TRADOC Pamphlet 525-7-17

The United States Army
Concept Capability Plan for

Network Transport and Services

for the
Future Modular Force

2015-2024

Version 1.0

12 August 2008

Foreword

From the Director
U.S. Army Capabilities Integration Center

Emerging joint and Army concepts emphasize enhanced Modular Force capabilities that are enhanced and enabled by the rapid and secure sharing of information. *The U.S. Army Concept Capability Plan for Network Transport and Services for the Future Modular Force 2015 - 2024* identifies the network transport and services capabilities required to meet the demands of Army operations in the period from 2015 to 2024 as defined by those concepts.

The complexity of combined arms and joint operations will place extreme demands on future Modular Force commanders and their staffs to manage and integrate enormous amounts of critical information. The advancement of military and commercial communications networks and information service technologies presents an opportunity to enhance information protection and delivery capabilities throughout the force in ways that will enable the warfighting functions envisioned in our future Modular Force concepts. Within this context, the Army may influence and shape the design and development of the network transport and services-related capabilities of the future Modular Force.

TRADOC Pam 525-7-17 describes how the future Modular Force will leverage the power of network transport and services capabilities on the future battlefield. The capabilities identified provide a coherent way ahead for the further examination of potential doctrine, organization, training, materiel, leadership and education, personnel and facilities solutions. As such, TRADOC Pam 525-7-17 is a starting point for a comprehensive capabilities based assessment that will involve virtually every proponent.

As we address network transport and services capability enhancements, we must maintain our focus on enabling Soldiers to transmit information from the “first tactical mile” all the way back to the operational base. LandWarNet provides full spectrum, integrated connectivity from the deployed Soldier to Home Station Operations Centers, national/strategic intelligence centers and logistic support and sustainment locations that creates a collaborative environment providing effective and efficient flow of information to enable information superiority and decision making. Network transport and services are key components of LandWarNet that support these critical capabilities.

Many of the network transport and services-enabled capabilities introduced will be further developed in other proponent capability documents. Because the capabilities addressed in TRADOC Pam 525-7-17 cross so many Army and joint functional areas, I encourage its use in our interactions with other proponents, Services, and joint organizations.

MICHAEL A. VANE
Lieutenant General, U.S. Army
Director, Army Capabilities
Integration Center

This page intentionally left blank.

Executive Summary

Introduction

TRADOC Pam 525-7-17 defines capabilities that provide the required details to initiate a network transport and services (NTS) focused capabilities based assessment (CBA) within the Joint Capabilities Integration and Development System (JCIDS). An NTS CBA will identify doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) solutions or solution sets for a concept focused on the strategic, operational, and tactical application of integrated NTS capabilities required to conduct full spectrum operations in the 2015 - 2024 timeframe. This concept capability plan (CCP) is derived from approved and draft documents addressing the Army's future Modular Force, and also addresses requirements specified in the Army Future Combat Systems Operational and Organizational Plan, the Army's LandWarNet Concept of Operations, emerging joint and Army concepts relevant to Department of Defense (DOD) and Army transformation, and relevant commercial "best practices."

Purpose

The NTS CCP provides a plan for integrating NTS capabilities for the future Modular Force. This CCP defines capabilities associated with network transport, network services, network communications relay, assured mobility communications, future Modular Force network, and federation of networks. The CCP will focus on a knowledge-based network of networks that enables collaboration and the ability to share information across an integrated operations environment unhindered by distance, terrain, weather, or hostile activity. The CCP will define leader-centric NTS capabilities that enable battle command applications and commanders' critical information exchanges to get the right information to the right place at the right time in a format that meets the requirements of leaders and Soldiers while training at home station and through all phases of an operation. In addition, NTS capabilities will enable preparation for and conduct of testing and training functions essential to the readiness of the future Modular Force.

Scope

NTS capabilities support all Army organizations in the conduct of full spectrum operations. When directed, NTS capabilities may also support joint, intergovernmental, interagency, and multinational organizations. This CCP considers all aspects of NTS capabilities connecting users, information systems, and applications at all echelons across the enterprise during all phases of future Modular Force operations. It includes human interaction, application interoperability with the Network, and interoperability with joint, coalition, and commercial capabilities.

Military Problem

a. The future Modular Force must be agile and rapidly configurable and scalable, capable of deploying on short notice and fighting upon arrival. In addressing these requirements, the Army's Future Force capstone concept places significant emphasis and reliance on network-enabled systems and services that will provide a pervasive inter and intratheater communications

infrastructure that connects Soldiers and platforms to global information sources, and integrates sensor networks that collect, modify, and simultaneously disseminate information from multiple noncontiguous locations to enable timely situational awareness and command and control (C2). In order to achieve these future Modular Force capabilities, the Army must influence the design, development, acquisition, and employment of fully integrated NTS capabilities.

b. The future Modular Force will require NTS capabilities that can adjust to modular force missions, better employ joint capabilities, facilitate force packaging and rapid deployment capabilities, and enable units to fight autonomously or as part of a joint and coalition force—linked by the network—in a nonlinear, noncontiguous area of operation. Commanders and Soldiers will depend on information—the ability to share and collaborate—enabled by a full suite of network services through all phases of an operation conducted anywhere in the world. In the 2015 - 2024 timeframe, globally available NTS capabilities will be essential to enabling warfighting functions at all echelons, and will propel both operational and cultural changes in the way the Army fights. NTS must be capable of passing information vital to situation awareness (SA), decisionmaking, and collaborative mission planning, and must provide the infrastructure for integrating network-enabled C2, joint fires, joint maneuver, logistics, protection, and intelligence functions.

Solution Synopsis and Key Ideas

a. The success of the future Modular Force will depend on NTS capabilities. NTS capabilities are fundamental and essential components of future Modular Force operations. Viewed in the larger construct of joint operations, Army NTS capabilities are keys to successful transformation and exploitation of the information environment.

b. NTS capabilities described in this CCP are part of a multitiered construct that combines advanced communications and network management technologies with the expertise, skills, and capabilities of network professionals at theater, corps, division, brigade, and battalion levels. These systems and people combined with globally positioned NTS capabilities that provide access to network services, to space communications assets, and to robust and responsive aerial and terrestrial communications layers, form the “always on” global network that enables the future Modular Force to connect to applications, conduct knowledge management, and execute network-enabled missions.

c. Advanced NTS capabilities will form the backbone of the future Modular Force, introducing potentially revolutionary advances in force effectiveness. NTS capabilities will provide the connectivity, capacity, and network services for forces at all levels to achieve situational understanding; establish, maintain, and distribute a common operating picture; create a commander-centric C2 environment; and operate within a noncontiguous battlefield framework. At the same time, NTS capabilities will sharply enhance the lethality, survivability, agility, versatility, and sustainability of the force, enabling more precise and timely application of the elements of combat power. With an enhanced home station installation information infrastructure, NTS capabilities will support live, virtual, constructive, and distributed training, collaborative planning, en route mission updates, and access to sustainment and information resources. NTS capabilities, providing connection across terrestrial, aerial, and space domains,

will establish the foundation on which all future Modular Force warfighting capabilities will be built.

d. The desired end state envisioned in this CCP is a single, integrated framework for Army NTS capabilities. These capabilities will be responsive to the commander's intent, priorities, and security policies. Integrated networks will provide end-to-end quality of service, enabling the transmission of all data at any classification level effectively and seamlessly from the Soldier/sensor through leaders and command posts up to Army, joint, and national levels to provide the right information to the right people or systems at the right places and times and in formats that satisfy the warfighter's information demands.

e. The span of required capabilities identified in the CCP indicates the need for a NTS focused CBA to determine if current and projected DOTMLPF solutions are adequate, identify capability gaps, and determine possible solutions to mitigate gaps.

Department of the Army
Headquarters, United States Army
Training Doctrine Command
Fort Monroe, Virginia 23651-1046

TRADOC Pamphlet 525-7-17

12 August 2008

Military Operations

THE U.S. ARMY CONCEPT CAPABILITY PLAN FOR NETWORK TRANSPORT AND SERVICES FOR THE FUTURE MODULAR FORCE 2015 - 2024

FOR THE COMMANDER:

OFFICIAL:

DAVID P. VALCOURT
Lieutenant General, U.S. Army
Deputy Commanding General/
Chief of Staff

RANDALL L. MACKEY
Colonel, GS
Deputy Chief of Staff, G-6

History. This pamphlet (pam) is a new U.S. Army Training and Doctrine Command (TRADOC) concept capability plan (CCP) developed as part of the Army Concept Strategy for the future Modular Force and as part of the capabilities based assessment process.

Summary. This CCP defines capabilities that provide the required details to initiate a network transport and services (NTS) -focused capabilities based assessment (CBA), if necessary, within the Joint Capabilities Integration and Development System (JCIDS). An NTS CBA will identify doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) solutions or solution sets for a concept focused on the strategic, operational, and tactical application of integrated NTS capabilities required to conduct full spectrum operations in the 2015-2024 timeframe. This CCP is derived from approved and draft documents addressing the Army's future Modular Force, which includes brigade combat teams, divisions, corps, and Army service component commands. It also addresses requirements specified in the Army Future Combat Systems Operational and Organizational Plan, the Army's TRADOC Pam 525-5-600, emerging Army and joint concepts relevant to Department of Defense (DOD) and Army transformation, and relevant commercial "best practices."

Applicability. This CCP applies to all TRADOC and non-TRADOC Army proponents, and Department of the Army (DA) activities that identify and develop DOTMLPF solutions to field

required NTS capabilities. Active Army, Army National Guard, U.S. Army Reserve operating forces, and U.S. Army Materiel Command may use this CCP to identify future NTS trends in the Army. This CCP may also serve as a reference document for agencies within the joint community that are planning or are otherwise concerned with Army NTS initiatives.

