

11 March 2009

The Global Information Grid (GIG) 2.0
Concept of Operations
Version 1.1



THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY
DISCLOSURE UNDER THE FOIA. EXEMPTIONS APPLY.

Joint Staff J6

Washington, D.C. 20318-6000

THIS PAGE INTENTIONALLY BLANK

FOREWORD

From the Director, C4 Systems, Joint Staff



This Global Information Grid (GIG) 2.0 Concept of Operations (CONOPS) lays the groundwork to evolve our information technology (IT)/ National Security Systems (NSS) services into a single information environment with common standards and centralized governance providing the information advantage to our warfighting commanders. This will improve command and control and increase our speed of action in combat. Through this effort we will provide an IT/ NSS infrastructure that is accessible anywhere and anytime to ensure the agility of the Department and to allow our most valuable resources, our people, nearly instant access to the information they need to make decisions in the execution of their missions. In turn, GIG 2.0 must be designed and optimized to support warfighting functions of advantaged and disadvantaged users, to include mission partners, across the full range of military operations in any operational environment. Finally, GIG 2.0 is expected to streamline GIG architectures by reducing GIG variation and complexity; reduce downtime by delivering processes that are as mistake-proof in execution as possible; ensure effectiveness by improving the ability to share information in support of the mission; promote efficiencies by ensuring that the GIG consumes fewer resources than the status quo and deliver operational flexibility by delivering processes that can deliver mission success despite rapid change.

Nancy E. Brown
Vice Admiral, USN
Director for Command, Control,
Communications and Computer
Systems

Table of Contents

1	Executive Summary	1
2	Overview of GIG 2.0.....	4
2.1	Purpose	4
2.2	Evolution of Net-Centricity.....	4
2.3	Goals and Direction	5
2.4	Background.....	5
2.5	Methods	6
2.6	Scope.....	6
2.7	GIG 2.0 Characteristics	7
2.8	GIG 2.0 in support of the JCAs	13
3	GIG 2.0 Use Case Descriptions	16
3.1	Overview.....	16
3.2	Overall Scenario.....	16
3.3	Perspectives.....	17
4	GIG 2.0 Hierarchy and Structure	29
4.1	Overview.....	29
4.2	GIG 2.0 Command Relationships	Error! Bookmark not defined.
4.3	Roles and Responsibilities	Error! Bookmark not defined.
5	Summary	31
	References	32
	Glossary	34
	Acronym List.....	37

Table of Figures

Figure 1: GIG 2.0 Operational View (OV-1)	2
Figure 2: GIG 2.0 Characteristics, Goals, and JCA Relationship	8
Figure 3: Global Authentication, Access Control and Directory Services	9
Figure 4: Information and Services from the Edge	10
Figure 5: Joint Infrastructure	11
Figure 6: Common Policies and Standards	12
Figure 7: Unity of Command	13
Figure 8: GIG 2.0 and Joint Capability Areas	14
Figure 9: JCA and GIG 2.0 Vignette Perspectives	28
Figure 10: Global NetOps C2 (USSTRATCOM is Supported Command)	Error! Bookmark not defined.
Figure 11: Theater NetOps C2 (GCC is Supported Command)	Error! Bookmark not defined.

RECORD OF CHANGES

This is a "living document" and as such it will be updated as changes are suggested for incorporation. The Joint Staff J6 will accept, adjudicate, and make those changes once approved.

Change No.	Date of Change	Date Entered	Name of Person Entering Change

1 Executive Summary

Achieving and maintaining the information advantage as a critical element of national power requires the concentrated effort of the entire Department of Defense (DoD) to provide a seamless information environment optimized for the warfighter.

Operational experiences in Iraq and Afghanistan support the continued need to eliminate barriers to information sharing that currently exist on DoD's multiple networks. A concerted effort to unify the networks into a single information environment providing timely information to commanders will improve command and control, thus increasing our speed of action. Providing an information technology (IT) / National Security Systems (NSS) infrastructure that is accessible anywhere and anytime is key to ensuring the agility of the Department and allowing our most valuable resources, our people, nearly instant access to the information they need to make decisions in the execution of their missions. In turn, the Global Information Grid (GIG) must be designed and optimized to support warfighting functions of advantaged and disadvantaged users, to include mission partners, across the full range of military and National Security operations in any operational environment. The GIG must also be resilient and able to support the missions despite attacks by sophisticated adversaries.

The operational concept of GIG 2.0 is depicted in Figure 1, and builds upon net-centric concepts as articulated in DoD Information Enterprise Architecture (DIEA) Version 1.0 (April 2008).

Furthermore, GIG 2.0 is founded upon the following 5 characteristics which are further discussed in section 2.7:

- Global Authentication, Access Control, and Directory Services
- Information and Services "From the Edge"
- Joint Infrastructure
- Common Policies and Standards
- Unity of Command.

GIG 2.0 will facilitate mission accomplishment by providing tactical services "from the edge" in support of the warfighter. The warfighter tactical edge user solutions must work in austere deployed environments. Today many IT services and systems are designed to work in a robust IT environment and often do not scale down to the deployed user. This separation between home station and deployed capabilities requires the user to transition from garrison IT services to tactical IT services, often losing functionality in the deployed environment. This document presents the GIG 2.0 Concept of Operations (CONOPS) as it relates to five key critical characteristics of the GIG and their relationship to the DoD Joint Capability Areas (JCA).

The operational capabilities identified in this document will be further developed in the GIG 2.0 Initial Capability Document (ICD). The resulting requirements will drive implementation of

DoD-wide infrastructure capabilities managed as part of the Net-Centric Capability Portfolio and other capability portfolios as required. GIG 2.0 challenges the Department to deliver results that are timely, relevant, and focused on the needs of the warfighter while providing tools (e.g., operational outcomes, validated requirements, and architectures) to ensure stakeholder communities move toward a common and unified end state. Together, we must do what is necessary to ensure our information advantage and give our people the tools they need to accomplish their mission. GIG 2.0 transforms the current GIG of stove-piped systems, processes, governance, and control to a unified net-centric environment. This allows GIG 2.0 to support all DoD missions and functions in war and peace, along with supporting DoD's involvement with interagency, coalition, state, local, and non-governmental organizations (NGOs). GIG 2.0 integrates all DoD IT/NSS resources together to support the United States national interests and national strategies.

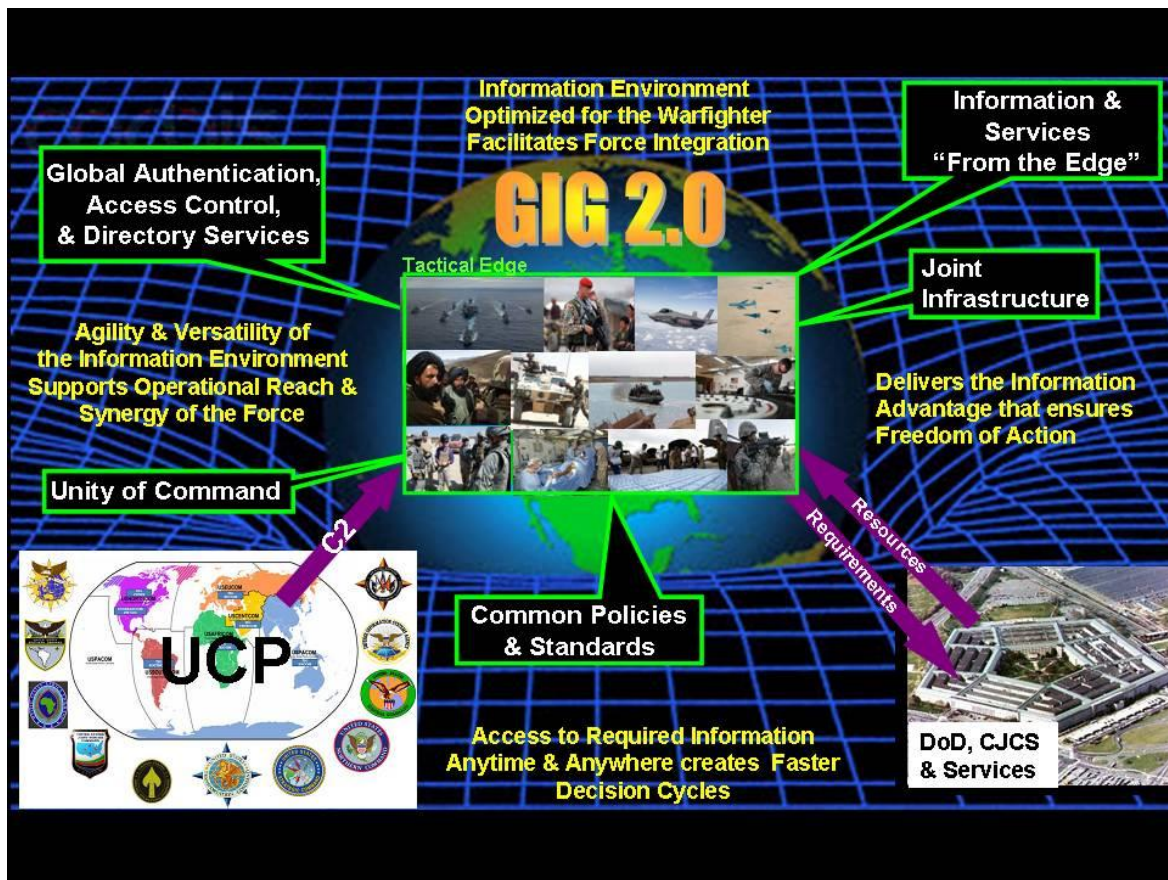


Figure 1: GIG 2.0 Operational View (OV-1)

The GIG 2.0 CONOPS supports the implementation of DoD strategies such as the National Military Strategy, National Military Strategy for Cyberspace Operations, National Military Strategic Plan for the War on Terrorism, and the Unified Command Plan (UCP). These plans

require joint, common, integrated IT/NSS infrastructures that enhance operational capabilities. The visionary concepts outlined in this CONOPS are centered on Joint operations. This GIG 2.0 CONOPS recognizes all aspects of Joint IT as the coherent “Enterprise” that exists ultimately to support the Combatant Commanders (CCDR) in their Joint Warfighting missions. This GIG 2.0 concept does not contradict the Military Service and Agency Title 10 authority to man, train, and equip the force. The GIG 2.0 concept promotes unified, common standards and policies to enhance effectiveness across the DoD. Lastly, GIG 2.0 will become an enabler by effectively linking our forces from the forward edge of the battlefield through the Combatant Commands and back to home stations.

