-1
			Antiterrorism/security plan is coordinated, approved, and executable.	Yes/No	M3-1

			Compliance with DOD antiterrorism standard.	Yes/No	M3-1
--	--	--	---	--------	------

Tasks and Measures on this sheet Support the "Defend Cyber Information***" master Task					
*** After analysis this task was combined with Defend Information Systems Task ***					
UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure
SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Of traffic sent on nondedicated or non-DOD lines or channels.	Percent	M4-1
SN 5.5	Coordinate Worldwide Information Operations	To coordinate the elements of offensive and defensive IO	To modify national-level IO plans and actions due to operational contingencies.	Hours	M3-3
			Of national-level IO cell nominated "targets" struck with lethal or nonlethal means during the timeframe planned for in the IO appendix or other planning document	Percent	Offensive Measure
SN 5.5.1	Conduct Strategic Information Operations	To conduct offensive and defensive IO for implementing Presidential and SecDef national military strategy, policy, objectives, and operations at the strategic level.	To implement measures for full spectrum IO in support of global computer network defense (CND) mission.	Hours	M1-1

SN 5.5.3.2	Protect and Defend the Theater Information Grid (TIG)	To collect and consolidate TIG intrusion detection reports and data, assessing the compiled data, and reporting the results to the appropriate command authorities.	Of unauthorized access (root, user, privileged) to Mission Assurance Category (MAC) I, MAC II, and MAC III systems and networks within the TIG since last reporting period.	Percent	M1-1
ST 1.6.4	Gain and Maintain Information Superiority in Theater	To achieve information superiority by affecting an adversary's information, information-based processes, and information systems, while defending one's own information, information-based processes, and information systems.	Of friendly communications traffic delayed, disrupted, or corrupted by adversary IW/C2W.	Percent	M2-1
			Without significant security breach.	Weeks	M3-1
ST 5.5	Conduct Theater-Wide Information Operations (IO)	To conduct information operations for implementing the Secretary of Defense's national military strategy, policy, objectives and operations at the theater level.	Of US or allied plans or objectives in theater being delayed, defeated, or disrupted due to adversary offensive IO actions.	Instances	M2-1
			To conduct battle damage assessment of IO "targets" struck with lethal and nonlethal means after receipt of information.	Days	M1-2
			Of theater level IO objectives verifiably achieved.	Percent	M2-1
			Delay to operations because of the lack of information security.	Days	M1-2
			To achieve information superiority after crisis onset.	Days	M2-1
ST 5.5.2	Control Theater Information Operations (IO)	To monitor and adjust the theater IO efforts during execution.	To achieve information superiority after crisis onset.	Days	M2-1

OP 6.2.14	Employ Operations Security (OPSEC) in the Joint Operations Area	To employ OPSEC measures to deny critical information necessary by an adversary commander to accurately estimate the military situation.	Before joint force knows of possible compromise of EEFI.	Hours	M2-1
			To develop critical info list from EEFI.	Hours	M2-1
			Of identified friendly vulnerabilities exploited by enemy action.	Percent	M1-2
			Of joint operations disrupted as result of enemy detection and response.	Percent	M1-2
OP 6.3.2	Supervise Communications Security (COMSEC)	To supervise the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.	Of frequency allocation or frequency management failing to prevent signal fratricide.	Instances	M1-2
			Of interceptions of friendly communications during planning and execution.	Instances	M1-2
			Of communications encrypted.	Percent	M3-1
			Of communications sent by secure means.	Percent	M3-1