Proponent and exception authority. The proponent of this pamphlet is the TRADOC Headquarters, Director, Army Capabilities Integration Center (ARCIC). The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. Do not supplement this pamphlet without prior approval from Director, ARCIC (ATFC-ED) 33 Ingalls Road, Fort Monroe, VA 23651-1061.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Director, ARCIC (ATFC-ED), 33 Ingalls Road, Fort Monroe, VA 23651-1061. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program Proposal).

Distribution. This publication is only available on the TRADOC Homepage at http://www.tradoc.army.mil/tpubs/pamsndx.htm.

Contents

Foreword **i**
Executive Summary **ii**

Chapter 1 Network Transport and Services Purpose **5**
1-1. Purpose 5
1-2. Why This CCP is Needed 5
1-3. Functional Area 6

Chapter 2 Scope **7**
2-1. NTS Scope 7
2-2. Relation to the Family of Joint and Army Concepts 7

Chapter 3 The Military Problem **14**
3-1. Operational Environment 14
3-2. Problem Statement 20

Chapter 4 Solution **20**
4-1. Solution Synopsis and Key Ideas 20
4-2. Vignettes 24
4-3. Summary 38

Chapter 5 Required Capabilities **40**
5-1. Introduction 40
5-2. Battle Command Network Transport and Services Capabilities 40
5-3. See Network Transport and Services Capabilities 42
5-4. Move Network Transport and Services Capabilities 42
5-5. Strike Network Transport and Services Capabilities 43
5-6. Protect Network Transport and Services Capabilities 43
5-7. Sustain Network Transport and Services Capabilities 44

Chapter 6 DOTMLPF Implications and Questions **45**
6-1. Introduction 45
6-2. Past and Future Experimentation and War Games 45
6-3. Experimentation 46
6-4. Modeling and Simulation 46
6-5. Concept Development and Experimentation (CD&E) 46
6-6. Wargaming 47
6-7. DOTMLPF Questions 47
6-8. Plan for Assessment 54

Chapter 7 Risk and Mitigation **57**
7-1. Introduction 57
7-2. Operational Risk 57
7-3. Expectation Risk 57
7-4. Adversary Action Risk 58

Appendixes
A. References **59**
B. NTS CCP Integrated Concept Development Team Members **62**
C. Bridging Current to Future Capabilities **63**
D. Network Operations (NETOPS) **86**

Glossary **90**

Chapter 1
Network Transport and Services Purpose

1-1. Purpose

a. This concept capability plan (CCP) provides a plan for integrating network transport and services (NTS) capabilities for the future Modular Force and, upon approval, provides the details necessary to initiate an Army NTS-focused capabilities based assessment (CBA). The NTS CBA will identify doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) solutions or solution sets that address NTS capability gaps in the 2015-2024 timeframe.

b. This CCP will integrate efforts to define capabilities associated with network transport, network services, network communications relay, assured mobility communications, future Modular Force network, and federation of networks. The CCP will focus on a knowledge-based network of networks that enables information superiority and decision dominance and facilitates the synchronization of activities required to accomplish the mission. The network will function through comprehensive physical and virtual connections enabling collaboration and the ability to share information across an integrated operations environment, as well as with federal and state agencies, unhindered by distance, terrain, weather, or hostile activity. NTS capabilities must enable command and control (C2) regardless of echelon or manner of employment. In addition, NTS capabilities must facilitate a leader-centric information network that provides the right information to the right place at the right time in a format that meets the information requirements of leaders and Soldiers through all phases of an operation.

1-2. Why this CCP is Needed

a. There is no Army concept or plan that provides a holistic view of the Army's NTS requirements during the future Modular Force concept period (2015 - 2024). The future Modular Force will require NTS capabilities that can adjust to modular force missions, better employ joint capabilities, facilitate force packaging and rapid deployment capabilities, and enable units to fight autonomously or as part of a joint and coalition force—linked by the network—in a nonlinear, noncontiguous area of operation. Commanders and Soldiers will depend on information—the ability to share and collaborate—enabled by a full suite of network services through all phases of an operation conducted anywhere in the world. To meet these demands in the 2015-2024 timeframe, the Army must transform NTS capabilities. Globally available NTS capabilities will be essential to enabling warfighting functions at all echelons, and will propel both operational and cultural changes in the way the Army operates. NTS must be capable of passing information vital to situation awareness (SA), decisionmaking, and collaborative mission planning, and must provide the infrastructure for integrating network-enabled C2, joint fires, joint maneuver, sustainment, protection, and intelligence functions.

b. This CCP describes Army future Modular Force requirements for NTS capabilities. The expected increase in new technologies across all warfighting functions will place heavy demands on NTS capabilities. Operations will consistently be conducted in joint and coalition environments that will increase the complexity of information sharing and collaboration. This

CCP will serve as the foundation for a thorough review of NTS-related DOTMLPF requirements and capabilities. Through the use of illustrative vignettes, the NTS CCP will describe the application of elements of Army and joint concepts to selected mission, enemy, terrain, troops, time available and civil consideration factors, focusing on conditions specific to NTS missions or functions in support of full spectrum operations. The NTS CCP will provide architecture data and details sufficient to initiate, if needed, a CBA within the joint capabilities integration and development system (JCIDS) process.

c. The NTS CCP uses draft and approved documents: TRADOC Pamphlet 525-3-0 the Army in Joint Operations; Army operating and functional concepts; joint operating, functional, and integration concepts; current approved capability documents; and emerging joint and Army concepts relevant to the Department of Defense (DOD) and Army transformation.

1-3. Functional Area

The NTS CCP examines NTS capabilities that will support Army operations from 2015 to 2024. The CCP incorporates key elements of battlespace awareness, command and control, and net-centric operation joint functional areas. This CCP is fully nested with current Army concepts, including TRADOC Pamphlet 525-3-0 and subordinate functional concepts.

Chapter 2
Scope

2-1. NTS Scope

a. NTS capabilities support all Army organizations in the conduct of full spectrum operations. When directed, NTS capabilities may also support joint, interagency, intergovernmental, and multinational organizations. This CCP considers all aspects of NTS capabilities connecting users, information systems, and applications at all echelons across the enterprise during all phases of future Modular Force operations. It includes human interaction, application interoperability with the network, and interoperability with joint, coalition, and commercial capabilities.

b. The CCP covers tactical and strategic (operational base) requirements, all operational phases, including generating force (phase zero) requirements, en route C2 requirements, and joint, coalition, interagency, and nongovernmental organization (NGO) interoperability

c. The CCP considers required capabilities generated at the following multinational, joint and Army echelons: Generating force (United States (U.S.) Army Forces Command and U.S. Joint Forces Command); geographic combatant command and a joint task force (JTF); Army Service Component Command (ASCC) and the numbered Army; joint force land component (JFLC), Army force; functional combatant commander; corps, division, brigade (brigade combat team (BCT)), support brigade, functional brigade), battalion, the company, platoon, squad, and Soldier; special operations force, and allied and coalition forces.

d. The CCP addresses existing and projected network transport and services via assured end-to-end connectivity across the net-enabled environment in a multi-tiered architecture including terrestrial, aerial, and space.

e. The CCP addresses the joint capability area net-enabled tier 2 and 3 services listed below.

(1) Information transport (for example, voice, data, imagery, and video (including full-motion real-time video)), wired transmission, wireless transmission, and switching and routing

(2) Enterprise services (network operations (NETOPS) global enterprise management (GEM) and global content management (GCM)), including information sharing and computing (physical and virtual access to hosted information and data centers); core enterprise services (common collaboration, mediation, discovery, and messaging); and, position, navigation, and timing (precise location, orientation, time and course corrections anywhere in the battlespace).

(3) Network management to include optimize network functions and resources; deployable scalable and modular networks; spectrum management; and enabling of operations conducted in Army cyberspace.

(4) Information assurance (NETOPS global network defenses (GND) that apply protect, detect, respond and restore measures to information and information systems). This includes secure information exchange (secure dynamic information flow within and across domains); protect data and networks (anticipate and prevent successful attacks on data and networks); and, respond to attack or event (maintain services while under cyber-attack, recover from cyber-attack, and ensure availability of information and systems).

(5) Appendix D describes NETOPS, network operations functions, and the relevance of NETOPS to NTS capabilities.

f. The NTS CCP will consider spectrum management as it relates to NTS considerations, but will not specifically address the larger aspects of electromagnetic spectrum operations as a topic. Spectrum management is a subset within the newly established electromagnetic spectrum operations (EMSO) construct. Frequency assignment, as described in the EMSO CCP, is the EMSO function primarily associated with NTS.

g. The NTS CCP will consider operations in cyberspace as it relates to NTS considerations but will not specifically address the larger aspects of cyberspace operations as a topic. This is currently being considered by a separate TRADOC-chartered Integrated Capabilities Development Team (ICDT) (Information & Cyberspace).

2-2. Relation to the Family of Joint and Army Concepts

a. Net-Centric Environment Joint Functional Concept. The TRADOC Pam 5257-17 recognizes the importance of conducting full-spectrum operations in a net-centric environment. The Net-Centric Environment Joint Functional Concept is expressed as an information and decision superiority-based concept describing how joint forces might function in a fully

networked environment 10 to 20 years in the future (2015 - 2024). Within this concept, the networking of all joint force elements creates capabilities for unparalleled information sharing and collaboration, adaptive organizations, and a greater unity of effort through synchronization and integration of force elements at the lowest levels. This concept also states, "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." TRADOC Pam 525-7-17 describes the NTS capabilities necessary to enable the effective execution of warfighting functions in a net-centric environment.

b. Net-Centric Operation Environment (NCOE) Joint Integration Concept. This concept describes, "…a new synergy of DOTMLPF and policy energized by the advances of the information age—a synergy that will enable warfighters and other decision-makers at every joint force level to make and execute superior decisions faster than our adversaries." The NCOE describes the translation of information superiority into combat power by effectively linking, both horizontally and vertically, knowledgeable entries throughout the area of operation, making possible dramatic new ways of operating by optimizing the use of available NTS capabilities in a net-centric environment.

c. The Army in Joint Operations: The Army Future Force Capstone Concept

(1) Focusing on the theater-strategic level of war, the concept reinforces the fact that Army forces will always conduct operations as an integrated component of a joint force. It is clear that the Army will depend on an array of capabilities from other Services and the larger joint community to maximize effectiveness. The future Modular Force will be a strategically responsive, campaign quality force, dominant across the range of military operations (ROMO) and fully integrated with the joint, interagency, and multinational framework. In this context, a campaign is linked firmly to theater strategy and the emerging challenges of traditional, irregular, catastrophic, and disruptive threats posed to the Army in support of joint operations.