2 Overview of GIG 2.0

“The entry fee (for Net Centric Warfare) is a high performance information grid . . . the information grid enables the operational architectures of sensor grids and engagement grids.”
VADM A.K. Cebrowski

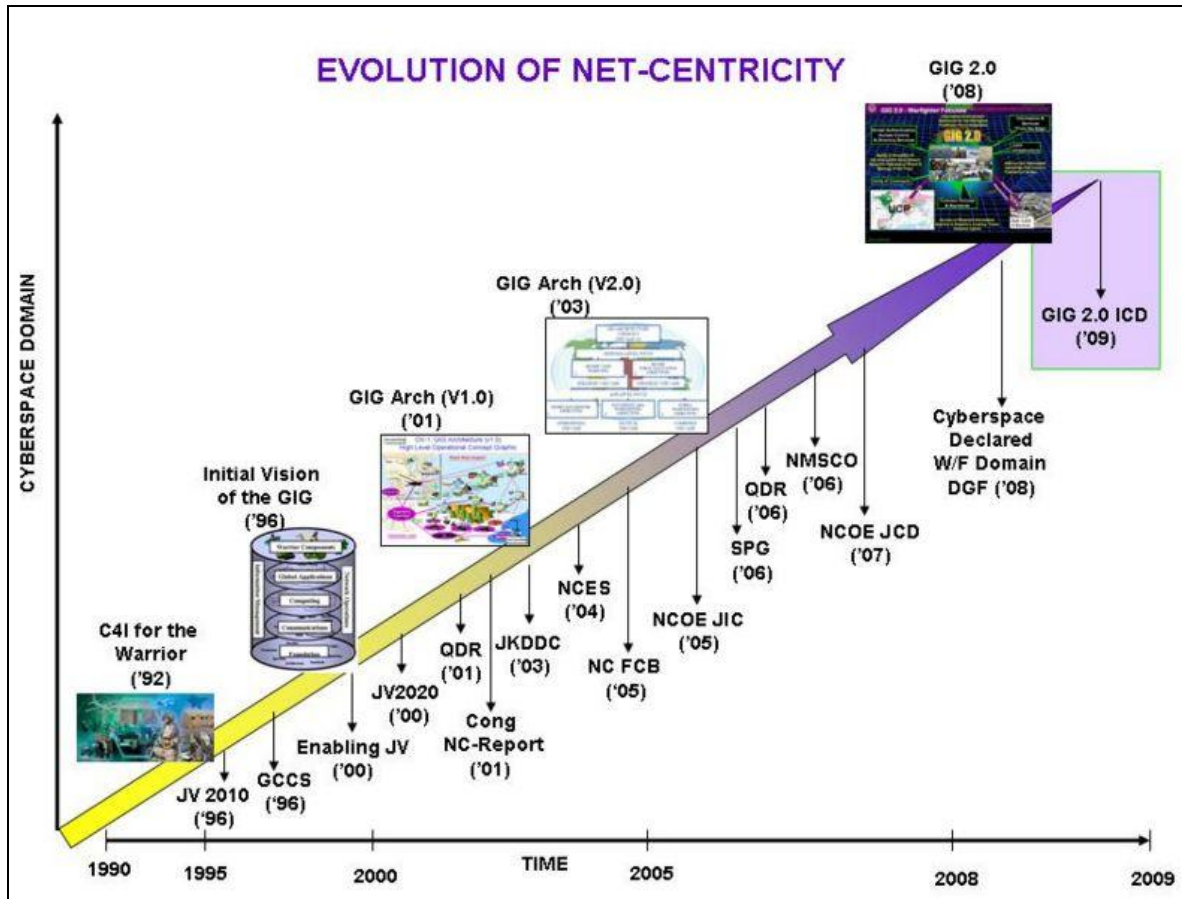
2.1 Purpose

This document was sponsored by the Joint Staff to establish a CONOPS for achieving a next generation GIG referred to as GIG 2.0. Specifically, the purpose of this document is to:

- Present a vision that serves as a baseline for the GIG 2.0 capabilities and to combine operational concepts with governance components and on-going acquisition strategies
- Identify key components of this GIG 2.0 vision
- Expand upon those key GIG 2.0 characteristics to identify deficiencies and identify known impediments to implementation, and provide an approach to develop solutions.

2.2 Evolution of Net-Centricity.

The evolution of net-centricity can be traced by its roots back to DoD network centric warfare (NCW) initiatives of the 1990s, through the Chairman of the Joint Chiefs of Staff Joint Vision emphasis on developing information superiority and translating it to increased combat power across the spectrum of operations. GIG 2.0 further advances net centricity into the cyberspace domain, providing increased agility, and operational effects and capabilities for the warfighter at the tactical edge.



2.3 Goals and Direction

The overarching goals of the GIG 2.0 vision are taken from the Joint Net-Centric Operations (JNO) Strategy and the Net-Centric Operational Environment (NCOE) Joint Capabilities Document (JCD). The overarching GIG 2.0 goals are to: accelerate availability of trusted information to achieve decision superiority; transform to a single information environment; and drive policy, resources, and cultural changes to achieve net-centric operations.

GIG 2.0 transforms the GIG into a single information environment with standardized interfaces across all DoD components. GIG 2.0 will reduce our vulnerabilities through standardized, controlled access to the information environment. Assured system and network availability, assured information protection, and assured information delivery are central to providing the IT/NSS services required to implement GIG 2.0. The GIG 2.0 concept focuses on providing access to resources and services in accordance with the user's mission.

As stated in Department of Defense Instruction (DoDI) 8410.0 and the Unified Command Plan 2008, Commander, U.S. Strategic Command, CDRUSSTRATCOM's specific responsibilities are to direct GIG operations and defense. CDRUSSTRATCOM fulfills these responsibilities with the assigned forces listed in SECDEF Memorandum, "FY 08-09 Global Force Management Implementation Guidance (S)," 4 June 2008. CDRUSSTRATCOM is tasked to develop and

implement a command and control structure to execute NetOps operational priorities in coordination with other Combatant Commanders and other DoD Components.

2.4 Background

The capabilities describing GIG 2.0 were developed through inputs received from multiple Combatant Commands (COCOMs) as a result of lessons learned during exercises and operations. These Joint Force Commanders found themselves caught in the seams of Military Service-centric networks and systems that did not enable the free flow of information amongst their forces. Their frustration over the lack of integrated capabilities that are optimized for the warfighter led to the development of the GIG 2.0 concept to address technical and governance issues. The GIG 2.0 concept is one that leverages service oriented architectures to provide a unified information environment that eliminates duplicative network efforts. The GIG 2.0 concept was viewed as an enabler to creating true joint bases with integrated IT/NSS systems and services.

In regard to joint basing, an Information Technology Service Management (ITSM) Sub-Working Group (SWG) composed of OSD, Joint Staff, and the Military Services was formed to accomplish specific tasks identified in the Joint Basing Implementation Guidance (JBIG). The first version of the ITSM Supplemental Guidance has detailed implementation guidance for IT/NSS services on the joint bases in addition to defining performance standards for each IT/NSS service. The ITSM Supplemental Guidance and associated performance standards have been approved by the Deputy Secretary of Defense. The lack of joint/common IT/NSS services on the joint bases must be addressed holistically and across the entire DoD. The Joint Staff will use current operational lessons learned as an opportunity to address IT/NSS shortfalls such as stove-piped data services or bandwidth challenged tactical edge users. Today the development, acquisition, management, and sustainment of our networks are fragmented. This fragmentation consistently results in interoperability problems, and lack of operational flexibility. This drives excessive cost and justifies the need for the GIG 2.0.

2.5 Methods

As with any significant change to an existing globally deployed architecture, the transition from the current DoD IT/NSS environment to a GIG 2.0 will be challenging. Implementation of GIG 2.0 will be a transformational process that seeks incremental improvement over time. There will be a period when some of the GIG 2.0 capabilities will be implemented and others will require development. GIG 2.0 will be embedded into our global command and control (C2) structures through the ongoing integration efforts from the United States Strategic Command (USSTRATCOM), the Military Services, and Agencies to include the Defense Information Systems Agency (DISA) and the National Security Agency (NSA). This transition will evolve over time to ensure maximum results while minimizing the impact to ongoing missions, and will bring the IT/NSS services and connectivity fully in-line with the joint warfighting activities.

2.6 Scope

This CONOPS proposes a management concept and addresses the roles, functions, and relationships of key organizations. The CONOPS presents requirements for the initial

implementation of GIG 2.0. It will define the type of information (not the format) that is to be exchanged between organizations.

GIG 2.0 is envisioned to fulfill the global requirements of the C/S/A communities and serves as a platform to implement the ASD (NII)/DoD CIO Department of Defense Information Enterprise (DoD IE). As such, GIG 2.0 and the DoD IE will establish effective implementation and policies to assure that the DoD, our interagency partners, and other mission partners (federal, allied & coalition) have the integrated global IT connectivity to fulfill their mission requirements.

GIG 2.0 provides capabilities to all operating locations (bases, posts, camps, stations, facilities, mobile platforms and deployed sites), in addition to providing interfaces to mission partners, and non-DoD users and systems. GIG 2.0 will facilitate mission support emanating from joint bases in support of the warfighter.

2.7 GIG 2.0 Characteristics

The relationships between the GIG 2.0 goals, characteristics, and the JCAs are depicted in Figure 2 below. The nine Tier 1 JCAs (shown in the purple ring) represent the joint enabling mechanism for achieving the GIG 2.0 end state. These are discussed in Section 2.8 below. Furthermore, the JCA construct provides an organizing structure for managing the investments and programs of record that will enable the GIG 2.0 vision. The GIG 2.0 characteristics are discussed in the following sub-paragraphs, along with a graphical view of the current state, and the envisioned end state of each characteristic.

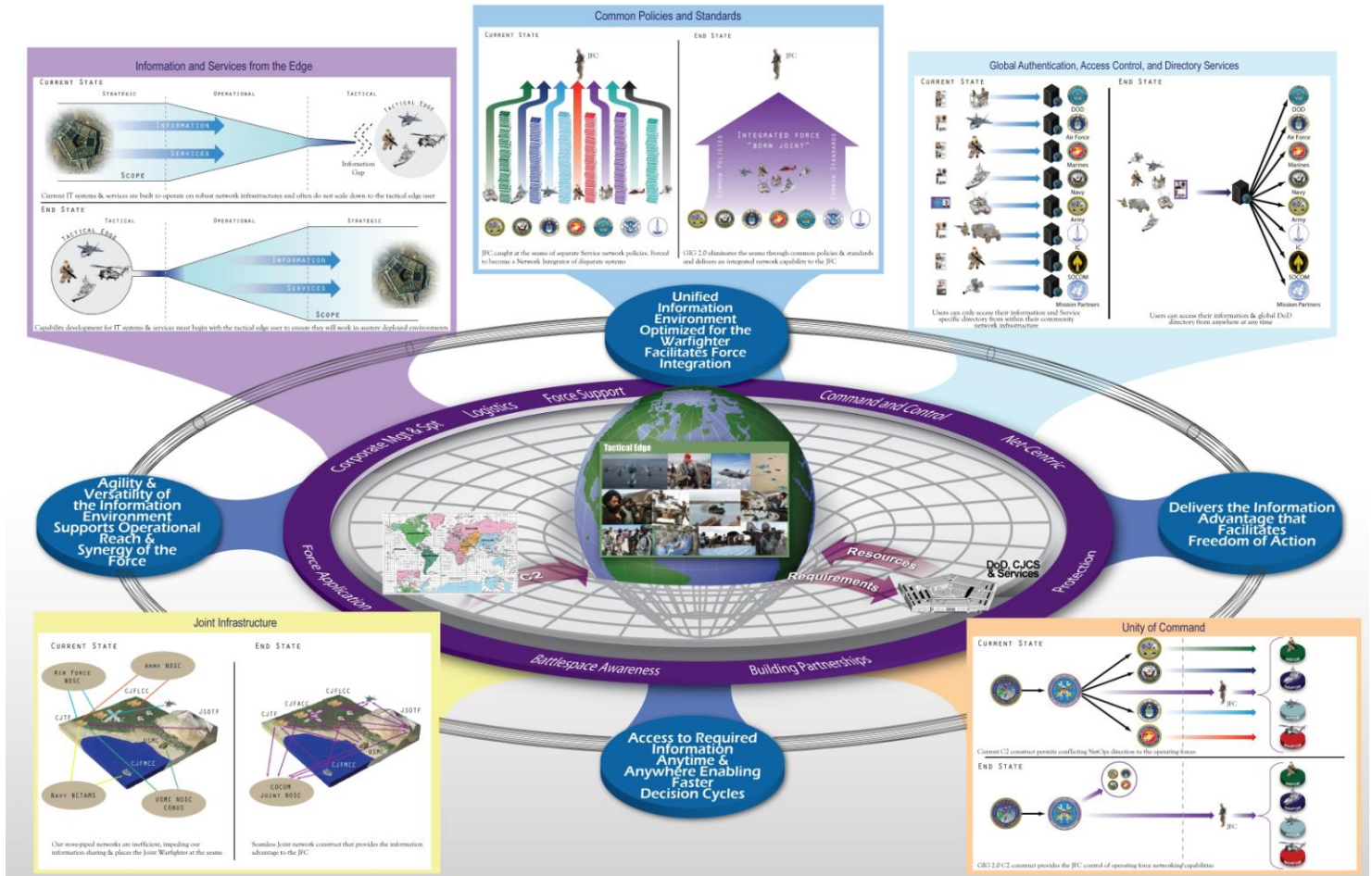


Figure 2: GIG 2.0 Characteristics, Goals, and JCA Relationship

2.7.1 Global Authentication, Access Control and Directory Services

This characteristic ensures any authorized user can access the global network infrastructure from any location with common and portable identity credentials which enable visibility of, and access to, all warfighting, business support, or intelligence related information, services and applications related to the mission and community of interest (COI). This characteristic includes single sign-on and anytime/anywhere access to the network, IT/NSS services, and the entire DoD Global Address List.