OP 6.4	Conduct Military Deception in Support of Subordinate Campaigns and Major Operations	To manipulate enemy operational level commander's perceptions and expectations into a false picture of reality that conceals friendly actions and intentions until it is too late for enemy forces to react effectively within the context of the geographic combatant commander's deception plan.	Of EEFI/Critical Information addressed in deception plan.	Percent	M3-3
			Of enemy forces deployed to deal with deception threat.	Percent	M2-1
			Of deception plans not including smoke and obscurants.	Instances	M3-3
TA 5.6	Employ Tactical Information Operations	Tactical Information Operations (TIO) employed by joint services produce tactical information and gain, exploit, defend, or attack information or information systems.	Identified processes have fully integrated all available capabilities to ensure a defense in depth. Should be integrated in all military operations, to include activities by other government and nongovernment agencies or organizations.	Percent	M3-3
			Of friendly operations delayed, disrupted, or degraded due to ineffective tactical information operations.	Percent	M1-2
SN 3.4.4.1	Support Force Protection	To provide assessments which ensure mission survivability to critical facilities by determining single point vulnerabilities, mitigation techniques and/or enhanced force protection postures.	To provide written report of observations/vulnerabilities to the combatant commander with mitigating options.	Days	M2-4

			Of identified defensive measures validated by installation / unit commander to ensure the physical security of personnel, facilities, and equipment.	Percent	Infrastructure
			Of the time Force Protection (FP) enhancement recommendations have been taken to reduce risk from threats to acceptable levels based on FP operational risk assessment.	Percent	M4-2
			To determine FP enhancement processes/procedures/facility modifications, etc and provide "answer" to the combatant commander.	Days	M2-4
			Of required installations receive periodic Force Protection Assistance Visits.	Percent	M3-1
			To respond to combatant command request; complete plans review process.	Months	M3-1
			Of Research and Development (R&D) funding used to meet Defense Technology Objectives (DTOs) in the Scientific and Technical (S&T) Reliance Process to meet current and future requirements.	Percent	M4-1

Tasks and Measures on this sheet Support the "C2 of Cyber Defense" master Task					
UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure

SN 3.4.6	Coordinate Protection of National Strategic Information, Information-Based Processes, and Information Systems	To coordinate the protection of information, information-based processes, and information systems by planning and implementing comprehensive defensive information operations (IO) measures.	Of commands have adequate information processing hardware and software.	Percent	M3-1
			Of commands have current processes and programs to protect information systems, processes, and networks.	Percent	M3-1
			Of commands have fully trained and manned information systems management and operating personnel.	Percent	M3-2
			Of time, command joint information systems down.	Percent	M4-1
			Organization applies resources to protect against IO, detect and react to offensive IO, and restore capabilities should defensive measurers fail.	Yes/No	M1-1, M1-2, M1-3
			To implement countermeasures in response to a confirmed intrusion.	Minutes	M1-1
			To activate a change in information condition (INFOCON) in response to increased threats or actual activity.	Minutes	M2-3
			To switch to an alternate system after attack on major information system.	Minutes	M1-3
			Of penetrations of multiple command information systems.		M1-2

SN 5.1	Operate and Manage Global Strategic Communications and Information Systems	To receive information and data on the strategic situation worldwide, including: combatant command, theater component command, and operational level command missions, disposition of friendly and enemy forces, strategic centers of gravity, and characteristics of the theater areas (worldwide).	To begin transmitting force direction (FD) emergency action message (EAM) to bombers, tankers (positive control launch (PCL) only) (availability of individual Nuclear Command and Control System (NCCS) command, control, communications, computers, and intelligence (C4I) systems).	Minutes	M3-1
			To begin transmitting force management (FM) messages to bombers/tankers/intercontinental ballistic missile('s) (ICBM's) (availability of National Military Command System (NMCS) and combatant commander C4I systems).	Minutes	M3-1
			To begin transmitting FM messages to bombers/tankers/ICBMs (availability of bomber/tanker/ICBM NCCS C4I systems).	Minutes	M3-1
			To begin transmitting situation monitoring (SM), threat warning (TW), and attack assessment (AA) messages (availability of NCCS C4I systems).	Minutes	M3-1
			To begin decision-making conference.	Minutes	M2-2

SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Interact with the NMCS network and nodes to obtain or send strategic information.	Hours	
SN 5.5	Coordinate Worldwide Information Operations	To coordinate the elements of offensive and defensive IO	National-level IO coordination policies and procedures exist.	Yes/No	M3-1
			To identify qualified personnel from various elements and activities and augment national-level IO planning cell after onset of planning requirement.	Hours	M3-3
			To identify required national-level IO information necessary for IO planning after onset of planning.	Hours	M3-3
			To task intelligence community and other national-level support organizations and agencies to fill information requirements for IO planning.	Hours	M3-3
			Of identified national-level IO information requirements unfilled at time-critical points in planning process.	Percent	M3-3
			To get interagency approval for proposed national or subordinate level IO plans and actions.	Days	M3-3
			Of uncoordinated IO actions at different levels (national, theater, AOR) or different theaters causing disruption or delay of US plans and objectives.	Instances	M3-3, M2-1

			Of national-level IO objectives verifiably achieved.	Percent	M2-1
SN 5.5.1	Conduct Strategic Information Operations	To conduct offensive and defensive IO for implementing Presidential and SecDef national military strategy, policy, objectives, and operations at the strategic level.	Of planners with access to the information operations (IO) plan within 12 hours of plan initiation message.	Percent	M3-3
SN 5.5.3.3	Provide a Common Operational Picture (COP)	To provide an integrated capability to receive, correlate, and display, functional and operational pictures of systems and networks and the integrated view(s) of networks that display network health, security status, and information sources.	Of availability of the TIG integrated COP delivery to the GNC.	Percent	M4-1
			Of ESM/NM operations information integrated into the TIG COP.	Percent	M3-3
			Of IA/CND information integrated into the TIG COP.	Percent	M3-3
SN 8.3.5	Coordinate DOD/Government Information Operations (IO)	To work with the Services, combatant commands, and civil/military agencies on issues involving offensive and defensive IO.	Development and approval of information operations.	Yes/No	M4-2
ST 5.5	Conduct Theater-Wide Information Operations (IO)	To conduct information operations for implementing the Secretary of Defense's national military strategy, policy, objectives and operations at the theater level.	To task intelligence community and other theater level support organizations and agencies (including those of allies where appropriate) to fill information requirements for IO planning.	Hours	M3-3
			Of identified theater level IO information requirements unfilled at time-critical points in planning process.	Percent	M3-3

			To get theater level approval for proposed IO plan.	Hours	M3-3
			To respond to subordinate command requests for IO support or coordination.	Hours	M3-3
			Of uncoordinated IO element or activity actions within theater causing disruption or delay of US or allied plans and objectives.	Instances	M3-3
			To modify theater level IO plans and actions due to operational contingencies.	Hours	M3-3
			Of planners with access to the IO plan within 12 hours of plan initiation message.	Percent	M2-3
ST 5.5.1	Plan and Integrate Theater-Wide Information Operation (IO)	To plan theater-wide IOs, integrating military operations and non-DOD USG activities.	Does a theater level IO cell exist?	Yes/No	M3-1
			To task intelligence community and other theater level support organizations and agencies (including those of allies where appropriate) to fill information requirements for IO planning.	Hours	M3-3
			Of identified theater level IO information requirements unfilled at time-critical points in planning process.	Percent	M3-1
			Are appropriate allied and coalition IO resources and capabilities factored into theater IO plans?	Yes/No	M3-3
			To get theater level approval for proposed IO plan.	Hours	M3-3

			To respond to subordinate command requests for IO support or coordination.	Hours	M3-3
ST 5.5.2	Control Theater Information Operations (IO)	To monitor and adjust the theater IO efforts during execution.	Of uncoordinated IO element or activity actions within theater causing disruption or delay of US or allied plans and objectives.	Instances	M1-2
			To modify theater level IO plans and actions due to operational contingencies.	Hours	M1-1, M2-1, M3-3
			Of US or allied plans or objectives in theater being delayed, defeated, or disrupted due to adversary offensive IO actions.	Hours	M1-2
			To conduct battle damage assessment of IO "targets" struck with lethal and nonlethal means after receipt of information.	Days	M2-1
			Of theater level IO objectives verifiably achieved.	Percent	M2-1
			To change IO plan upon receiving status updates to ensure supporting elements of IO plan coordinate actions.	Hours	M3-3