(2) The capstone concept lays out seven key operational ideas across the spectrum of conflict to achieve full spectrum dominance and address the diverse threats and the volatile conditions expected to characterize the future operating environment. They are shaping and entry operations, operational maneuver from strategic distances, intratheater operational maneuver, decisive maneuver, concurrent and subsequent stability operations, distributed maneuver support and sustainment, and network-enabled battle command.

(3) The capstone concept states that networked capabilities are the foundation for full spectrum effectiveness, and expects the future Modular Force will be designed as a network-enabled, knowledge-based force. Nested within the evolving joint architecture, the future Modular Force will require a level of globally networked integration that extends from strategic to tactical levels, provides situational awareness to all elements of the force, and effectively links interagency and coalition players at appropriate levels. It will also depend on a networked education system to extend training capabilities from the institutional training base to units and individual Soldiers.

(4) This concept depends heavily on the ability of network-enabled battle command to "facilitate the situational understanding (SU) needed for the self-synchronization and effective application of joint and Army combat capabilities in any form of operation." It also suggests that the Network will improve information sharing, "enabling more effective application of combat power, decentralization, and noncontiguous operations." A key benefit of the network described in this concept is the ability to decentralize operations without sacrificing the coordination or unity of effort typical of centralized C2.

(5) The pursuit of information superiority, from pre-deployment through final decisive operations, is a key requirement defined in this concept. To achieve information superiority, the concept acknowledges the need for a joint-integrated, knowledge-based network of networks, vertically and horizontally integrated across all operational echelons. The knowledge backbone will furnish forces at all levels situational information to inform a joint common operating picture (COP) tailored to force and situation, which will help accelerate the battle command decision-action cycle.

(6) The concept recognizes the future Modular Force will be a space-empowered force that routinely exploits the constellation of military and commercial space platforms to establish communications links that provide global reach for C2, warfighting, intelligence, and business systems. It also notes the importance of improving information dissemination management and information assurance capabilities to provide accurate and timely information. The concept further highlights the need for network advances that will enable the distribution of battle command capabilities among multiple distributed nodes and support multi-echelon collaborative planning. This will eliminate much of the sequential aspect of today's planning methods, and allow streamlining of the military decisionmaking process.

d. The Army Concept for Operational Maneuver

(1) The concept addresses the operational level of war and focuses on the ways and means by which future Modular Force commanders link a broad array of tactical actions to achieve a joint force commander's campaign objectives. The concept presents a detailed discussion of the seven key operational ideas identified in TRADOC Pam 525-3-0 and how they are applied at the operational level of war. The concept reinforces the idea that the Army is a network-enabled force and recognizes the Army's dependence on NTS capabilities.

(2) This concept states that operational effectiveness depends on network-enabled battle command and acknowledges the need for a continuous flow of high quality information about enemy and friendly forces, terrain, and the population. It further states that the future Modular Force will be a knowledge-based, commander-centric force that employs a flexible, adaptive, joint-integrated C2 system to operate within the collaborative information environment.

(3) The concept notes the importance of network-enabled SU to promote self-synchronization and the effective application of joint and Army combat capabilities across the operational spectrum. Networked communications and information service capabilities, embedded at all levels, will enable ground commanders to operate non-linearly and focus operations against the enemy's most critical forces and capabilities. The concept notes that the

network will enhance the lethality, survivability, agility, and versatility of the force, and enable more effective and timely application of the elements of combat power.

(4) Extended range communications networks will expand the commander's reach and ensure continuous connectivity. Further enhanced by advanced information processing and electromagnetic spectrum operations, the network will enable the higher order battlefield visualization needed for commanders and staffs to more effectively and reliably anticipate enemy actions and set conditions for future operations.

(5) Operational maneuver will require a network that can counter threat capabilities through a combination of redundant, multi-layered systems that eliminate single points of failure. Self-healing qualities that automatically adjust and reconfigure the Network, reroute information flows, and execute immediate action measures to thwart enemy actions will be essential to maintain required levels of service. Defenses against computer network attack, deception, electronic intrusion, and monitoring, and the effects of electromagnetic pulse must be embedded within the network to support operational maneuver.

e. The Army Concept for Tactical Maneuver

(1) The concept describes the future Modular Force within the framework of tactical operations–battles and engagements. The Army's future Modular Force must be able to conduct decisive tactical operations in complex, lethal environments to support directly the achievement of campaign objectives across the ROMO. Tactical maneuver involves full dimensional maneuver throughout every domain of the operational environment and features the generation of joint and combined arms synergy.

(2) The concept presents a detailed discussion of five key ideas as defining the most important vectors of change in tactical operations. Underpinning these five key ideas is the need to develop and maintain a deep understanding of the increasingly complex tactical environment. The key ideas are simultaneous and continuous operations, decisive maneuver—new tactical paradigm, routine employment of joint capabilities at tactical level, self-synchronizing, and cooperative engagement, and the quality of firsts (see first, understand first, act first, finish decisively, and re-engage at will).

(3) The tactical maneuver concept emphasizes the idea that successful tactical operations rely on the commander's ability to see first, understand first, act first, re-engage at will, and finish decisively. Achieving these qualities demands superior situational awareness and intelligence capabilities. Tactical formations will exploit higher levels of situational awareness, networked command and control, and improved mobility to defeat the enemy in close combat, maneuver throughout the depth and breadth of the area of operations, transition rapidly from one engagement to the next, and combine offensive, defensive, and stability operations in changing combinations to accomplish assigned missions in any conflict environment.

(4) Network-enabled battle command will facilitate the SU needed for the effective application of Army and joint combat capabilities in any type of operation. At the tactical level,

NTS capabilities will be vital to synchronization, maintenance of a high operational tempo, and continuous operations.

(5) Networked tactical forces will be capable of cooperative engagement between ground-force elements committed in battle together. Tactical forces will also depend on the network to enable the routine employment of joint strike capabilities in support of tactical operations.

f. Army functional concepts. The remaining concepts describing the role of the future Modular Force are the six Army functional concepts: *Battle Command*, *See*, *Move*, *Strike*, *Protect*, and *Sustain*. These concepts describe Army functional capabilities needed to conduct successful full spectrum operations. The following paragraphs address the Army warfighting functional concepts and their relation to NTS capabilities.

(1) The Army Battle Command Functional Concept for 2015 - 2024

(a) This concept calls for "an agile, ubiquitous communications network from space to ground," and notes that such a network will be the "vehicle critical to all aspects of command." The concept considers that a robustly networked force will improve information sharing, and that, in turn, will enhance collaboration, self-synchronization, sustainability, and the speed of command. The concept looks to the network to be, "…the means for distributing battle command capabilities among multiple distributed nodes to enable multi-echelon collaborative planning" and battle command on the move (OTM).

(b) The concept highlights the need to maintain a robust and unbroken C2 network with assault forces during entry operations, to include an en route mission planning and rehearsal (EMPR) capability with which commanders can continuously adjust their plans and conduct virtual rehearsals. The concept further states that in the future, command posts must be capable of maintaining connection to the network while displacing. The concept notes the need for a network that will tie together all components of the integrated operational force, and provide access to the global information grid (GIG) to facilitate sharing of information from and between national, component, and multi-national partners.

(2) The Army See Functional Concept for 2015 - 2024

(a) This concept describes how the future Modular Force will acquire and generate knowledge of itself, its opponent, and the operational environment. The function of seeing and creating knowledge of the operational environment is essential to becoming a knowledge-based, net-enabled force capable of seeing first, understanding first, acting first, and finishing decisively. Every aspect of future Modular Force operations derives increased effectiveness through the ability to see and know, and from that, the ability to anticipate and act. Accurate and timely adversary and environmental information, including precise geo-location, rapid understanding of environmental constraints and cultural knowledge require integration through analysis enabled by reliable network access, data sharing, and collaboration.

(b) The concept notes the network will be an essential factor in radically advancing data exploration, pattern development, and analysis, and the discovery of links and relationships normally hidden in vast quantities of data scattered throughout multiple global data bases. The concept states future Modular Force knowledge requirements will demand a robust network. It indicates entry forces must be capable of employing joint data acquisition capabilities—including the network—to act in coordination with the larger force. It also recognizes that Soldiers acting as sensors will rely on the network to report information incidental to the conduct of their missions. The concept notes that the network will enable cooperative employment of a vast array of intelligence, surveillance, reconnaissance (ISR)—humans, sensors, and data from collection activities—and emphasizes the need for networks and processes that provide "nearly continuous access to internal and external data sources, as well as the flexibility to link with new or non-traditional partners."

(3) The Army Move Functional Concept for 2015 - 2024

(a) This concept focuses on strategic force projection and operational agility in support of joint campaign objectives. The Army's approach to this requirement for strategic responsiveness is through a "…prompt and sustained framework." The future Modular Force will fight as an interdependent part of a networked joint force, integrated at every level. The goal is to establish entry conditions and a knowledge base sufficient to ensure strategic maneuver is not executed as a strategic meeting engagement, but rather as a deliberate introduction of force packages tailored and ready for immediate operations.

(b) NTS capabilities will be essential for knowledge-building and continuous connectivity of forces in the power projection base, in transit to the area of operations, and maneuvering in forward operational locations.