GLOBAL AUTHENTICATION, ACCESS CONTROL, AND DIRECTORY SERVICES

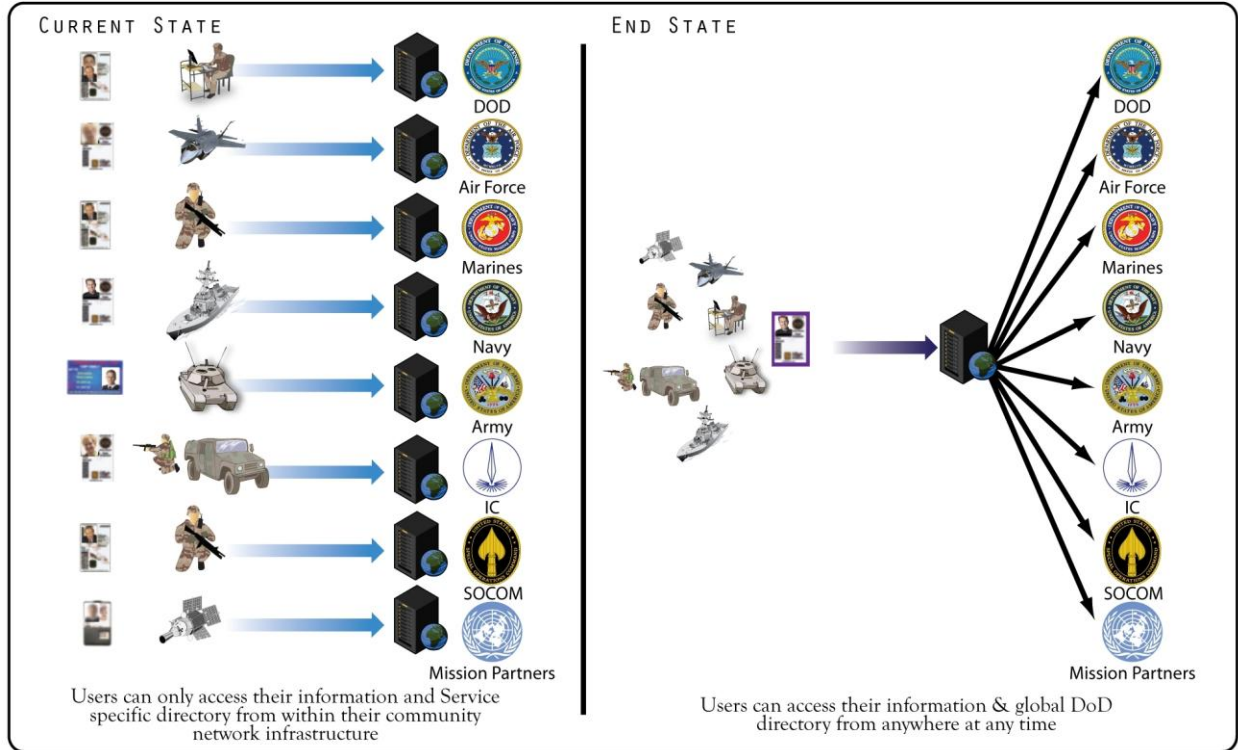


Figure 3: Global Authentication, Access Control and Directory Services

2.7.2 Information and Services “From the Edge”

The warfighter is provided timely assured access to required data and services at the edge of the battlespace to fully leverage the information advantage in direct support of the mission. The warfighter network must be designed and optimized to support warfighting functions of advantaged (robust environment) and disadvantaged (austere environment) users, to include mission partners, across the full spectrum of military and National Security operations in any operational environment while supporting DoD/Military Service-unique processes. This includes a resilient warfighter network capable of providing information and services despite attacks from sophisticated adversaries. As depicted in Figure 4, services supporting information flows at the tactical edge up to headquarters must be developed to support the tactical edge first. In the past, services were geared for headquarters where bandwidth was not a problem; however, when these same services were applied to the tactical edge, their performance was often inconsistent, at best, given bandwidth constraints. If services are built to support the tactical edge, all users up to the strategic level will be able to use them and promote unity of command.

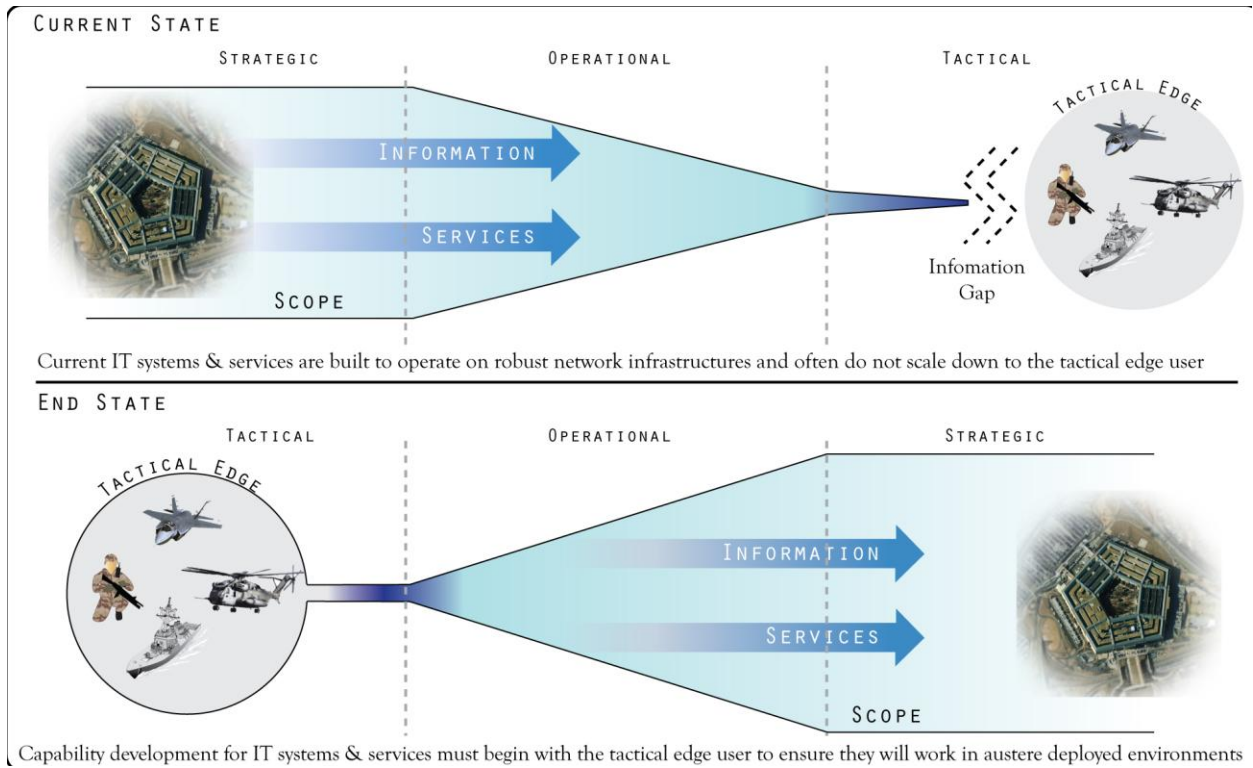


Figure 4: Information and Services from the Edge

2.7.3 Joint Infrastructure

This single information environment interconnects GIG 2.0 users securely, reliably, and seamlessly. The infrastructure enables shared information services to joint warfighters and mission partners, business support personnel, intelligence personnel, and systems from the tactical edge to any global location. This includes present and future military and commercial communications capabilities such as the aerial layer relay and gateway capabilities to expand communications coverage, communications network distribution services (routing, switching), data center facilities, and transmission systems.