OP 5.6	Coordinate Operational Information Operations (IO)	To coordinate the use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, in order to deny information, influence, degrade, or destroy adversary information, information-based processes, and information systems, and to protect one's own against such actions.	To get JFC approval for proposed operational IO plans and actions.	Hours	M3-3
OP 6.2.14	Employ Operations Security (OPSEC) in the Joint Operations Area	To employ OPSEC measures to deny critical information necessary by an adversary commander to accurately estimate the military situation.	Of information (pieces or types) commander needs to make decision listed as FFIR.	Items	n/a
			Of information (pieces or types) commander needs to make decision listed as PIR.	Items	n/a
			Of information (pieces or types) joint force needed to protect itself listed as EEFI.	Items	n/a
TA 5.6	Employ Tactical Information Operations	Tactical Information Operations (TIO) employed by joint services produce tactical information and gain, exploit, defend, or attack information or information systems.	Actions taken must be appropriate to the situation and consistent with US objectives. They must be permissible under the law of armed conflict, consistent with applicable domestic and international law, and in accordance with applicable rules of engagement.	Percent	M3-1

Tasks and Measures on this sheet Support the "Organize, Train, and Equip" master Task					

UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure
SN 3.4.6	Coordinate Protection of National Strategic Information, Information-Based Processes, and Information Systems	To coordinate the protection of information, information-based processes, and information systems by planning and implementing comprehensive defensive information operations (IO) measures.	Organization applies resources to protect against IO, detect and react to offensive IO, and restore capabilities should defensive measurers fail.	Yes/No	M1-1,M1-2, M1-3
			To detect attempted penetration of information system.	Minutes	M1-2
SN 5.1.1.1	Provide Information Assurance Products and Services	To provide products, services, infrastructure, and capability to assure availability and appropriate application of evaluated/validated products and solutions.	Of fully qualified Information Systems Security Engineers as a percentage of required.	Percent	M3-2
			Of quick response requirements met by existing inventory of equipment and parts stockpiles.	Percent	M3-1
SN 5.1.1.3	Provide Information Assurance Education and Awareness	To prepare individuals, leaders, and organizations to accomplish mission activities in coordination with multination, interagency, nongovernmental, private voluntary and United Nations (UN) agencies/forces/organizations. This task applies to providing guidance on national information assurance (IA) policy and foreign information exchange.	To identify knowledgeable personnel to research and interpret policy or procedural solutions.	Days	M3-2
			To provide policy interpretation/information to the customer.	Days	

			To publish validated/evaluated information assurance security issues.	Days	M2-3, M3-4
SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Of communications systems provide access by intelligence personnel to consumers.	Percent	M4-1
SN 5.5	Coordinate Worldwide Information Operations	To coordinate the elements of offensive and defensive IO	National-level IO planning/coordination cell exists.	Yes/No	M3-3
			National-level IO planners from all appropriate US departments, agencies and organizations are involved in development and coordination of national IO plans and actions.	Yes/No	M3-3
			To conduct combat assessment of national IO "targets" struck with lethal and nonlethal means.	Hours	M2-1
			Of national IO cell nominated "targets" attacked when called for after combat assessment of initial strike.	Percent	offensive measure
SN 5.5.1	Conduct Strategic Information Operations	To conduct offensive and defensive IO for implementing Presidential and SecDef national military strategy, policy, objectives, and operations at the strategic level.	To provide assistance in the preparation and legal review of a request for supplemental ROE.	Hours	M3-3