(4) The Army Strike Functional Concept for 2015 - 2024

(a) The concept addresses joint and future Modular Force fires at the strategic, operational, and tactical levels. It reflects future Modular Force elements that will have fully integrated capabilities to employ direct and long-range, precision, highly responsive, reliable, sustainable, readily available and easily deployable fires coordinated with information operations (IO)-related military activities that can support future Modular Force and applicable joint operations. Future Modular Force strike, in conjunction with joint fires, will create interdependent joint and Army fires networks that mutually enhance strike and joint fires capabilities. The future Modular Force strike network will capitalize on joint C2 and joint intelligence, surveillance, and reconnaissance networks, using the collaborative information environment (CIE) and the COP to gain the near real-time SA required to effectively employ strike in support of future Modular Force operations.

(b) The strike function is built around the following key ideas, each of which is supported by NTS capabilities, including reduced response gaps between organic and non-organic strike assets; near real time SA and SU for fires employment; seamless employment of lethal and nonlethal effects; collaborative and dynamic strike planning; and, synchronization and exploitation of joint interdependencies.

(c) Advanced generation technologies will provide commanders a seamless, transparent, reliable, network that enables consistent and sustained strike planning and employment throughout the duration of the campaign.

(5) The Army Protect Functional Concept for 2015 - 2024

(a) The concept lays out a set of enabling tasks and capabilities by which the future Modular Force protects people, physical assets, and information against the full spectrum of threats. The function of protect will take place on land, in the air, on the seas, in space, and in the electronic domains. NTS capabilities will play a role in accomplishing each of the seven enabling tasks: detect, assess, warn, prevent, deter, defend, and respond. These tasks are interconnected and represent the processes of a full dimensional protection environment.

(b) The future Modular Force will rely on knowledge gained through a network-enabled battle command system to facilitate protect functions. A current and accurate COP will support self-synchronization and cooperative engagements throughout campaigns and operations. NTS will protect itself from interruptions or destruction of knowledge that would affect the ability of the Army to maintain its agility, speed, and precise application of power.

(6) The Army Sustain Functional Concept for 2015 - 2024

(a) The concept establishes the logistics support framework for the future Modular Force. At the strategic and operational levels, future Modular Force sustainment is envisioned as a single joint system that senses and interprets the operational environment and responds through networked capabilities and advanced distribution platforms from the source of support to the point of effect. Future Modular Force sustainment will rely on air mobility, advanced distribution platforms, precision delivery systems, and a state-of-the-art command and control network.

(b) NTS capabilities will support future Modular Force logistics operations by enabling logistics command and control, force situational awareness and understanding, data links for logistics operations, in-transit visibility, and seamless medical support from point of injury through evacuation.

(c) An adaptive and dynamic network will support logistics operations on the distributed and asymmetric battlefield. The network will link joint forces and increase operational effectiveness by allowing distributed sustainment forces to efficiently communicate, maneuver, and share a COP.

Chapter 3
The Military Problem

3-1. Operational Environment

a. Threat to the Changing Operational Environment

(1) In the future operational environment, adversaries will use adaptive strategies to defeat our NTS systems. Since information systems collect, modify, and store the battle command information necessary to integrate the elements of future Modular Force combat power, enemy targeting of those systems with every available means must be expected. As the military seeks to both anticipate and shape the future, the joint operating environment indicates the U.S. will not operate in a single, static, operational environment. Instead, U.S. forces will operate in layers of operational environments, which will be in a constant state of flux. The complexity, increasing interaction, and rapid change manifested in political, military, economic, social, informational, and infrastructure effects of globalization will cause rapid change to the operational environment. The joint operating environment establishes a baseline both for understanding what joint operational environments might be and for developing a way to think through the enormous complexities our military will face while planning and conducting operations in the future.

(2) NTS system components will be subjected to the same threats as the platforms being supported. New and emerging technologies will transform the method and manner of warfare. In the next few decades, the U.S. will confront unstable, sometimes diverse, and highly uncertain geopolitical alignments that will generate major changes in adversaries' intent, force array, and strength. There will be increased global and regional interest in local matters that will place greater value in alliances and coalitions. Also, potential adversaries will apply lessons learned based on their study of U.S. methods.

(3) New threats may emerge from aspiring great powers, new regional alignments, or transnational terrorist or criminal organizations. The global explosion in space-based communications, sensor networks, and information technologies, together with continuing proliferation of military and commercial technologies, will allow less wealthy states and non-state entities to enhance their ground combat command and control, communications, computer, and ISR capabilities to a level once maintained only by armies supported by fully industrialized national economies.

b. Threat to be Countered

(1) Future adversaries will not be limited to today's conventional munitions, but will develop both the intent and capability to employ both highly lethal (such as, weapons of mass destruction) and nonlethal weapons (such as cyber and electronic attacks) or effects. Adversaries may also attack spacecraft industrial facilities, launch sites, and even space vehicles during their ascent. Electronic attacks will aim to degrade satellite communications (SATCOM); telemetry, tracking, and control links; and ground stations. Low-power signals, such as those emitted by

the global positioning system (GPS), will be particularly susceptible to localized electromagnetic spectrum interference.

(2) The physical characteristics of a future theater of war also are likely to prove more challenging. Continuing global urbanization increases the probability that U.S. forces will confront complex topography, even where nature itself does not impose it. Early entry operations, support systems, and facilities will be more vulnerable to direct attack because of the proliferation of hostile communications; sensor, missile, and night vision capabilities; an ever expanding array of precision munitions; special operations forces, and insurgent or terrorist capabilities together with a growing threat of WMD. These threats may even dictate that combat forces avoid prolonged occupation of detectable and targetable locations.

(3) Additionally, most adversaries will become more sophisticated with the adaptive use of camouflage, cover, concealment, denial, and deception (C3D2). Skilled employment of C3D2 capabilities will increase ambiguity and obscure the identity of potential foes and forces. Such capabilities are relatively inexpensive, easy to employ, and in most cases, effective, which will ensure their proliferation across the area of operations. Combined with dispersion of forces and other adaptive tactics, the use of C3D2 will affect all forms of intelligence gathering, including space-based assets, making them less effective and harder to employ.

(4) Since NTS will provide Army users access to the GIG, adversaries will use their access to commercial networks (to include the Internet) to attempt command and control warfare (C2W) attacks on the NTS infrastructure and supporting systems. The DOD reliance on non-secure web-based systems with centralized databases accessed through global reach (such as, web-based logistics, non-secure Internet protocol router networks (NIPRNET), and Army Knowledge Online) is another vulnerability that an adversary may exploit to deny service at the database location and penetrate the network through those means. While external threats from potential and actual adversaries pose a significant threat, the immediate vulnerability lies with trusted users who are authorized access to our systems and trusted insiders who design and build the systems and develop the software.

(5) The use of commercial-based technology further increases the risk of malicious activity. Information about commercial off-the-shelf (COTS) and government off-the-shelf technologies, including security and vulnerability features, is readily available from open sources. The Army also relies heavily on globally connected commercial networks to carry information across increasingly extended lines of communication, which may increase the potential for attacks and exploitation of systems on the network. Attacks against information systems can severely affect mission accomplishment by reducing the combat effectiveness of weapon systems, distorting the picture of the battlefield, and adversely affecting tempo and battlefield synchronization. Computer and information system threat mechanisms are grouped into the four categories below.

(a) Compromise of information. When an adversary gains access to friendly information either by making an electronic copy of it or by gaining access to the hosting machine and simply reading it.

(b) Data deception or corruption. When the data contained in a system or transmitted over a data or sensor link is modified intentionally or unintentionally.

(c) Information denial or loss. When access to friendly information is disrupted. This could occur via denial of service or destruction of the bit stream, signal, or database.

(d) Physical destruction or damage. When the original state of a system's physical components are altered or destroyed such that they no longer function according to their design.

(6) Foreign states have the ability to attack the GIG infrastructure. They possess the intelligence assets to assess and analyze infrastructure vulnerabilities, and a wide range of weapons, to include conventional munitions, WMD, and information operations tools, to take advantage of those vulnerabilities. The most immediate and serious infrastructure threats are from trusted insiders, terrorists, criminals, and other groups or individuals who are positioned to conduct well-coordinated strikes against selected critical nodes. While conventional munitions attacks are most likely now, over time our adversaries will develop an increased capacity and willingness to employ WMD. They are also likely to enhance their capabilities for operations in cyberspace. COTS products and seamless services present new security challenges and concerns, providing opportunities to develop software functions that allow unauthorized access, theft and manipulation of data, and denial of service.

(7) An adversary may target specific GIG interconnections around the world, end-to-end sets of information capabilities, or the GIG's associated processes and personnel. Threats to allies may become a threat to the GIG, even though the GIG may not be the primary target. Connectivity and interoperability with coalition, allied, and non-DOD users and systems suggests an expanding universe of potential insider threats to consider. Because the GIG uses commercial systems, widely available attack tools are becoming increasingly capable and deployable by people with limited technical skills. We may expect adversaries to develop asymmetric responses to perceived vulnerabilities.

(8) NTS capabilities constitute a mission-essential national security system that enables network-centric warfighting functions. NTS capabilities supported by commercial satellite platforms will be vulnerable to the same threats as most commercial satellite systems. Threats to NTS systems may originate from a variety of sources and include possibilities such as the capture or destruction of an NTS facility or attacks upon all physical nodes and electronic links associated with the network. Various elements of IO, traditional threats associated with physical destruction of system components, conventional and nuclear weapons effects, and environmental aberrations may all adversely affect NTS capabilities. Because various intelligence studies indicate the most significant threats to military SATCOM (MILSATCOM) originate from the electronic warfare (EW) elements of IO, these capabilities must be mitigated or avoided. Threats to NTS capabilities include warfare directed against the forward broadcast return links, information systems, EW directed against the satellite links, and physical destruction of the various segments.

(9) Adversaries, enabled by the worldwide proliferation of space based telecommunications and information technologies, will attempt to undermine the national will to

conduct operations, and dissolve the cohesion of coalitions and alliances. This undermining effort will evolve in new directions, stemming from reliance on computer systems for processing and storing sensitive information. Because information superiority is crucial to future Modular Force operations, the linkage between IO and space operations is paramount. Elements of space systems will be targets of computer/electronic attack activities, to include computer network operations and electronic warfare. Left unprotected, links will be jammed, spoofed, monitored, or pirated by adversaries. Protection of this friendly capability will be a major objective of space control operations. Information lines of communication (LOC) must be protected if the Army is to succeed.