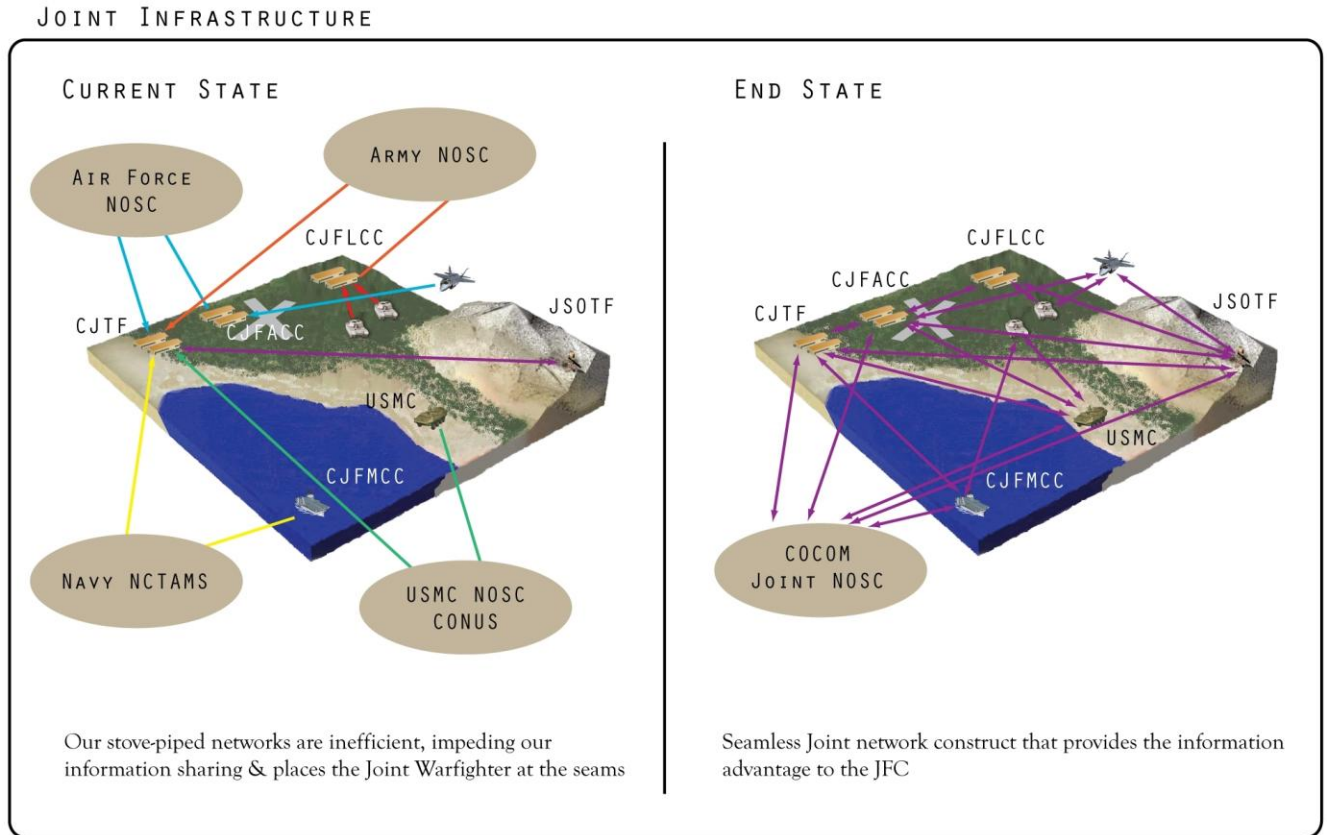


Figure 5: Joint Infrastructure

2.7.4 Common Policies and Standards

GIG 2.0 will be built upon common policies and standards that ensure all DoD networks and IT systems are integrated to provide seamless end-to-end information services. These common methodology and standards will ensure systems are developed, tested, certified and deployed with end-to-end enterprise interoperability and resilient against attacks. This concept does not imply a one size fits all approach to IT systems but rather one set of technical interface standards to ensure seamless interoperability of IT/NSS systems across the force. This effort will provide effective enterprise direction for data standards, information service standards, acquisition, certification, and enforcement to ensure the seamless flow of information between all DoD and mission partner users and systems. The GIG 2.0 components include: user access and display devices and sensors; networking and processing; applications and services; and related transport and management services will be governed by common policies and standards.

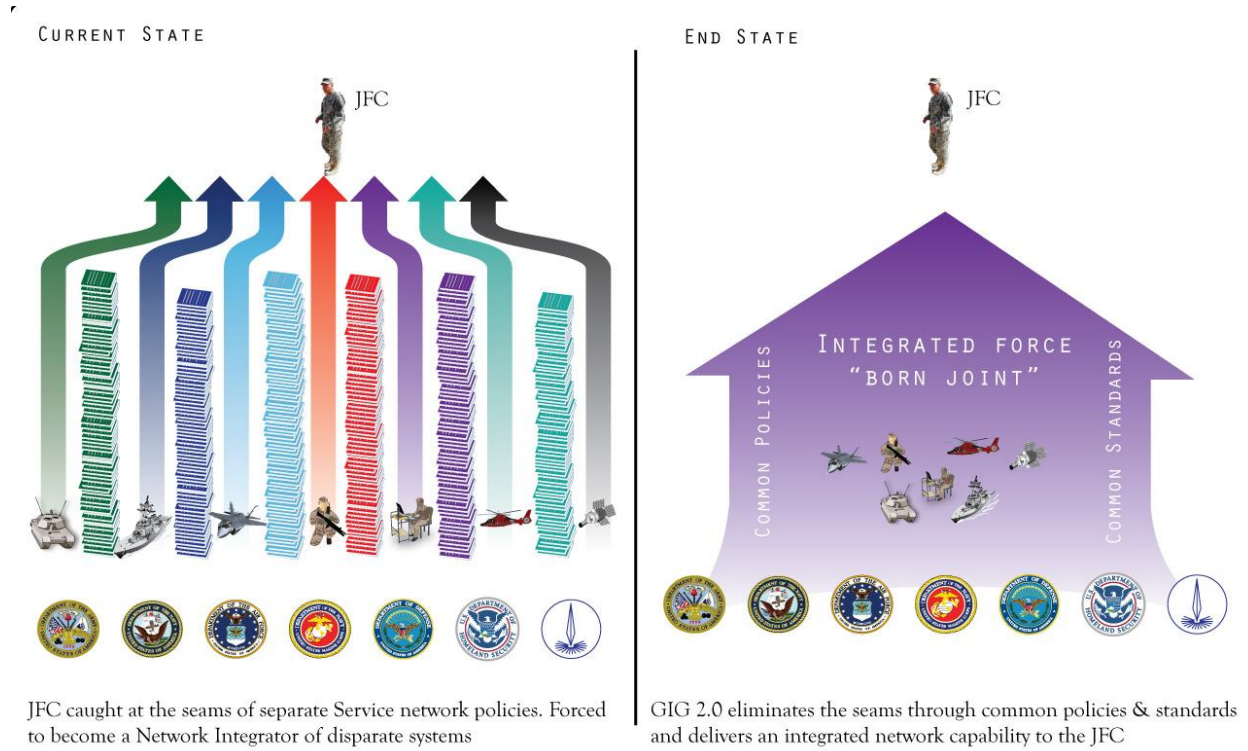


Figure 6: Common Polices and Standards

2.7.5 Unity of Command

According to Joint Publication 1, Doctrine for the Armed Forces of the United States, “Unity of command means all forces operate under a single CDR with the requisite authority to direct all forces employed in pursuit of a common purpose. Unity of effort, however, requires coordination and cooperation among all forces toward a commonly recognized objective, although they are not necessarily part of the same.” The GIG 2.0 characteristics of “unity of command” will be defined by USSTRATCOM and will include the command structure, supported/supporting relationships, and coordination requirements.

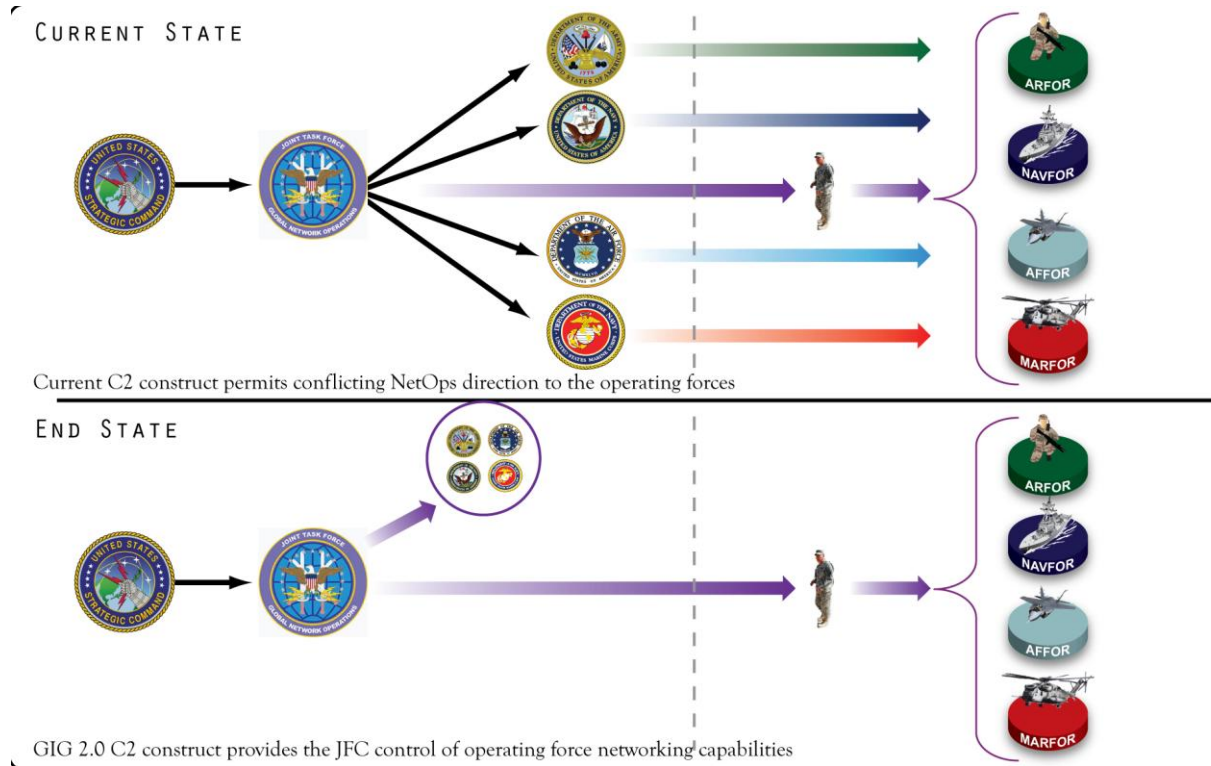


Figure 7: Unity of Command

2.8 GIG 2.0 in support of the JCAs

The changes realized through GIG 2.0 will have effects across all of the JCAs. The effects of GIG 2.0 are expressed as operational outcomes in relation to each JCA. The following descriptions of each GIG 2.0 characteristic are accompanied by at least one association with a JCA.

GIG 2.0 and The Joint Capability Areas (JCAs)

- **The GIG 2.0 will enable our forces, agencies and other mission partners across the full spectrum of military operations to gain the information advantage over our adversaries.**
 - Outcomes such as force integration, freedom of action, shortened decision cycles, operational reach and synergy of the force are but a few of those outcomes.
- **A new unified DoD Global Information Grid will provide relevant and ready military power to Joint Commanders**
 - Operational Missions with Joint and Mission Partner Forces demand continuous reliable GIG access
- **The JCAs provide the focus of effort for the GIG 2.0**
 - Force Application.....Increased effectiveness of Kinetic and Non-Kinetic Operations
 - Command and Control.....Faster decision cycles
 - Battlespace Awareness.....Synchronization and integration of intelligence
 - Net-Centric.....Leverage networks to act with confidence
 - Building Partnerships.....Shape and Strengthen our Global Defense Posture
 - Protection.....Improved Force and network protection
 - Logistics.....Provide Freedom of Action
 - Corp. Mgmt and Support.....Provide Standards and Oversight of resources
 - Force Support.....Enhance, Adapt and Sustain the force




Figure 8: GIG 2.0 and Joint Capability Areas

2.8.1 GIG 2.0 in support of Force Application (FA)

GIG 2.0 will optimize warfighting information services thus improving our abilities across the full range of military operations. This optimization will increase the effectiveness in both kinetic and non-kinetic means of engagement. GIG 2.0 will improve battlefield coordination and the effectiveness of the force by providing anytime/anywhere access to required information, and enable improved coordination of battlefield maneuver to generate the desired lethality in the engagement of enemy forces during kinetic operations and improved coordination of non-kinetic operations.

2.8.2 GIG 2.0 in support of Command & Control (C2)

From the GIG 2.0 environment we see an increase in the speed and effectiveness of information exchange across the force therefore speeding up our decision making cycles. Time sensitive information and decisions will travel securely and accurately, based on common policies and standards under a unified command to facilitate successful mission accomplishment. GIG 2.0 will also contribute to the Defense and National Leadership Command, Control, and Coordination capabilities.

2.8.3 GIG 2.0 in support of BattleSpace Awareness (BA)

The GIG 2.0 construct improves BA by enhancing Intelligence, Surveillance, and Reconnaissance (ISR) collection, analysis and processing/exploitation from sensor to shooter in support of the joint force. ISR products will be easier to disseminate in the GIG 2.0 environment rather than the segmented environment which we operate in today. This effort will enhance overall BA and affect decision making.

2.8.4 GIG 2.0 in support of Net-Centric (NC)

GIG 2.0 will give commanders confidence in their IT/NSS capabilities and enable them to act with confidence on the information they receive. This approach is a step forward in embracing the Net-Centric approach to warfighting and supports the required exchange of information.