			To provide assistance in the preparation and legal review of a review and approval package (RAP) in connection with computer network operations (CNO).	Hours	M3-3
SN 5.5.3.1	Provide Network Management for the Theater Information Grid (TIG) Transport and Computer Network Infrastructures	Equip, train, maintain, and sustain the theater-level NetOps centers to enable them to manage and control the command, control, communications, computer systems, and networks, including space systems that define the TIG transport infrastructure within their AOR.	Of authorized personnel on hand.	Percent	M3-2
			Of theater-level network operations center (TNC) personnel trained/certified to perform network operations (NETOPS) systems and network management (S&NM) tasks.	Percent	M3-2
			TNC is organized under the NETOPS CONOPS.	Yes/No	M3-1
SN 8.3.5	Coordinate DOD/Government Information Operations (IO)	To work with the Services, combatant commands, and civil/military agencies on issues involving offensive and defensive IO.	Identifications and organization of appropriate agencies and organizations to support interagency process.	Yes/No	M4-2
			Recommended versus approved DOD capabilities and activities employed in support of information operations tasks.	Percent	M3-3

ST 5.1.6	Establish Information Assurance (IA) Procedures	To establish information assurance procedures for deployed operations.	Do commands responsible for design, operation, and maintenance of theater strategic C4 systems have IA and defensive IO policies and procedures?	Yes/No	M3-1
			IA included in the command's plans and orders.	Yes/No	M3-1
			To appropriately respond to indications of hostile (domestic or foreign) information attack.	Minutes	M1-1
ST 5.5	Conduct Theater-Wide Information Operations (IO)	To conduct information operations for implementing the Secretary of Defense's national military strategy, policy, objectives and operations at the theater level.	Do theater level IO coordination policies and procedures exist?	Yes/No	M3-1, M3-3
			Does a theater level IO cell exist?	Yes/No	M3-1
			Are theater IO planners involved in identifying IO targets, deconflicting with conventional and other targeting efforts, and coordinating with conventional targeting efforts for enhanced effects-based operations within all plans?	Yes/No	M3-1
			To identify qualified personnel from various elements and activities and augment theater level IO planning cell after onset of planning requirement.	Hours	M3-3
			To identify required theater level IO information necessary for IO planning after onset of planning.	Hours	M3-3

ST 6.3.5	Protect Theater Information Systems	To coordinate theater-wide activities to protect and defend information and information systems. This task includes integrating and synchronizing indigenous and joint force capabilities for defensive IO, ranging from technical security measures (such as INFOSEC) to procedural measures (such as counterintelligence, physical security, and hardening of communications nodes).	Of licensed system administrators for critical C4I systems.	Percent	M3-2
			Of system administrators with full OPSEC training.	Percent	M3-2
			Of system administrators with full information system security training.	Percent	M3-2
			Of personnel familiar with command policies on information security.	Percent	M3-2
OP 6.2.14	Employ Operations Security (OPSEC) in the Joint Operations Area	To employ OPSEC measures to deny critical information necessary by an adversary commander to accurately estimate the military situation.	Of units equipped with antisurveillance sensor and sensor jamming devices.	Percent	M4-1
OP 6.3	Protect Systems and Capabilities in the Joint Operations Area	To identify critical information and subsequently analyze friendly actions attendant to planning and conducting campaigns and major operations to identify those actions that can be observed by adversary intelligence systems	Of system administrators with full OPSEC training.	Percent	M3-2
			Of licensed system administrators.	Percent	M3-2

SN 3.4.7	Coordinate Force Protection for Strategic Forces and Means	To coordinate force protection for strategic forces and means to enhance freedom of strategic action by reducing friendly vulnerability to hostile acts, influence, or surprise.	Of personnel who receive level one antiterrorism/force protection (AT/FP) training prior to deployment or travel overseas.	Percent	M3-2
			Of personnel who receive annual security awareness training.	Percent	M3-2
			Of strategic forces able to execute mission operations in an nuclear, biological, and chemical (NBC) environment	Percent	M3-2
ST 6	Coordinate Theater Force Protection	To conserve the fighting potential of a joint force, including actions taken to counter the enemy taking strategic action against that force.	Of forces operate in areas under control of friendly ground forces (during execution).	Percent	M2-1
			Of forces operate under air superiority umbrella (during execution).	Percent	M2-1
			Of forces operate within maritime superiority area (during execution).	Percent	M2-1
			In-place theater-wide system for tracking status of US personnel vaccines, antidotes, chemical/biological protective training.	Yes/No	M2-1