(10) Adversaries will attempt to use space for hostile purposes. Domestic and international commercial space organizations are expanding our capabilities and, at the same time, those of our adversaries. The majority of new satellites will be communication systems, but new and increasingly more sophisticated imaging satellites are also proliferating. Nations that previously showed little interest in space ventures are now purchasing satellites and paying other nations to launch these satellites into orbit. As a result, states, transnational organizations, factions, or individuals are able to buy militarily significant space products or services. In fact, one-meter or better resolution imagery, sufficient for tactical targeting (if timely) is commercially available today. Other commercial products include radar imagery that penetrates clouds; position, velocity, timing, and navigation services; and a multitude of highly mobile, highly capable communication systems.

(11) Adversaries will not restrict themselves to the use of military satellites, but will use a combination of military and commercial satellites. Therefore, Army operations must assume an adversary will have at least limited access to overhead observation capabilities and telecommunications satellites capable of supporting operations in remote or undeveloped areas, as well as in urban environments. Finally, just as the Army future Modular Force seeks space-enabled capabilities delivered directly to forces in the field, technology advances will allow adversary forces to receive quickly space enabled products in mobile, tactical, or urban environments.

c. Space Operational Environment

(1) Adversaries may alter the space operations environment by interfering with spacecraft, communication links, ground stations, terminals, or the associated information infrastructure. Adversaries may employ a variety of anti-satellite techniques. Enemy special or conventional forces, theater missiles, electronic warfare (EW) means, cyber-attack, and terrorists all pose a threat to vulnerable ground stations, control facilities, and terminals.

(2) Space support to land component operations has traditionally focused on the global strategic missions of facilitating national ISR; long-haul satellite communications relay; positioning, velocity, timing, and navigation data; and weather. Theater-focused operational and tactical space applications have generally piggy-backed on strategic assets, and, with the exception of the global positioning system, generally have been neither persistent nor dedicated to the component commanders. This has limited the extent to which space, as an enabler, has

been integrated into Army C2; reconnaissance, surveillance, and target acquisition, logistics support, and missile defense and warning systems.

(3) Space is a distinct operating domain that is different from land, air, and sea domains. Space assets transcend geographical borders unimpeded. Since there are no recognized political boundaries in space, satellites enjoy "open skies" global coverage. Although space transcends geographical borders, it is the subject of international and domestic laws, regulations, and national policies. While there is no formal definition of where space begins, the treaty known as the, *Outer Space Treaty of 1967*, describes the lower boundary of space as the lowest perigee attainable by an orbiting space vehicle. The fundamental difference between the space and air domains is that objects in space orbit the earth while objects in the air domain fly over the earth.

(4) Operations in space are a primary enabler of the information revolution. Space operations and information management capabilities are interdependent. Space systems are critical in moving high volumes of data at great speed over vast distances to enable the formation of interactive, globally networked databases that provide support to industry, government, and our military forces. The Army must identify its requirements in the development of these systems early, in order to leverage their capabilities in support of Army future Modular Force operations.

d. Information Operations

(1) The primary tactical threat to NTS capabilities comes from IO. IO coordinates and synchronizes the employment of the five core capabilities—psychological operations, military deception, operational security, EW, and computer network operations (CNO)—in support of the combatant commander's objectives or to prevent the adversary from achieving their desired objectives. With regard to NTS, the relevant portions of the IO threat stem from adversary actions: EW (specifically electronic attack (EA) and EW support), elements of CNO (computer network attack (CNA) and computer network exploitation (CNE)), and the supporting capability of physical attack.

(2) EW. EW refers to any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW includes three major subdivisions: EA, electronic protection, and EW support. Threats to NTS include jamming, interception, and exploitation, which result in degradation of commercial and military communications links or the signal environment. NTS uplinks and downlinks are subject to electromagnetic interference, jamming, and geo-location. NTS equipment could be vulnerable to directed energy weapons, which could be used to physically destroy or disrupt electronic circuits.

(3) EA. The objective of EA or electronic degradation is to deny or disrupt an opponent's use of the electromagnetic spectrum. It is defined as the deliberate or incidental radiation, re-radiation, or reflection of electromagnetic energy to degrade or neutralize military combat capability. Electromagnetic jamming, electromagnetic deception, and nondestructive directed energy weapons attacks are intended to disrupt, degrade, or deny use of the electronic spectrum. Jamming can be intentional or unintentional, fixed or transportable, and can vary in

power. Interference and jamming of the Global Broadcast Service (GBS) could disrupt user communications.

(4) Electronic protection. Electronic protection is the protection of friendly forces against enemy employment of electromagnetic emissions for surveillance, targeting, and weapons control, as well as against undesirable effects of friendly employment of EW.

(5) Electronic support. Electronic support is that division of EW involving actions to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Electronic support efforts against GBS beam locations could lead to detection of signals that would assist an enemy in locating friendly forces and could allow the interception of SATCOM signals for intelligence purposes.

(6) The IO threat continues to spread worldwide, with more mature technologies and more sophisticated tools being developed continuously. However, the level of threat varies widely from adversary to adversary. Most opponents currently lack the foresight or the capability to fully integrate all IO tools into a comprehensive attack. Many, with limited resources, will seek to develop only computer network attack options, relying on modest training, computer hardware and software purchases, and the use of hired criminal hackers.

e. Computer Network Operations (CNO)

(1) Computer network operations pose unique problems that continue to hamper our ability to assess and warn of the cyber threat and which reduce our confidence in the assessments contained herein. Military satellite communications and NTS capabilities rely heavily on computer networks. Attempts to degrade, disrupt, deceive, destroy, or deny the functionality of those computer systems poses a significant threat to NTS mission accomplishment. Computer network operations encompasses the elements of computer network attack (CAN), computer network defense (CND), and computer network exploitation (CNE). CNA includes data deception or corruption, compromise of information, information denial or loss, and physical destruction or damage. CND includes efforts to ensure that friendly computer networks are adequately protected from attack, intrusion, and exploitation.

(2) CNE is defined as obtaining information from computer networks. Assessed capabilities include insider recruitment, cryptology, viruses, software and hardware attacks, and remote penetration. An adversary who successfully attacks a computer network that the NTS relied on could substantially degrade the military's combat effectiveness and civil functions. As with the IO threat, the security accreditation process required of NTS mitigates the CNO threats. CNO threats will also be mitigated by the use of information assurance (IA) products of the common criteria list and products that are certified and accredited by an authorized certification laboratory.

f. Physical attack. Physical threats include the entire spectrum of direct and indirect lethal fire, chemical or biological contamination, and nuclear destruction. NTS equipment is also

vulnerable to capture if deployed with forward units. The threat is likely to rise due to foreign nations' growing awareness of the significance of NTS to the U.S. military.

g. Documentation. Threat and threat assessment references are listed in annex A.

3-2. Problem Statement

a. Current NTS capabilities restrict the ability of operational commanders to quickly exploit opportunities, maneuver forces over extended distances, and develop a level of SU that allows them to consistently act within an adversary's decision cycle. Today's networks exist at each command echelon in relative isolation, and must connect through gateways to enable the movement of information between echelons and to access global information resources. The Army is equipped with a mixture of older technologies, newer technologies, and a variety of user-procured and -operated systems, which have generally been developed, acquired, fielded, trained, and deployed separately. Systems are not fully integrated or networked, and some newer systems are not compatible with older systems that are still in use.

b. Networks have to be individually planned and managed using a variety of planning tools, both automated and manual, that are not designed to enable centralized management or the generation of a common network picture. This requires extensive lead times to install networks and to reconfigure networks to keep pace with rapidly changing operations. The requirement to manage advanced technologies—multicast, transmission control protocol, Internet protocol, electromagnetic spectrum use, firewalls, transmission security, and Center for Internet Security stacks for every device on the network—has added to the challenge. Lastly, the current force has a limited ability to provide anything more than voice service to mobile users, and that service has typically been limited to senior commanders and key staff personnel.

Chapter 4
Solution

4-1. Solution Synopsis and Key Ideas

a. The Army's adoption of network-enabled warfighting capabilities demands the creation of fully integrated NTS solutions. As stated in the Net-Centric Operational Environment Joint Integrating Concept. The joint force and mission partners must have rapid access to relevant, accurate, and timely information, and also the ability to create and share the knowledge required to make superior decisions in an assured environment amid unprecedented quantities of operational data. Warfighting commanders must have the ability to rapidly share operational information between widely dispersed locations in austere environments. There must be an enterprise schema for storing and sharing information for warfighting, intelligence, business, and network mission areas across all DOTMLPF domains within the Army and across the joint community.

b. The future Modular Force must be agile and rapidly configurable and scalable, capable of deploying on short notice and fighting upon arrival. In addressing these requirements, future

Modular Force concepts place significant emphasis and reliance on network-based systems and services. These concepts highlight the need for NTS capabilities that support a pervasive inter- and intratheater communications infrastructure that connects Soldiers and platforms to global information sources, and integrates sensor networks that collect, process, and simultaneously disseminate information from multiple noncontiguous locations to enable precision fire and maneuver. In order to achieve these future Modular Force capabilities, the Army must influence the design, development, acquisition, and employment of fully integrated NTS capabilities (see fig 4-1).

c. As stated by the U.S. Army Fires Center of Excellence, The Modular Force requires a flattened robust high speed communications architecture that expedites target data nomination, collateral damage estimation, time-sensitive target engagement, and battle damage assessment across joint echelons. This capability will decrease the living space of high-value individual targets and enemy formations, limit their freedom of maneuver, and reduce or eliminate the damage they can inflict on friendly forces. Communications speed of service is a key enabler in the reduction of targets in-process through economy of force, and makes the difference between target elimination, and pounding the dirt where the target used to be.