2.8.5 GIG 2.0 in support of Building Partnerships (BP)

The GIG 2.0 vision includes a single information environment that will enable mission partnership solutions for access to information and services through common standards, policies, and procedures. We must focus on providing the warfighter with the ability to better enable mission partners to fully participate as members of the total force. This coordination will strengthen our relationships and improve our global defense posture.

2.8.6 GIG 2.0 in support of Protection (P)

The speed of information and shortened decision making cycles enabled through GIG 2.0 will give the Joint Force Commander the ability to react to emerging threats thus providing for improved protection of the force.

2.8.7 GIG 2.0 in support of Logistics (L)

The improved BA and C2 of the force through GIG 2.0 will enable logistics units to better support the joint force. This improved sharing of logistics information will improve freedom of action and timely sustainment of the force.

2.8.8 GIG 2.0 in support of Corporate Management & Support (CMS)

The foundation of GIG 2.0 will be the common set of standards that will mandate required changes to move into an open information environment. Providing these standards is the first step on the road to seamless information sharing.

2.8.9 GIG 2.0 in support of Force Support (FS)

GIG 2.0 will be built on common policies and standards that will simplify our training and create a more agile force. The networks will better support the total force and drive the evolution of information exchange requirements and methods. Through this effort we will have a better prepared force to support information requirements across the full range of military operations around the globe.

3 GIG 2.0 Use Case Descriptions

“Network-centric capabilities allow the force to attain an improved information position that can partially “lift the fog of war” and enable commanders to improve their decision making and fight in ways that were not previously possible.” - Network Centric Warfare, Department of Defense, Report to Congress, 27 July 2001

3.1 Overview

To further illustrate the positive effects of GIG 2.0, a scenario is used to convey potential changes and impacts to the Department. Defense Planning Scenario - Major Combat Operation One (Swiftly Defeat) [10] was chosen from the draft C2 JCD to illustrate the current problems and potential benefits of GIG 2.0. The following section sets up the overall situation followed by a look from various perspectives within DoD at the current problem and potential change with the advent of GIG 2.0.

3.2 Overall Scenario

A well-equipped hostile nation-state seized control of a neighboring country’s key terrain, controlling access to international sea lanes. The adversary country and the seized country are made up of rural and urban settings. The GCC directs that a combined joint task force (CJTF), built around a Continental United States (CONUS)-based Army Corps Headquarters (HQ), reestablish the seized friendly country. The Army Corps Commander will serve as the Commander CJTF (CCJTF), along with other assigned joint forces to constitute ground, air, maritime, and special operation components. Some friendly neighboring nations will participate in the operation as mission partners, but will not place their forces under CJTF command. Threats to friendly forces consist of air, ground, ballistic missile, and surface-to-air missile (SAM) threats and various cyber threats. Component commanders maintain the ability to access GIG 2.0 and thus collaborate with each other and participate in the planning process while en route to their deployed HQ. As the CCDR shifts to direct action, the staff will enter a planning phase comprised of crisis action and adaptive campaign planning. Throughout planning and execution, the GIG 2.0 links the GCC staff, CJTF, geographically separated staffs, the Interagency Community, and Centers of Excellence for information, planning, operations, administration, and logistics support. GIG 2.0, including a knowledge portal and other tools, becomes the primary venue for accessing and sharing information throughout the operation. GIG 2.0 enables planning and C2 from distributed sites, reducing the time required for coordination and information sharing. It also enables all involved in crisis resolution to share 24/7 access to the same situational information, orders, briefings and data as members of a COI.

Upon receipt of the task, the CCJTF establishes a COI for CJTF information sharing and collaboration on GIG 2.0 and obtains appropriate access for multinational partners and international agencies that participate in the operation.

In consultation with the CCDR and multinational leads, CCJTF establishes a hybrid command structure consisting of combined and joint component commanders for maritime, air and space, land, logistics and special operations, plus multifunctional mission components. Teams are tailored within the CJTF staff and across the force to address emerging problems or new missions. Mission partners include supporting commands, USSTRATCOM, United States Special Operations Command (USSOCOM), United States Transportation Command (USTRANSCOM), DISA, Defense Intelligence Agency (DIA), national intelligence agencies, and non-DoD agencies (Department of State (DOS), non-governmental organizations (NGO), inter-governmental organizations (IGO), etc.). These mission partners create a COI to share information per the mission requirements and security risks associated with each mission partner. All information is tagged such that it is immediately available to those COI authorized to use the information.

Although the CCJTF has selected a course of action (COA), the Commander and his staff refine and adjust the plan based on the changing situation while en route to the theater. Using the en route configuration established aboard a C-17 Globemaster, the commander and battle staff continue monitoring the situation and adjusting the plan as necessary. The battle staff coordinates with garrison staffs, GCC HQs, and subordinate Functional Component Commands utilizing GIG 2.0. The staff also uses tactical satellites to coordinate with Special Operations Force (SOF) elements and the advance party already on the ground. The commander and his staff use tailorable, user-friendly information displays to assimilate battlespace information, and increase situational awareness. The CCJTF and staff move to an amphibious warship, augmented with Joint C2 applications. The amphibious warfare ship is able to support medium-sized CJTF HQs, utilizing reach-back and collaboration capabilities. The same information and services used while airborne on the C-17 are available via authentication with terminals located on the amphibious warship. The GIG 2.0 capabilities enable the staff and Functional Component Commanders to participate in the planning process with minimal downtime or administrative change requirements when moving from C-17 airborne based resources to the shipboard services. It also allows the CCJTF staff to coordinate with the GCC, multinationals, U.S. agencies, and NGOs to obtain and report the most current information from available sources and provide real-time situational awareness. This real-time situational awareness enables the commander and staff to quickly and collaboratively make timely adjustments to the operation. CCJTF directs action through mission-type orders to Functional Component Commanders. Component Commanders and their subordinate units keep each other and the CCJTF apprised of their progress via GIG 2.0.

3.3 Perspectives

The following subsections describe an aspect of the main scenario from different perspectives or viewpoints. To have a balanced look at GIG 2.0, three views from DoD Components (a GCC, a Military Service, and an Agency) and one from an outside view (a mission partner) are provided. Associations are then made to the JCA and operational impacts within each area are also expressed. Each of the views lists a problem and vignette describing the potential solution along with an analysis of the GIG 2.0 attributes from each perspective.

3.3.1 Combatant Commander

3.3.1.1 Problem Statement

The current GIG environment does not allow the CCDR the means to seamlessly execute C2 and enable operations without “work-arounds,” “sneaker-nets,” and manual processes. The result of this inability drives the CCDR into the role of systems integrator for core functions of C2, distracting the Command from the imperatives of conducting their operations. An additional and unfortunate implication of this situation is the fact that each GCC solution may be implemented differently. This lack of a unified approach leads to different technical solutions across what should be a unified and integrated information battlespace. GIG 2.0 is focused on building networks to enable operations rather than recreating data, services, and networks to support operations.

3.3.1.2 Vignette

The CCDR bears the responsibility of conducting the warfighting operations to meet national security needs. Today, the COCOMs expend considerable resources accomplishing what should be a seamless, automated process of incorporating arriving forces and elements into the theater’s networks and services. GIG 2.0 resolves these issues by ensuring the smooth transition of data and services regardless of geographic locations. The COCOM must seamlessly integrate the efforts of organizations that have enduring relationships with their component commands, dispersed CONUS-based organizations, and globally oriented resources and supporting functional commands (such as USSOCOM and USTRANSCOM). Operations will likely include other mission partners and allies, along with interagency representatives from other federal cabinet agencies such as the DOS, the Department of Justice (DOJ), and representatives from the Director of National Intelligence (DNI). Each of these organizations is postured to help the COCOM meet operational needs and succeed in the national mission, but require extensive coordination and integration to support the operation.

In the scenario, CJTF must nest the operations and functions with forces they are familiar with (those units organic to the Army Corps assigned to the Joint Task Force) while also establishing C2 with other units (such as the component commands and the COCOM headquarters). The need to plan a forcible-entry operation into enemy held territory while simultaneously moving headquarters and forces into the theater increases the complexity of the planning and emphasizes the need for a unified and integrated C2 environment. This scenario reinforces the fact that joint forces must be capable of immediate C2 from land, sea, or air. In our scenario the JTF postures for operations from all of these environments.

The result of GIG 2.0 melds all warfighting needs in an information environment that allows the COCOM to exercise C2 during all the phases of operation. Prior to the onset of deliberate combat operations, GIG 2.0 enables the COCOM to quickly establish the CJTF and facilitate the flow of combat power toward the theater. GIG 2.0 enables the transition into direct combat and the transition (in tandem with our mission partners and interagency elements) to post-combat reconstruction and stability operations. Each of these phases requires different approaches and resources, but the need for unhindered C2 predominates throughout. At each phase, GIG 2.0

facilitates the COCOM's ability to execute the mission through the use of the CJTF, mission partners, and interagency representatives. The functions that GIG 2.0 provides the COCOM and CJTF will enable all of the JCAs.

3.3.1.3 Operational Impacts

The GIG 2.0 results in the better integration of C2. The COCOM and associated forces are able to quickly build, integrate, deploy, fight, sustain, and transition during combat operations. The seams between our CONUS-based forces and the OCONUS scenario are eliminated and increased speed and flexibility in reacting to the external threats will be realized by the joint force.

Force Application: GIG 2.0 enables the COCOM's ability to execute operations in the full range of Force Application (Engagement and Maneuver). The GIG 2.0 environment enables engagement by supporting and integrating our battle-command systems and providing the platform for execution of many non-kinetic measures. GIG 2.0 also enables the execution of all portions of maneuver, from air, land, and sea and during all phases of the conflict.

Command and Control: GIG 2.0 is probably most useful to the COCOM and the fighting forces assigned to CJTF as an integrated environment to support C2. The ability to organize, understand, plan, direct, and monitor are improved in GIG 2.0 via the joint infrastructure and common policies and standards. This environment allows Commanders to more effectively and rapidly join the separate fighting elements into a cohesive fighting force. This unified and integrated environment also supports the ability to rapidly reach out and include new mission partners as operational needs change.

Battlespace Awareness: Effective collection, sharing, analysis, and dissemination, through the use of ISR and understanding of the environment, requires the support of GIG 2.0. In GIG 2.0, the ISR capabilities and the use of information and intelligence gleaned by knowing the environment move rapidly up and down the CJTF command chains and laterally through the component and mission partner forces. This environment allows both the intelligence and operations staff to fuse capabilities in a revolutionary manner.

Net-Centric: The needs of the COCOM are inherently Net-Centric. The commands need assured information transport and the core enterprise services to support operations in all phases of conflict. GIG 2.0 provides an effective Net-Centric approach to successfully exercise C2 across vast terrain, airspace, and maritime environments. This C2 requirement also requires a unified Net Management approach that enables the COCOM to exercise their unity of command in the unified C2 environment.

Building Partnerships: GIG 2.0 assists the COCOM's ability to rapidly and flexibly communicate with new mission partners and shape their engagement as the operation progresses. The range of support that GIG 2.0 provides is useful to the CCJTF in helping to persuade mission partners to join the effort, enabling our security services to become more deeply involved in support of the operation.

Protection: GIG 2.0 supports the CJTF commander's need to prevent and mitigate threats from hostile capabilities (such as adversary theater missile systems). Additionally, the ability to move data laterally throughout the CJTF enables our forces to protect themselves from symmetric and asymmetric attacks.

Logistics: The combined strength of GIG 2.0 will enhance the joint logistics COI in their ability to deploy and distribute, supply the forces, maintain vital equipment (while improving the understanding of our current stocks and spares), and provide needed logistics services. Additionally, the GIG 2.0 environment will help our contract management personnel to support a mobile fighting force through the transfer of crucial information and services in a more effective manner.