Tasks and Measures on this sheet Support the "Test & Acquire Secure Information Systems" master Task					
UJTL Task #	Task Title	Task Description	Measure of Effectiveness	Unit of MOE	Consolidated Measure

SN 5.1	Operate and Manage Global Strategic Communications and Information Systems	To receive information and data on the strategic situation worldwide, including: combatant command, theater component command, and operational level command missions, disposition of friendly and enemy forces, strategic centers of gravity, and characteristics of the theater areas (worldwide).	To process and authenticate EAM for execution of preplanned options against fixed Single Integrated Operational Plan (SIOP) targets (ICBM/fleet ballistic missile submarine (SSBN)/Bomber crews).	Minutes	M3-1
			To process RECORD COPY emergency action message (EAM) for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			To process VOICE emergency action message (EAM) for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			To transmit EAM to bombers for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			To transmit EAM to intercontinental ballistic missile(s) (ICBMs) for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			To transmit EAM to SSBNs for execution of preplanned options (against fixed SIOP targets).	Minutes	M3-1
			Of addressees received messages.		M2-3, M2-4

SN 5.1.1.1	Provide Information Assurance Products and Services	To provide products, services, infrastructure, and capability to assure availability and appropriate application of evaluated/validated products and solutions.	To complete information assurance product evaluations.	Months	M3-1
			To develop a secure interoperable Communications Security (COMSEC) solution to be submitted for approval from the Committee for National Security Systems in support of a validated customer requirement.	Weeks	M3-3
			Of National Security Agency (NSA) information assurance solutions that have full lifecycle support plans as a percentage of total.	Percent	M3-3
			To respond to validated customer requirements.	Days	M3-3
			Of microelectronics stockpile inventories maintained.	Percent	M4-1
SN 5.1.2	Establish and Direct National Military Command, Control, Communications, and Computers (C4) Systems Worldwide for Communicating Strategic Information	To establish, direct, and control or interact with the networks and nodes (including space systems) used to send or receive strategic information (including data) and to use these systems to obtain or send strategic information.	Of articles on netted system available in heavy demand environment.	Percent	M4-1
			Of essential command and control (C2) nodes have redundant communication paths for minimum required communication capabilities to ensure timely receipt of all record traffic.	Percent	M4-1

			Of communications networks critical to operations fully operational.	Percent	M2-1
			Of communications outages equipped with adequate redundant communications paths to ensure timely receipt of record traffic.	Percent	M4-1
			Of DOD long-haul communications channels saturated.	Percent	M4-1
			Of information system interfaces require information scanning, retyping, reformatting, or other nondirect translation methods.	Percent	M4-2
			Of surge capacity available in DOD long-haul communications.	Percent	M4-1
			Each NC2 node can communicate by voice and record copy in a locally degraded environment.	Yes/No	M3-1
SN 5.1.2.1.1	Provide Global, Secure, Interoperable Communications and Networks for the Department of Defense	Provide global classified and unclassified voice, data, video, network, and transport backbone and access services through a combination of terrestrial and satellite assets.	Outages of any Defense Information System Network (DISN) global classified or unclassified voice, data, video, network, or transport backbone or access service that support a command and control network that isolates any combatant command headquarters.	Yes/No	M4-1