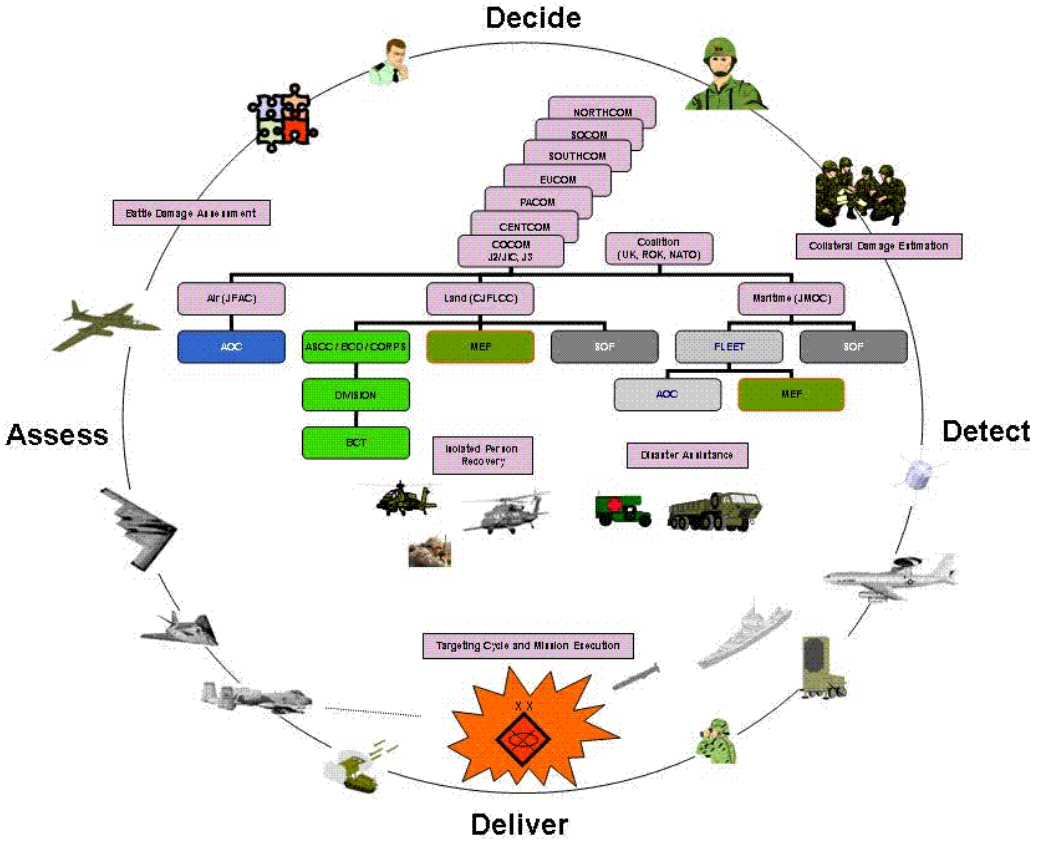

Figure 4-1. Joint Targeting Cycle

d. The complexity of combined arms operations envisioned in joint and Army concepts will create a high demand for accurate, timely information. Future NTS capabilities must provide seamless integration with joint and coalition forces, with federal and state agencies, and with

coalition partners for shaping and peacetime engagement. Faced with dangerous, pervasive, and ever-morphing adversaries, the U.S. will require relevant and ready forces that can provide full spectrum dominance anywhere on short notice. Future NTS capabilities must enable enhanced SU and support a collaborative COP that conveys the mission and the commander's intent, the concept of operation and scheme of maneuver, the logistics structure and status, and the C2 plan. NTS capabilities must enable the establishment of a global collaborative environment that provides shared end-state visualization and an increased ability to see, know, and anticipate. The future Modular Force will require a fully integrated information network that supports all warfighting functions and is compliant with GIG quality of service and speed of service standards and protocols. NTS capabilities must provide a single, integrated information framework capable of responding to the commander's intent and security policy, transporting all forms of information (voice, data, imagery, and video) at all levels of classification, serving all categories of users (joint, national, and coalition), and effectively linking sensors to shooters.

e. Advanced NTS capabilities will form the backbone of the future Modular Force, introducing potentially the most revolutionary advances in force effectiveness. Forces will rely on a knowledge based network of networks, vertically and horizontally integrated from strategic to tactical level. The network will provide the means for forces at all levels to achieve SU; establish, maintain, and distribute a COP; create a commander-centric C2 environment; and operate within a noncontiguous battlefield framework. At the same time, the NTS capabilities will sharply enhance the lethality, survivability, agility, versatility, and sustainability of the force, enabling more precise and timely application of the elements of combat power. With an enhanced home station installation information infrastructure, NTS capabilities will support collaborative planning, en route mission updates, and access to logistics and information resources. Conversely, shortfalls in the achievement of these capabilities will adversely affect nearly all of the operational themes within this concept. NTS capabilities, providing connection across terrestrial, aerial, and space domains and a full range of network-enabled services, will establish the foundation on which all future Modular Force warfighting capabilities will be built.

f. As the Army's component of the GIG, LandWarNet, by definition, makes use of transport and services capabilities provided by the DOD, other services, and commercial vendors. While LandWarNet is capable of operating independently, the ability to leverage non-Army capabilities adds to the robustness and flexibility of the network and network services, providing warfighters access to the collaborative information environment and adding critical support to other communities, such as logistics and home station Battle Command Training Course network training.

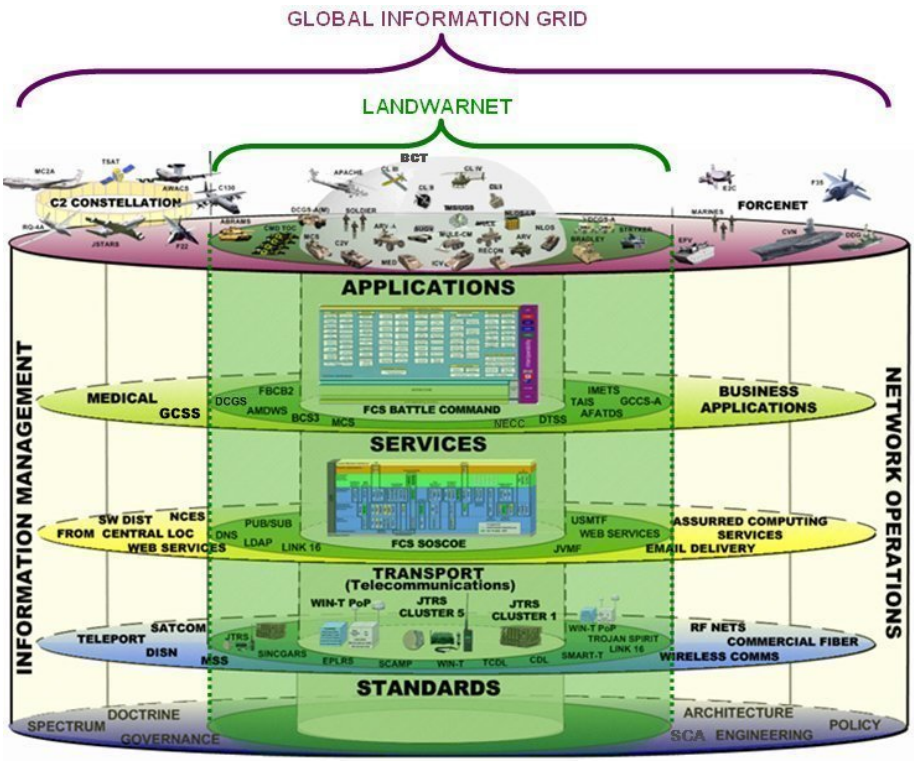

Figure 4-2. Network Layers

g. As depicted in figure 4-2, LandWarNet provides the tools to conduct network-enabled warfare. It consists of several components or "layers" that when brought together provide an integrated information capability that is responsive to commander's needs. These layers are described below.

(1) Applications. Applications translate the required capabilities derived from the warfighting functions into a computer resource. This is achieved through the development of functional applications.

(2) Services. Services provide basic and common computing and networking capabilities that support the functional application. Services allow the free flow of data and information among and between applications and systems. The goal is a common toolset of information technology (IT) infrastructure services.

(3) Transport. Transport provides the “highway” by which information is passed between data systems, platforms, and sensors.

(4) Standards. To ensure interoperability, standards (for data, services, applications, transport, and others) must be implemented and enforced. Without standards, sharing information and the production of a common operating picture become nearly impossible and, at the least is extremely expensive.

(5) Inside the cylinder the layers are held together by information management and network operations capabilities that ensure a robust, dependable, and protected network

capability. The desired end state is a single integrated framework for the Army's network. This network adheres to the commanders' intents, priorities, and security policies. It transports all data at any classification level effectively and seamlessly from the Soldier and sensor through leaders and command posts up to national, joint, and Army levels to provide the right information to the right people or systems, at the right places, at the right times, and in the right formats to satisfy information demands.

h. Army Operations within a Joint Campaign Framework

(1) The joint force will conduct a phased campaign to achieve assigned objectives. The phases, as elements of the joint campaign, can be inferred from the current Capstone Concept for Joint Operations and the Major Combat Operations Joint Operating Concept. These phases often overlap and are described as shape, deter, seize initiative, dominate, stabilize, and enable civil authority.

(2) The Army future Modular Force will conduct operations fully integrated within the joint operational or campaign framework across the spectrum of conflict. Army operations will enable the joint force commander to seize the initiative early, transition rapidly to decisive operations, sustain operations to achieve strategic objectives, and maintain stability thereafter.

(3) Within the context of the joint campaign framework, the Army future Modular Force will apply adaptive combinations of seven key operational ideas, shaping and entry operations, operational maneuver from strategic distances, intratheater operational maneuver, decisive maneuver, concurrent and subsequent stability operations, distributed support and sustainment, and network-enabled battle command. To facilitate the vignette-based description of NTS operations in support of the future Modular Force, this plan will focus on these seven key operational ideas.