3.3.2 Military Services

3.3.2.1 Problem Statement

The Military Services have a difficult time addressing the various IT service requirements placed on them from the CCJTF. A CCJTF is formed for a particular mission and each mission has different information requirements. The COCOMs do not all follow the same standards in developing requirements for warfighting support from the Military Services. This results in varying "flavors" of solutions to meet the COCOM requirements. The following two deploying unit situations have example problems encountered by a Military Service that will be addressed through the adherence to the GIG 2.0 vision. As with the Combatant Commands, the Military Services require the JCA that support our warfighting strategies, plus the needs to sustain the base force.

Electronic Warfare Squadron Deploying Worldwide

An EA-6B Prowler aircrew squadron deploys from an aircraft carrier (CVN) as it heads for the Area of Responsibility (AOR) of the GCC who commands the CCJTF. The carrier has a unique network configuration that requires creation of new e-mail addresses for all squadron personnel while deployed. The squadron must supply their own data storage devices and/or servers since none of their data is resident on the aircraft carrier. When they arrive in the AOR, a detachment of four EA-6B aircraft is flown to a Forward Operating Base (FOB) in theater. The FOB is run by another Service and has tenants from every DoD Service Component and agency as well as foreign mission partners. While waiting for their network services to be connected, the detachment Officer in Charge is forced to use the base Morale, Welfare, and Recreation (MWR) facility to stay in touch with his parent command aboard the CVN via commercial e-mail accounts. At the FOB, new e-mail addresses and accounts are created for the detachment personnel to access SIPRNET and NIPRNET resources while detached to that base. Their data storage must be brought with them to FOB. Joint Worldwide Intelligence Communications System (JWICS) access and security clearances must be verified in the Joint Personnel Adjudication System (JPAS) before new AOR-specific JWICS accounts can be created at the FOB. JWICS data left on the CVN servers is not available to the aircrew at the FOB. Aircrews must transport and set up specific workstations particular to the EA-6B for mission preparation. These systems require classified network connections and are difficult and time consuming to

establish. When the aircrew and planes return to the CVN, they must revert back to their original deployed e-mail accounts and set-up their data servers on the ship's LAN. Upon return to CONUS, the aircrews must re-establish their squadron's e-mail connectivity and data servers back at their home base.

National Guard Unit Mobilized to Active Duty

An Army National Guard Unit operates on the unclassified NIPRNET Reserve Component Automation System (RCAS). RCAS is an automated information management system that links Army National Guard and Reserve units around the world. Personnel have email, shared drives and files that reside on this network. The RCAS network does not share resources, such as files and folders with AKO (Army Knowledge Online), so a separate account for all active Army files is required. When a State National Guard unit is activated from they are moved from home station to a mobilization station. At the mobilization station, the National Guard unit no longer has access to RCAS and must either obtain network access and a new email account from the mobilization station network infrastructure, or they must use personal mobile access devices to get on the public internet. The unit command element spends much time communicating with the unit they will replace, the cadre conducting mobilization training, and the original state command structure. Because the unit does not have connectivity to its original RCAS, steps must be taken to ensure all unit data is replicated and hand carried prior to home station departure. Additionally, specialized programs such as the USR (Unit Status Reporting) program PC-SORTS must be reconfigured to support new command channels and reporting criteria. Lastly, the same challenges take place on classified networks. If a unit requires SIPRNET or JWICS connectivity at home station and is receiving data from the theater to support their upcoming mission, then this data must be replicated and hand carried in order to allow use at the mobilization station. This adds the additional security and administrative burden of hand carrying classified data during an already chaotic time. E-mailing large files from RCAS or SIPRNET to AKO or AKO-S (AKO SIPR) for access at the mobilization site is unrealistic. The network services to support large files, such as graphics, are often not available. After departing the mobilization station, the unit then moves to an interim point of departure. The unit may be in a forward location awaiting movement for some time. Again, steps must be taken to create new NIPRNET and SIPRNET accounts on the local infrastructure. When the unit finally relocates to the forward operating base (FOB), steps must be taken to obtain new accounts for personnel on all relevant networks (NIPRNET, SIPRNET, and JWICS). Until these new accounts are established, the unit often must use the MWR network or other available facilities to communicate on commercial email systems.

3.3.2.2 Vignette

When GIG 2.0 is fully implemented, the Military Services will be able to employ systems and services per the Unified Combatant Command requirements. Information services and applications are immediately available to them at any location with access to GIG 2.0. There will be no need to transport data servers or set up and configure systems for a new network every time a unit deploys to a new location. Access to classified data will be immediately available to authorized users wherever they touch GIG 2.0. COI are groups of users and systems which share a common set of required information and/or services to facilitate a mission or required function.

This focus on community requirements for services will allow users to better utilize data and services specific to their COI. Universal access control will be developed and implemented that works across the entire GIG 2.0. Additionally, GIG 2.0 supported Frequency Spectrum Management will cut across all services minimizing electronic frequency mutual interference experienced today.

3.3.2.3 Operational Impacts

The implementation of GIG 2.0 will have a positive impact on the Military Services and Agencies ability to prepare and train their troops to fight and win conflicts.

Force Application: Military Services will be able to employ a higher tempo of operations by depending on the distributed networked environment to support dynamic planning and redirection. Military Services will be better able to self-synchronize through shared situational awareness and collaboration. GIG 2.0 supports the use of Military Service specific data or web services by the Joint Community when that type of information can support Joint Operations. An example this type of data would be weather, logistics, sensor data or services.

Command and Control: GIG 2.0 will enable the Military Service's ability to support their personnel by providing the ability to locate, communicate, and collaborate with their personnel. GIG 2.0 provides for integrated C2 systems and information assurance capabilities. GIG 2.0 also supports the joint interoperability by integrating infrastructure, data, services, and NetOps capabilities with the C/S/A and mission partners.

Net-Centric: GIG 2.0 supports net-centricity for the Military Services as the network, enterprise services, and information assurance mechanisms allow for tactical, operational, and strategic interoperability that supports the operational employment of the force.

Force Support: GIG 2.0 supports the ability to conduct joint training operations across all the Military Services as we share a common IT framework. The shift to an integrated enterprise management capability reduces IT workloads and provides for the development of joint tactics, techniques, and procedures for IT services. The interoperability testing for GIG systems will be simplified when the GIG 2.0 capability is realized. This common standards approach may reduce both the amount of testing required before fielding IT solutions.

3.3.3 Agencies

3.3.3.1 Problem Statement

All DoD Agencies and field activities have significant involvement with GIG 2.0 in its design, implementation or use of the fielded capabilities. The Defense Information Systems Agency (DISA) will be used in this example because of its responsibilities to field global communications and computing networking and enterprise services. The vignettes below illustrate DISA's role as a Combat Support Agency and how it supports C2, Net-centric, Building Partnerships, Logistics, Force Support, Corporate Management and support JCAs.

Fixed Installation Focus

DISA supplies transport and connectivity services to DoD customers worldwide along with other functions such as data center and enterprise services. The network ordering process is currently designed for long-haul, large service delivery node to large service delivery node connectivity. The Military Departments are then responsible for completing the connectivity to fixed installations or expeditionary forces. Payment for connectivity is determined by the size and type of connectivity requested; this process is governed by the DISN Rates Management Council chaired by PA&E and the DOD Comptroller. The DISN rates process is a bureaucratic one with emphasis on a Military Department's ability to pay vice a direct link to mission support. While all military services today determine their fixed installation and expeditionary force network configurations, those COIs that cross Service/Agency/COCOM lines often suffer from seamless mobility and agility from their network providers.

Customer Added Optimization

Many customers purchase "off-the-shelf" connectivity solutions from DISA and then try to add on technology that will improve the service level they receive. Reliance on tactical user groups to develop and implement transport solutions to get them connected back to the DISN core fosters customized, varied, and non-mission focused solutions. One primary motivation for the customers is to eliminate the need to go back through the DISA ordering process to change service levels. Another is the lack of adequate connectivity solutions for mobile platform and dismounted users. The customer can address some of the shortfalls through "bolt on" appliances as easy solutions to increase throughput via locally caching of recently accessed information, or manipulation of the network session, or both. The implementation of many different types of network transport optimization, utilizing varying proprietary means to improve service levels, can cause overall system degradation through interference or unpredictable traffic patterns.

3.3.3.2 Vignette

Under GIG 2.0, DISA fulfills the needs of DoD C/S/A and mission partners by:

- a. producing engineering standards for voice, video and data transport and information systems
- b. contributing to end-to-end engineering analysis and architectural review
- c. operating the global backbone known as the DISN including modeling and simulation of new transport requirements
- d. operating enterprise computing centers
- e. developing Information Assurance capabilities
- f. providing global C2 applications
- g. providing enterprise services

COIs that utilize the GIG are able to connect quickly from previously unknown/unanticipated locations via standardized transport media provided either by the Military Departments (primarily tactical units) or DISA (primarily fixed stations connected to Service Delivery nodes). Members of the COI, JTF or specific unit will be able to access the network using standard identity management capabilities, receive information regardless of location, access information

necessary to achieve their mission based on role-based authentication methods and communicate via various means across enclaves, COIs and networks. Network service providers will maintain visibility of required network resources, reprioritizing in real time to meet operational requirements.

Warfighters will be equipped by their military service to access network assets via fixed, mobile, wireless or wired capabilities available in that operating area.

3.3.3.3 Operational Impact

Agencies must be ready to support the warfighting mission through extensive pre-planned operations conducted in accordance with well understood and trained procedures. Agencies are responsible for supporting the warfighters with information services in accordance with pre-planned service levels, while maintaining systems and personnel in a state of readiness to rapidly react to those mission requirements they have not proactively planned.

Command and Control: Information regarding the current status of IT services is available to the CCDR to aid in their decision making processes. DISA has operational entities that are available to respond to change orders for a COI within a particular theatre in support of warfighting requirements. Information service levels are maintained in accordance with mission requirements in an environment with a high rate of change through pre-planned and highly automated processes. CCDRs can have confidence that the information services they require to exercise their C2 of mission forces are defined and available per pre-planned agreements, with the ability to rapidly deal with contingencies that impact the IT service levels.

Net-Centric: In this example, DISA is directly involved in satisfying the Net-Centric service requirements in information transport, core enterprise services, network management, and information assurance. Information transport within GIG 2.0 will be developed to support the end-to-end connectivity via a unified set of systems, processes, and personnel. Information Assurance (IA) will be achieved through pre-planned world wide deployment with redundancy, common service levels, and ease of management to eliminate single points of failure from the data center all the way to the tactical edge. GIG 2.0 IA will support confidentiality, integrity, availability, authentication, and non-repudiation. As communications sometimes become degraded during warfighting then continuity of operations and disaster recovery (COOP/DR) plans will be implemented to maintain service to the most critical elements. Interference between multiple systems utilizing a common infrastructure (such as the electromagnetic spectrum) will be prevented through proper planning based on the system use priorities and the battlefield situation.

Building Partnerships: The participating Agencies, DISA in this example, have coordinated how they can improve communications and information services between nations thus building a common understanding and non-combative relationship. These capabilities are planned and directly relate to enhancing the warfighter sharing of information with mission partners thus building an environment of trust and teamwork.

Logistics: GIG 2.0 ensures that DISA has implemented IT capabilities to ensure common levels of service to all worldwide locations to support the deployment and distribution of personnel and supplies in accordance with baseline IT capabilities established by DISA. Supply systems within GIG 2.0 are integrated and consolidated to achieve optimum information sharing capabilities among all DoD and mission partner organizations. Information regarding personnel, facilities, and supplies is available with full support of the re-supply processes and materiel availability within the theater.