SN 5.1.2.1.2	Provide Global Information Grid Transport Backbone Networks for Data Communications	To provide the long-haul telecommunications infrastructure segment including the communication systems and services between the fixed environment and the deployed Joint Task Force (JTF) and/or Coalition Task Force (CTF) warfighter.	Of circuit or network availability.	Percent	M4-1
			Outages of the Defense Information System Network (DISN) that support a command and control network that isolate any combatant command headquarters.	Yes/No	M4-1
SN 5.5.3.1	Provide Network Management for the Theater Information Grid (TIG) Transport and Computer Network Infrastructures	Equip, train, maintain, and sustain the theater-level NetOps centers to enable them to manage and control the command, control, communications, computer systems, and networks, including space systems that define the TIG transport infrastructure within their AOR.	TNC has required facilities to conduct NETOPS S&NM tasks.	Yes/No	M3-1
SN 5.5.3.2	Protect and Defend the Theater Information Grid (TIG)	To collect and consolidate TIG intrusion detection reports and data, assessing the compiled data, and reporting the results to the appropriate command authorities.	Of TIG computer assets that are compliant or operating with approved extensions and mitigation plans with negligible risk on information systems capability to perform required theater missions	Percent	M2-1
OP 6.3.2	Supervise Communications Security (COMSEC)	To supervise the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the	Of multinational units operating from a common JCEOI.	Percent	M4-2

		possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study.			
			Of US joint force units operating from common JCEOI.	Percent	M4-2

Bibliography

- 8th Air Force Staff. (2007). *Draft cyber warfare air force operations concept*, United States Air Force.
- Brown, Hindley, Kozdras, Treat. (2007). *Joint capabilities document of cyberspace defense*, Air Force Institute of Technology.
- Chairman of the Joint Chiefs of Staff. (2005). *CJCSI 3170.01 joint capabilities and integration development system*, Department of Defense.
- Chairman of the Joint Chiefs of Staff. (2006). *National military strategy for cyberspace*, Department of Defense.
- Colombi, John M., LtCol. (2007). *Concept definition and analysis lecture notes*, Air Force Institute of Technology.
- Elder, Robert J., LtGen. (2007). *Effects-Based operations A command philosophy*. *Air & Space Power Journal*.
- Elder, Robert J., LtGen. (2007). *Warfighting in cyberspace briefing*, United States Air Force.
- Feuchter, Christopher A., (2000). *Air Force Analyst's Handbook: On Understanding the Nature of Analysis*, Office of Aerospace Studies, Air Force Materiel Command, United States Air Force.
- Jacques, David R., Dr. (2006). *Systems engineering design lecture notes*, Air Force Institute of Technology.
- Joint publication 1-02*(2007). Department of Defense.
- Office of the Secretary of Defense. (2005). *National defense strategy of the the united states of America*, Department of Defense.
- Office of the Secretary of Defense. (2006). *Quadrenial defense review 2006*, Department of Defense.
- Wynne, Michael W., Hon. (2007). *Flying and fighting in cyberspace*. *Air & Space Power Journal*.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY) 5 Jun 07		2. REPORT TYPE Graduate Research Paper		3. DATES COVERED (From - To) May 2006 - June 2007	
4. TITLE AND SUBTITLE The Way Ahead for Cyberspace Operations: A JCIDS Analysis				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Major Tim Treat				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765				8. PERFORMING ORGANIZATION REPORT NUMBER AFIT/IC4/ENG/07-08	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT As the mission of the military become increasingly interdependent on machine-to-machine operations and interoperability, the need for cyberspace superiority becomes more and more critical for our military to dominate in all domains. To achieve cyberspace superiority, our military services must field fully joint cyberspace capabilities that are designed and acquired to operate in a joint environment. Joint Capabilities Integration Development System (JCIDS) analysis can facilitate a broad focus and military leaders must understand and mandate its use to field truly joint capabilities in cyberspace.					
15. SUBJECT TERMS Cyberspace					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Robert Mills, PhD (ENG)
U	U	U	UU	180	19b. TELEPHONE NUMBER (include area code) (937) 255-6565; ext 4527; robert.mills@afit.edu

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