4-2. Vignettes

a. Operational setting (see fig 4-3). The illustrative vignettes used in this CCP are built on a notional scenario. National and ethnic tensions in the region have grown over a period of years. Recently, B-Land initiated a campaign to control areas of A-Land populated by a similar ethnic population. A-Land does nothing to reclaim the region involved, and B-Land moves an army corps into the claimed region. Emboldened by the lack of A-Land response, B-Land increases its support of insurgent activities throughout A-Land focusing on population centers. Terrorist acts directed against oil and natural gas production and pipelines increase. B-Land and E-Land initiate military training operations along their shared border and, in a show of solidarity with its ethnic brothers, E-Land repositions forces along its northern border. Rogue paramilitary forces in the eastern region of C-Land seize key pipeline flow regulation and pump facilities and threaten the flow of oil. A-Land requests United Nations and U.S. assistance, and shortly thereafter the President authorizes military intervention.

Figure 4-3. Operational Setting

b. Homeland defense implications. Although not discussed in the following vignette, defense of the homeland remains our highest priority effort. The increase in international tensions associated with these vignettes and the corresponding need for increased vigilance will place additional demands on capabilities both at home and abroad. Integrated NTS capabilities will enable the global communications, ISR, and early warning resources supporting homeland defense operational requirements.

c. Shaping and entry operations (see fig 4-4). Army future Modular Force shaping operations include actions intended to shape regional security conditions and as such are an integral part of the joint prepare and posture phase of a joint campaign. Shaping and entry operations influence the operational environment and set conditions for decisive maneuver.

Figure 4-4. Shaping and Entry Operations

(1) The joint force commander (JFC), staff, and component commanders conduct crisis action planning to update existing contingency plans and initiate shaping and early entry operations. The joint force maritime component commander (JFMCC) deploys forces to gain maritime superiority, secure and establish the sea port of debarkation (SPOD) in west C-Land, and open lines of communication to the east. The joint force air component commander (JFACC) positions an air expeditionary force in D-Land to execute flexible deterrence options, establish air superiority, conduct initial air operations in support of JTF forces and coalition partners, and, as the JTF space authority, coordinate space support. The deputy area air defense commander (DAADC) or the theater Army air and missile defense coordinator (TAADCOORD) plans and coordinates protection of the JTF commander's prioritized defended assets, and plans and coordinates the integration of all required NTS enablers to obtain early warning and cue air defense systems throughout the joint operations area (JOA).

(2) The JFLC (Joint Forces Land Component), an Army corps, initiates deployment of a Future Combat Systems (FCS) BCT by air, to the eastern shore of A-Land, and two Army divisions via sea lift. A joint special operations task force (JSOTF) conducts reconnaissance, and assists in coordinating arrival of the FCS BCT. The theater sustainment command (TSC) and medical deployment support command (MDSC), in conjunction with U.S. Transportation Command, deploys a port opening package to both the aerial port of debarkation (APOD) and the SPOD to establish a single Army logistics C2 and distribution capability in theater for the JFC. The TSC and MDSC coordinate and leverage all joint and strategic partners in the joint operational area (JOA) in all matters of logistics. Additionally, the JSOTF begins cooperative training with coalition military partners. The end state for the shaping and early entry operations is as follows.

(a) The JFMCC established maritime superiority and opened SPOD.

(b) The JTF Forward prepared to deploy and establish initial lodgment area.

(c) The FCS BCT prepared to deploy to eastern port city APOD to secure and defend oil fields, and production facilities.

(d) The JFLC (Army corps headquarters (HQ)) and lead elements of one division initiate deployment operations.

(e) The JFACC air operations center and air expeditionary force is operational in D-Land.

(f) The JFACC exercises flexible deterrence options and joint strike operations to shape the operational environment.

(g) JSOTF forces, in conjunction with coalition partner, conduct reconnaissance and counterinsurgency operations, and provide targeting data to degrade anti-access operations near the APOD.

(h) The joint Public Affairs support element establishes an initial media operations center at the JTF HQ.

(3) NTS capabilities include a wide range of national, civil, and commercial systems and capabilities that influence military operations. In this first phase of the operation, NTS capabilities support all phases of the Army force generation (ARFORGEN) process. In all phases, sensor data coming from Soldiers and equipment platforms will be passed through the network to enable updating of the COP.

(a) Network planners at all echelons collaboratively employ network simulation tools to determine network loading, and levels of network services allocation.

(b) Network links enable individual and collective training; collaborative planning; pre-deployment coordination; the development of a COP, common tactical picture, and single integrated air picture; and orders generation as mission forces assemble at stations in both continental U.S. (CONUS) and outside CONUS locations.

(c) Information and battle command resources supporting preparation and rehearsal at home station are staged from local facilities (for example, local processing centers) to network service centers (NSCs) supporting the operation.

(d) JSOTF forces employ NTS capabilities to provide intelligence, receive instructions, and C2 elements in theater.

(e) APOD and SPOD facilities are connected to sustainment and C2 activities by deployed teams from an expeditionary signal battalion (ESB) through links established to an NSC or through DOD or available leased commercial capabilities.

d. Operational maneuver from strategic distances (see fig 4-5). During both the prepare and posture and shaping and entry operations of a campaign, rapid deployment of ground formations strengthen the JFC's ability to deter conflict, limit its escalation, or preclude early enemy success. Units capable of immediate employment upon arrival diminish an enemy's maneuver options. As the theater matures, forces flow from locations outside the theater with some deploying directly into objective areas while others flow through more traditional staging bases or lodgments.

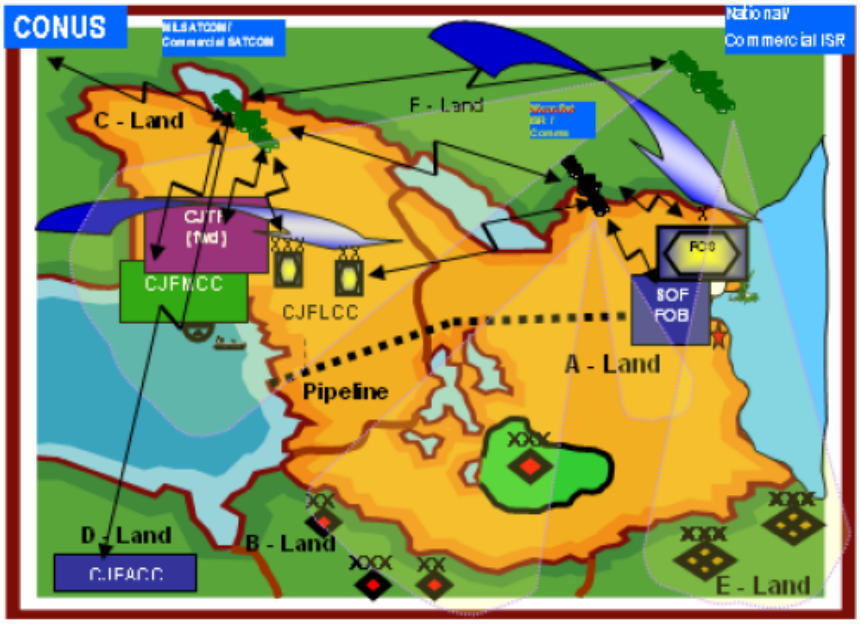

Figure 4-5. Operational Maneuver from Strategic Distances

(1) The JFLC rapidly projects modular combined arms forces into the JOA. Where possible, these mission-tailored force packages bypass intermediate staging bases, deploy in combat-ready unit configurations to positions of advantage, and initiate operations immediately upon arrival. Priority of effort is to the FCS BCT air deployment to the eastern shore of A-Land to secure oil fields and production facilities, and the intratheater deployment of divisional elements to C-Land to preclude the enemy from setting defenses and conducting access denial operations. As the theater matures, forces flow from outside locations through a combination of direct deployment to objective areas and initial lodgment areas. JFMCC maintains maritime superiority. The TSC continues to expand the SPOD in west C-Land, and expands lines of communication to the east. JFACC maintains air superiority, conducts strategic and intratheater lift operations, establishes air exclusion zones, executes counter-air operations, and conducts ISR and air operations to degrade enemy anti-access capabilities.

(2) The DAADC or the TAADCOORD, given the required air defense assets, extends protection of JTF commander's prioritized defended assets, and plans and coordinates the integration of all required NTS enablers to obtain early warning and cue air defense systems as the JOA expands. JFLC establishes entry points, secures critical infrastructure, and conducts military operations in support of A-Land forces against B-Land conventional forces, paramilitary forces, insurgent elements, and transnational terrorists. Two divisions prepare for intratheater

operational maneuver. The JSOTF continues to conduct reconnaissance and cooperative training with coalition military partners. End state for the operational maneuver from strategic distance operations are listed below.

(a) The JFMCC established maritime superiority

(b) The TSC and MDSC bring the SPOD and APOD to a fully operational state.

(c) The JTF Forward is operational in fixed facilities.

(d) The FCS BCT deployment is complete, oil fields and production facilities secure, conducting coordinated operations with A-Land forces.

(e) The JFLC (Army corps HQ) entry points established, combat forces in theater, continues to secure critical infrastructure, conducting initial combat operations in support of A-Land forces, and combating unconventional forces in area of responsibility.

(f) The JFACC air operations center and air expeditionary force is operational in D-Land, strategic lift is 70 percent complete, maintaining air superiority, conducting air operations in support of JFC objectives.

(g) JSOTF forces, in conjunction with coalition partner, continue reconnaissance and counter-insurgency operations.

(3) NTS capabilities available during shaping and early entry operations continue to support operational maneuver from strategic distances are listed below.

(a) NTS capabilities, with heavy space support, enable en route C2 communications for deploying forces during air and sea movement. Commanders and staffs receive COP updates, monitor and adjust network information dissemination/content staging policies, adjust plans and issue revised orders, conduct virtual rehearsals, and receive unit status and logistics reports.