Corporate Management and Support: The Corporate Management and Support area is achieved through the GIG 2.0 vision that delivers capabilities in accordance with warfighter mission requirements as the primary driver. Agencies will have coordinated with the activities of program development, budgeting, and acquisition driven by the prioritized needs of the CCDR warfighting requirements. Research and operational testing are focused on supporting service levels needed at the edge to enable ease of movement and superior force application. Enterprise architecture products are coordinated across the DoD and with mission partners to ensure each stakeholder has a clear understanding of the systems, procedures, organizations and requirements.

Force Support: The supporting Agencies in the GIG 2.0 environment pre-planned their actions required to implement the posture change. They coordinated with host nations and partners relative to the configuration changes and implementation plans in the event of the mission execution. They put standard processes in place to prepare for unplanned operations to ensure all operators were fully trained and ready to rapidly address the changing requirements focused on meeting the warfighting mission. Combat Support Agencies, such as DISA, must be ready to support warfighting missions in both anticipated and unanticipated exercises and operations. COCOMS, Services, and Agencies must all participate in architectural and engineering efforts to ensure seamless, interoperable computing, communications and enterprise services now and into the future.

3.3.4 Mission Partners

3.3.4.1 Problem Statement

The ability to rapidly and seamlessly disseminate time-critical information to and from allies and mission partners is difficult. The current means to enable the secure exchange of information among U.S. forces, partner nations, governmental and nongovernmental agencies coordinating military operations is to build separate physical infrastructures for each COI. These separate infrastructures are not interoperable or standardized which results in limited to no information sharing between each COI. Furthermore, seamless and flexible connectivity worldwide does not exist to allow combined forces to interoperate regardless of location. "Seamless" refers to the ability of one user to exchange data with another user with little concern for the physical or virtual network and systems supporting the information exchange. "Flexible" refers to the ability to quickly reconfigure the infrastructure to meet the rapidly evolving and emerging needs of combatant commands and their partners. "Worldwide" refers to the ability of GIG 2.0 equipped

forces to "plug and play" in any region of the world with common levels of service and without excessive administrative action.

3.3.4.2 Vignette

Mission partners provide people to the CCJTF staff to aid in operational planning. These mission partners interact with and directly liaise with their home organization to assist in the overall mission. Some of these mission partners, while not directly involved, advise the CCJTF on cultural and social issues related to the conflict. Additionally, some mission partners do not want to be associated with any government or military force, but still would like to provide or receive information from the CCJTF in the region. Meanwhile, other partners are providing troops into the conflict and require real-time awareness to C2 the troops under tactical control of the CCJTF. Each mission partner has a choice to bring their own infrastructure or use the existing equipment to help execute their mission. The mission partner may directly connect the GIG 2.0 infrastructure with little effort or administrative support.

3.3.4.3 Operational Impacts

GIG 2.0 will help provide mission partners with better information to help shape their activities and thereby strengthening our global defense posture. GIG 2.0 operational impacts for the Mission Partners are categorized in several JCAs. The paragraphs below relate to the impact GIG 2.0 will have on each of the Tier 1 JCA in relation to working with Mission Partners.

Force Application: GIG 2.0 improves engagement and maneuver operations through seamless information flow across the battlefield. GIG 2.0 also improves the non-kinetic means of operations in cyber warfare by providing improved doctrine and refinement of cyber warfare tactics with our mission partners. Furthermore, the GIG 2.0 doctrine and procedures will improve the cyber defense posture of the US and mission partners.

Command and Control: GIG 2.0 supports the necessary coordination and cooperation of allies and mission partners. GIG 2.0 has large impact on the C2 JCA for Mission Partners. GIG 2.0 enables direct C2 with mission partner forces. GIG 2.0 also enables sharing of information and awareness with mission partners. The GIG 2.0 improvements in the infrastructure and policies help foster communications with mission partners. More specifically, a CCJTF is able to locate and communicate its intention and guidance with all members of its staff using GIG 2.0. For example, CCJTF will be able to disseminate changes to the Mission's Rules of Engagement consistently to all forces of the CCJTF. Furthermore, the combined forces have a seamless ability to identify and communicate within GIG 2.0 via secure access to authorized information and services.

Battlespace Awareness: GIG 2.0 provides a means to receive intelligence information and disseminate information to our mission partners. Real time data from US and mission partner forces feed directly to CCJTF via GIG 2.0's communications paths. As an example, GIG 2.0 enables the dissemination of position location information of US and mission partner forces to prevent Blue-on-Blue engagements. Furthermore, at the CCJTF, GIG 2.0 augments the planners with mission partner data to provide a seamless means to plan and execute the conflict.

Net-Centric: For mission partners, GIG 2.0 provides a framework for information exchange within the DoD. Proper cyber management is accommodated through mission partner involved processes based on pre-defined, common levels of information exchange across the entire GIG 2.0. Changes that accommodate unanticipated users and reconfiguration based on user population and mission needs are understood and accepted as mission essential changes that do not change the risk level incurred by all users. From an Information Assurance standpoint, the GIG 2.0 systems undergo a common set of certification testing and risk analysis to gain an accreditation that presents a known acceptable level of risk to all "worldwide" members.

Building Partnerships: GIG 2.0 enhances the ability to communicate with our mission partners. GIG 2.0 provides a standardized means for mission partners to directly connect during a mission. This direct connection builds trust and fosters better relationships between the US and other nations through ad-hoc relationships or pre-existing national agreements. COI can be rapidly established to provide domestic and foreign audiences up to date status of the mission.

Logistics: The use of common standards permeates throughout GIG 2.0. The interaction with mission partners requires the use of common, open standards to ensure interoperability. GIG 2.0 can enable the ordering and shipment of parts from a mission partner if needed for mission operation. This also applies to personnel replacements provided by mission partners who can be connected to GIG 2.0

Force Support: Under the GIG 2.0 concept, mission partners have access to authorized information when required based on mission needs. The mission partners and U.S. forces are trained using the common Tactics, Techniques, and Procedures (TTPs) and capabilities of GIG 2.0. Information and knowledge that benefits participants before the start of an operation can be rapidly shared as controlled by their authentication and authorization credentials.

3.3.5 GIG 2.0 and JCA Relationship Summary

The scenario above only partially illustrates the potential impacts of GIG 2.0. Figure 9 below presents, in a table form, the various perspectives and their potential applicability to the JCA. The C2 scenario used gives an illustration of GIG 2.0 impacts. While all the JCAs will be affected by the implementation of GIG 2.0, the check marks (✓) signify a potential near term improvement in these areas upon the implementation of GIG 2.0

	JCA Tiers		COCOM Perspective	Services Perspective	Agency Perspective	Mission Partner Perspective
	Tier 1	Tier 2				
Joint Capability Areas (JCA)	Force Application	Maneuver	✓			✓
		Engagement	✓			✓
	Command and Control	Organize	✓			✓
		Understand	✓		✓	✓
		Planning	✓		✓	
		Decide	✓		✓	
		Direct	✓			✓
		Monitor	✓			✓
	Battlespace Awareness	Intel, Surveillance & Recon	✓	✓		✓
		Environment		✓		
	Net-centric	Information Transport	✓	✓	✓	✓
		Enterprise Services	✓	✓	✓	✓
		Net Management	✓	✓	✓	✓
		Information Assurance	✓	✓	✓	✓
	Building Partnerships	Communicate				✓
		Shape	✓		✓	✓
	Protection	Prevent	✓			
		Mitigate	✓			
	Logistics	Deployment & Distribution	✓	✓	✓	
		Supply	✓	✓		
		Maintain		✓		
		Logistics Services	✓	✓		
		Operational Contract Support		✓		
		Engineering	✓	✓	✓	✓
	Forces Support	Force Management		✓		✓
		Force Preparation		✓		✓
		Installations Support		✓	✓	
		Human Capital Management		✓		
		Health Readiness	✓	✓		
	Corporate Management and Support	Advisory & Compliance			✓	
Strategy & Assessment				✓		
Information Management				✓		
Acquisition			✓	✓		
Program, Budget & Finance			✓	✓		
	Research & Development		✓	✓		

Figure 9: JCA and GIG 2.0 Vignette Perspectives

4 GIG 2.0 Hierarchy and Structure

4.1 Overview

Information superiority requires unity of command and unity of effort in command, control, operations, and management of the GIG. As a practical matter, unity of effort is necessary due to the vast number of IT resources required to support worldwide GIG 2.0 operations. Services in support of GIG 2.0 will fulfill requirements from all Combatant Command AORs, and all DoD users from anywhere in the world. GIG 2.0 supports DoD users that are deployed or operate from their home base. The GIG 2.0 IT infrastructure, information services, data, policies, standards, and procedures must support the operational forces in all of their assigned missions. GIG 2.0 must leverage current policies and directives and be flexible and tailorable to accommodate changes required by the various Combatant Command missions. GIG 2.0 must be capable of supporting all operations at all levels of warfare from strategic to tactical operations.

Under the current construct, USSTRATCOM directs GIG operations and defense, while GIG service providers (DISA, Services, Agencies, etc) provide transport, enterprise services, entity/access/authorization, authoritative data sources for NETOPS throughout the GIG. GIG service providers also maintain IT services IAW the respective Service Level Agreements (SLAs) for all GIG users. This centralized direction and coordination construct also acknowledges that there is some universal risk related to shared global infrastructure and services and that the USSTRATCOM must develop plans to mitigate that risk. The GIG 2.0 organizational construct will require additional visibility of the status of all services, and the ability to rapidly react to cyberspace operational situations that have instantaneous worldwide impact.

To adequately support the operational commanders, GIG 2.0 should be centrally directed and coordinated to ensure each joint commander receives the required level of service and effectiveness. GIG 2.0 provides a force multiplier effect by improving unity of command and unity of effort as detailed in the earlier sections of the CONOPS.

The objective chain of command and supporting relationships described herein are designed to achieve the GIG 2.0 goals by significantly improving unity of command, unity of effort, and speed of command through centralized control and decentralized execution of the GIG 2.0. Inherent in the new GIG 2.0 hierarchy is that CCDRs will exercise authority over assigned forces and prioritize GIG actions in support of their missions in their AOR. GIG 2.0 will allow global allocation of GIG resources among CCDR missions in response to new operational directives and GIG events.

4.2 GIG 2.0 Relationships and Responsibilities

The organizational relationships required to achieve success will ensure visibility, monitoring, coordination, management, defense, and control of the GIG 2.0. This will establish positive end-to-end distributed management and control while still providing common services and SLAs for each AOR. This will provide the DoD with an organizational structure where:

- The GIG is treated as a warfighting system. NetOps is institutionalized to support DoD missions, functions, and operations in a manner that enables authorized users and their mission partners to access and share timely and trusted information on the GIG
- NetOps is the responsibility of Commanders of all DoD Components. Commanders must recognize the vital role NetOps plays in mission accomplish and implement discipline and high standards to ensure prompt adherence to all GIG operation directives and instructions.
- GIG Enterprise Management (GEM), GIG Net Assurance (GNA), and GIG Content Management (GCM) functions shall be operationally and technically integrated to ensure simultaneous and effective monitoring, management, and security of the enterprise.
- NetOps-related data shall be shared and exchanged through common interoperable standards in accordance with DoD net-centric data strategy.
- A common set of NetOps mission-driven metrics, measurements, and reporting criteria shall be used to assess GIG operating performance and to determine the mission impact of service degradations or outages.
- GNA is informed by all-source intelligence, GIG defense postures are adjusted accordingly, and NetOps activities are coordinated and integrated with other cyberspace operations

The necessity for unity of command and unity of effort traverses traditional C/S/A boundaries and dictates commanders at all levels will implement and enforce the common, unified, joint infrastructure, policies, and standards defined to achieve information superiority. Control will be centrally directed with decentralized execution to provide for joint common IT services and to optimize GIG 2.0 resources to best support national priorities. This CONOPS proposes that command relationships for GIG 2.0 be established to facilitate the successful implementation and employment of GIG 2.0. The key characteristics of a successful organizational structure are the establishment of clear GIG organizational authorities and responsibilities in a hierarchical relationship that provides for top-to-bottom control of the GIG.

5 Summary

The GIG 2.0 CONOPS is a living document that supports the implementation of National and DoD strategies. These strategies require joint, common, integrated IT infrastructures which will enhance operational capabilities while mitigating risks. GIG 2.0 is designed to support the following goals: accelerate availability of trusted information to achieve decision superiority; transform to a single information environment; drive policy, resources, mitigation strategies, and cultural changes to achieve net-centric operations. Furthermore, GIG 2.0 is founded upon the following 5 characteristics: Global Authentication, Access Control, and Directory Services; Information and Services from the Edge; Joint Infrastructure; Common Policies and Standards; and Unity of Command. GIG 2.0 creates a holistic environment that provides for unified communications, computing infrastructure, core enterprise services, specialized services, service delivery, and information assurance.

GIG 2.0 supports all DoD missions and functions in war and peace, along with supporting DoD's involvement with interagency, coalition, state, local, and NGO mission partners. Joint basing efforts will be enabled by GIG 2.0. GIG 2.0 is a joint vision that incorporates existing and planned warfighting capabilities in order to facilitate mission accomplishment across the full range of military operations.

References

1. Joint Chiefs of Staff, *CENTRIXS Cross Enclave Requirement (CCER) Concept of Operations for Coalition Information Exchange, Version .2*, Joint Staff, June 2008.
2. Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, Washington, D.C., 2006.
3. Joint Chiefs of Staff, *The National Military Strategy of the United States of America: A Strategy for Today, a Vision for Tomorrow*, Washington, D.C., 2004.
4. United States Department of Defense, Chief Information Officer, *Defense Information Enterprise Architecture Version 1.0*, Washington, D.C., April 11, 2008.
5. United States Department of Defense, Chief Information Officer, *Department of Defense Information Sharing Strategy*, Washington, D.C., May 4, 2007.
6. United States Department of Defense, Chief Information Officer, *Department of Defense Net-Centric Services Strategy*, Washington, D.C., May 4, 2007.
7. United States Department of Defense, Chief Information Officer, *DoD Net-Centric Data Strategy, Memorandum for Secretaries of the Military Departments*, Washington, D.C., May 9, 2003.
8. United States Department of Defense, Deputy Secretary of Defense, *Transforming Through Base Realignment and Closure (BRAC) 2005 – Joint Basing, Memorandum for Secretaries of the Military Departments*, Washington, D.C., Jan 22, 2008.
9. United States Department of Defense, Secretary of Defense, *Quadrennial Defense Review Report*, Washington, D.C., February 6, 2006.
10. United States Joint forces Command. *Command and Control (C2) Joint Capabilities Document (JCD), Version 2.0 (Draft)*, Joint Staff , June 2008
11. United States Department of Defense, Deputy Secretary of Defense, *Joint Capability Areas (JCA), Memorandum for Secretaries of the Military Departments*, Washington, D.C., Feb 14, 2008.
12. Defense Base Closure and Realignment Commission, *2005 Defense Base Closure and Realignment Commission Report*, Arlington, VA, 8 Sep 2005
13. Unified Command Plan (UCP), 17 Dec 2008.
14. DoDD 5100.1, “Functions of the Department of Defense and Its Major Components”, 1 Aug 2002.

15. DoDD O-5100.30, "Department of Defense (DoD) Command and Control (C2)", 5 Jan 2006.
16. DoDD 8100.01, "Global Information Grid (GIG) Overarching Policy", 19 Sep 2002.
17. DoDD 8320.02, "Data Sharing in a Net-Centric Department of Defense", 2 Dec 2004.
18. DoDD 8500.01E, "Information Assurance", Oct 24, 2002.
19. DoDD 8581.1, "Information Assurance (IA) Policy for Space Systems Used by the Department of Defense", 21 Jun, 2002.
20. DoDI 8410.02, "NetOps for the Global Information Grid (GIG)", 19 Dec 2008.
21. Joint CONOPS for GIG NetOps, 4 Aug 2006
22. GAO Report to Congress, "Defense Acquisitions: DoD Management Approach and Processes Not Well-Suited to Support Development of Global Information Grid", January 2006.

Glossary

This Glossary is intentionally limited to those terms having very significant impact on the content of the base document. For the balance of terms used this document the reader is directed to Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms." The contents of JP 1-02 can be found on the Internet at <http://www.dtic.mil/doctrine/jel/DoDdict/>.

Command Authorities – The DoD has three forms of operational command authority. These are Combatant Command (COCOM), Operational Control (OPCON), and Tactical Control (TACON). Each of these authorities is defined below.

Combatant Command (COCOM) - COCOM is nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by Commanders of unified combatant commands unless otherwise directed by the President or the Secretary of Defense. COCOM cannot be delegated and is the authority of the Combatant Commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. COCOM (command authority) should be executed through the Commanders of subordinate organizations. Normally this authority is exercised through subordinate Joint Force Commanders and Military Service and/or Functional Component Commanders. COCOM (command authority) provides full authority to organize and employ commands and forces, as the Combatant Commander considers necessary to accomplish assigned missions. Operational control is inherent in COCOM (command authority).^[1]

Complex Systems - Complex-systems are systems that continually maintain or increase their own fitness by following the processes of natural evolution and maturation.

Direct Liaison Authorized (DIRLAUTH) –The authority granted by a commander (any level) to a subordinate to directly consult or coordinate an action with a command or agency within or outside of the granting command. DIRLAUTH is the key enabler to overcome cultural and political barriers regarding information sharing. DIRLAUTH will authorize the continuous electronic near real time exchange of critical NETOPS configuration and status information that will result in situational awareness and stimulate the NETCOP.

Global Information Grid (GIG) – A DoD CIO Memorandum, dated 22 September 1999, established the definition of the GIG, which subsequently was revised on 2 May 2001, by agreement between the DoD CIO, Under Secretary of Defense (USD) for Acquisition

^[1] Joint Pub 1-02, *Unified Action Armed Forces (UNAAF)*

Technology and Logistics (AT&L), and the Joint Staff/J6. The GIG is defined [Source: GIG Capstone Requirements Document, JROCM 134-01, 30 August 2001] as follows:

- a. Globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5124 of the Clinger-Cohen Act of 1996. The GIG supports all DoD, National Security, and related Intelligence Community (IC) missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems.
- b. The GIG includes any system, equipment, software, or service that meets one or more of the following criteria:
 - Transmits information to, receive information from, routes information among, or interchanges information among other equipment, software, and services.
 - Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services.
 - Processes data or information for use by other equipment, software, and services.
- c. Non-GIG IT – Stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

GIG 2.0 – The Department of Defense (DoD) effort to evolve the GIG into a seamless, single information environment optimized for the warfighter to achieve and maintain the information advantage as a critical element of national power.

Information superiority – the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (JP1-02) Information superiority is achieved in a non-combat situation or one in which there are no clearly defined adversaries when friendly forces have the information necessary to achieve operational objectives.

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

Tactical Edge – Tactical level of warfare users and the IT/NSS systems and services supporting the operational mission. The boundary of the tactical edge is considered to be everything forward of a deployed tactical network's DISN Point-of-Presence (POP)/Service Delivery Node (SDN). As with tactical unit boundaries, the contours of the tactical edge will vary by Service, mission, phase of an operation, bandwidth availability, and other factors (both technical and non-technical). The tactical edge is tiered with bandwidth availability and organizational boundaries as major factors defining the tiers. The lowest tiers of the tactical edge include disadvantaged/dismounted and mobile users.

Acronym List

AKO - Army Knowledge Online
AOR - Area of Responsibility
ASD /NII - Assistant Secretary of Defense (Networks & Information Integration)
BA - Battlespace Awareness
BP - Building Partnerships
BRAC - Base Realignment and Closures
C2 - Command and Control
CCDR - Combatant Commander
CCJTF - Commander Combined Joint Task Force
CDD - Capabilities Development Document
CDRUSSTRATCOM - Commander United States Strategic Command
CDIP - Capability Delivery Increment Plan
C/S/A - Combatant Command/Service/Agency
CJCS - Chairman of the Joint Chiefs of Staff
CJTF - Combined Joint Task Force
CM&S - Corporate Management & Support
CND - Computer Network Defense
COA - Course of Action
COCOM - Combatant Command
COI - Community of Interest
COOP - Continuity of Operations
CONUS - Continental United States
CONOPS - Concept of Operations
CPM - Capability Portfolio Manager
CVN - Carrier Vessel-Nuclear
DIA - Defense Intelligence Agency
DIE - Defense Information Environment
DIEA - DoD Information Environment Architecture
DISA - Defense Information Systems Agency
DISN - Defense Information System Network
DoD - Department of Defense
DoD CIO - Department of Defense Chief Information Officer
DoS - Department of State
DR - Disaster Recovery
EA - Enterprise Architecture
FA - Force Application
FCB - Functional Capabilities Board
FOB - Forward Operating Base
FOIA - Freedom of Information Act
FS - Force Support
FSA - Functional Solutions Analysis

GCC - Geographic Combatant Commander
GEM - Global Information Grid Enterprise Management
GNA – GIG Net Assurance
GIG - Global Information Grid
HQ - Headquarters
IA - Information Assurance
IC - Intelligence Community
ICD - Initial Capability Document
IP - Internet Protocol
ISR - Intelligence, Surveillance, and Reconnaissance
IT - Information Technology
ITSM - Information Technology Service Management
JBIG - Joint Basing Implementation Guidance
JCA - Joint Capability Area
JCB – Joint Capabilities Board
JCD – Joint Capabilities Document
JCIDS - Joint Capabilities Integration and Development System
JROC - Joint Requirements Oversight Council
JTF - Joint Task Force
JTF-GNO - Joint Task Force-Global Network Operations
JWICS - Joint Worldwide Intelligence Communication System
LAN - Local Area Network
MWR - Morale, Welfare, and Recreation
NC - Net-Centric Operations
NETOPS - Network Operations
NGO - Non-governmental Organization
NIPRNET - Unclassified but Sensitive Internet Protocol Router Network
NMCC - National Military Command Center
NSA - National Security Agency
NSS - National Security System
OSD - Office of the Secretary of Defense
OV - Operational View
RCAS - Reserve Component Automation System
SAM - Surface to Air Missile
SCAMPI - Standard CMMI Appraisal Method for Process Improvement
SIPRNET - Secret Internet Protocol Router Network
SLA - Service Level Agreement
SWG - Sub-Working Group
TCP/IP - Transmission Control Protocol / Internet Protocol
TTPs - Tactics, Techniques, and Procedures
UCP - Unified Command Plan
USNORTHCOM - United States Northern Command
USG - United States Government
USR - Unit Status Reporting
USSOCOM - United States Special Operations Command
USSTRATCOM - United States Strategic Command

USTRANSCOM - United States Transportation Command
WAN - Wide Area Network
WMA - Warfighter Mission Area