(b) NTS capabilities organic to early entry command posts and arriving combat forces provide immediate access to information and battle command applications staged at supporting NSCs.

(c) Satellite and aerial relays connect mobile command elements to the network as forces move from ports of entry and commence operations.

(d) NTS capabilities enable secure sharing of intelligence generated by sensors and Soldiers in the area of operations (AO), and distribute intelligence products from national assets to appropriate echelons. NTS capabilities enable the tailoring of available network transport to support local commander changing information requirements. NTS capabilities across the functions of enterprise management, content management, and network defense are synergistically integrated to ensure the information requirements of commanders and staffs are satisfied.

(e) ESB elements provide network connectivity, capacity, and services for units located in operating bases with limited infrastructure throughout the AO.

e. Intratheater operational maneuver (see fig 4-6). The future Modular Force executes intratheater operational maneuver to extend the reach of the joint force and enable the JFC to respond to uncertainty, isolate portions of the battlefield, exploit success, and accomplish key campaign objectives. Intratheater operational maneuver can secure positions of advantage to destroy key capabilities and forces, extend tactical reach, achieve surprise, accelerate the advance of the overall force, and block enemy forces.

Figure 4-6. Intratheater Operational Maneuver

(1) The joint force land component commander (JFLCC) executes the intratheater operational maneuver of two tailored division forces for the purpose of blocking enemy forces and preventing them from advancing on the capital city. The division in the north, the main effort, uses a combination of intratheater lift and ground maneuver to secure blocking positions and prepare to attack the B-Land corps. The division in the south, the supporting effort, executes ground maneuver to secure blocking positions that prevent enemy forces from reinforcing the B-Land corps. Extended range unmanned aircraft systems (UAS) and JFLC aviation assets combine with joint fires to support the maneuver of both divisions. Theater air defense assets protect maneuvering forces and provide early warning throughout the JOA. The JFACC provides joint fire support and intratheater lift assets. End state for this operation is as follows.

(a) JFLC divisions are in objective areas blocking the advance of B-Land forces on the capital city. The division in the north prepares to attack the B-Land corps and restore the territorial boundary of A-Land. The division in the south prevents the reinforcement of the B-Land corps. The FCS BCT secures the oil fields and production infrastructure.

(b) JFACC completes the intratheater lift of the division in the north, maintains air superiority throughout the JOA, and provides joint fires.

(2) NTS capabilities available during previous operational phases continue to support intratheater operational maneuver and sustainment. They are discussed below.

(a) Widely dispersed forces synchronize operations through robust OTM C2 capabilities supported by terrestrial, space, and aerial network components. NTS capabilities enable continuous collaborative planning and operational adjustment as the operation continues.

(b) Sharing of situational information to update the COP continues as forces maneuver, allowing commanders to recognize and seize opportunities and rapidly disseminate orders.

(c) NTS users receive continuity of operation plan (COOP) support from the servicing NSC, allowing immediate resumption of operation if service has been disrupted.

(d) NETOPS personnel and automated systems adjust and configure NTS capabilities to support the commander's intent across all mission areas ensuring information flows keep pace with ground force operational tempo.

(e) NTS capabilities enable the linking of ground, aerial, and space sensors with Army and joint strike and protect capabilities to support ground maneuver and force protection operations.

(f) Theater signal brigade and ESB elements deploy as required in support of theater assets.

(g) ESB provides communication packages that provide basic operational network capabilities to units not equipped with organic communications. Theater signal forces, as required, provide operational connectivity to coalition/multinational forces upon arrival to ensure their integration into the tactical network.

f. Decisive maneuver (see fig 4-7). The future Modular Force executes decisive maneuver to achieve the operational tasks assigned by the JFC. Decisive maneuver is characterized by simultaneous, distributed operations, direct attack of enemy decisive points and centers of gravity, and controlled operational tempo.

Figure 4-7. Decisive Maneuver

(1) The JFLCC executes decisive, simultaneous, distributed operations to conduct a direct attack on enemy forces occupying A-Land (main effort) and defensive operations to ensure the security of attacking forces and prevent further cross-border operations by B-Land (supporting effort). The FCS BCT moves to prevent any involvement by E-Land and secure the east coast approaches to the capital city. JFLC secures LOC and conducts operations to prevent paramilitary force disruption of logistics operations. Extended range UAS and JFLC aviation and TSC assets combined with joint fires continue to support the maneuver forces. The JFACC maintains air superiority, provides joint fire support, and conducts reconnaissance operations to monitor threat force movement. End state for this operation is as follows.

(a) JFLC brigades destroy B-Land forces within A-Land and restore the territorial integrity of A-Land. E-Land forces are prevented from conducting cross-border operations. Paramilitary forces are incapable of conducting operations above team level. The A-Land capital city, its domestic infrastructure, and government are intact, and coalition forces are conducting security operations throughout the eastern provinces of A-Land.

(b) JFACC maintains air superiority throughout the JOA and provides joint fires as required.

(2) The NTS capabilities supporting previous operational phases continue to support decisive maneuver operations:

(a) During this high tempo phase of the operation, the allocation of NTS assets is continually monitored and adjusted to ensure adequate network transport and other critical network services are provided in accordance with the commanders' priorities.

(b) OTM C2 capabilities are most critical during this phase, allowing commanders and leaders to position themselves at decisive points on the battlefield while maintaining SA and contact with both subordinate and senior commanders.

(c) OTM elements are able to maintain NTS access to meet mission requirements.

(d) NTS capabilities enable the continuous connection of sensors, shooters, and ground force commanders to maximize the effect of joint and Army fires and maneuver.

(e) Command posts receive a stream of locally- and nationally-generated intelligence products to maintain awareness of enemy force movements. Local intelligence information is passed through the same network transport links to higher headquarters and national agencies for further analysis and dissemination.

(f) Field medical facilities maintain contact with CONUS military and civilian medical centers to consult on patient treatment and conduct telemedicine activities.

(g) NTS capabilities enable updates of unit sustainment status, requests for supplies and repair parts, and casualty reporting. Connection of automated logistics management systems enables immediate updating of global data bases and prompt dispatch of needed materials to the AO.

(h) NTS capabilities enable the collection and distribution of live and recorded imagery from public affairs (PA), combat camera, and sensors for use by strategic communication, information engagement cells, and PA.

g. Concurrent and subsequent stability operations (see fig 4-8). The future Modular Force will conduct stability operations throughout the campaign, often simultaneously with major combat operations. Stability operations present significantly different operational requirements to the future Modular Force. They place a high premium on multifunctional units and Soldiers, involve dynamic mission tailoring, and require careful integration and synchronization of the actions of joint, interagency, intergovernmental, and multinational entities. At the core of this challenge is the requirement to maintain continuous pressure against hostile elements, such as terrorists or insurgents, to deny them freedom of action over an extended period.

Figure 4-8. Stability Operations

(1) The success of decisive maneuver operations causes the remaining team-sized paramilitary forces to withdraw to the more restricted portions of the JOA. These forces initiate ambush and improvised explosive device attacks on the lines of communication. Paramilitary forces target oil pipeline pumping stations and above-ground segments. Insurgents operating in and around the A-Land capital city conduct attacks against A-Land government and municipal facilities in an effort to undermine the government. In a coordinated effort, the JTF, in conjunction with its coalition partner, multinational entities, and interagency organizations conduct stability operations throughout the JOA. The JFLC conducts counterinsurgency operations in and around the A-Land capital with mission-tailored forces. These forces team with national and local civil authorities to ensure synchronization of action. One heavy BCT conducts security operations to protect the oil pipeline. JFLC continues LOC security and operations to defeat the remaining paramilitary forces. JFACC conducts intratheater lift operations to support stability and humanitarian operations, conducts reconnaissance, and provides joint fire support. The TSC and MDSC continue theater support operations. The DAADC or the TAADCOORD plan and coordinate for the continued air defense protection of the JTF commander's prioritized defended assets. End state for this phase of the operation is as follows.

(a) JFLC and coalition partners reduce the insurgent threat to a level civil authorities are able to manage. The remaining paramilitary forces are defeated and the oil pipeline and production facilities are intact. Local security missions are being transferred to coalition units.

(b) JFLC defeats remaining paramilitary forces operating in the vicinity of the LOCs, and the LOCs are secure.

(c) JFACC continues intratheater lift operations as required and begins the transition to coalition and civil operations and control.

(d) The legitimate government of A-Land is intact and fully functional.

(e) Heavy BCT and two combined arms battalions continue operations against insurgent elements.

(2) The NTS capabilities available during previous operational phases continue to support stability operations. They are as follows.

(a) NTS capabilities continue to support integrated operational forces operating against insurgent cells. NTS enables the sharing of intelligence, including live, full-motion video, to counter insurgent activities.

(b) Static command posts and support organizations begin the transition to commercial terrestrial communications capabilities to reduce load on space platforms.

(c) NTS capabilities extend network support to interagency elements and NGO.

h. Distributed maneuver support and sustainment (see fig 4-9). Distributed maneuver support and sustainment are integrated throughout all phases of future Modular Force operations. Collectively, these capabilities provide a significant portion of the backbone and infrastructure enabling the success of the force.

(1) Integrated maneuver shapes the operational environment and combines a variety of functional capabilities such as military police; engineers; aviation; and chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) to understand the operational environment, enable theater access, provide assured mobility, deny enemy freedom of action., enable force protection and security, engage and control populations, and neutralize hazards and restore the environment.

(2) Maneuver sustainment focuses on the continuous, precise, and assured provisioning of deployed Army and other supported Service forces. To achieve this, sustainment must flow through a fully integrated national-to-theater-to-tactical distribution system. Continuous sustainment presumes global resource management and depends on a unified joint theater and global logistics C2 structure.

(3) The JFLC conducts decisive operations with two divisions employing a combination of non-FCS and FCS BCTs. Although one division is designated the main effort, maneuver support and sustainment forces play significant roles in shaping and controlling the operational environment while ensuring the continuous sustainment of the force.

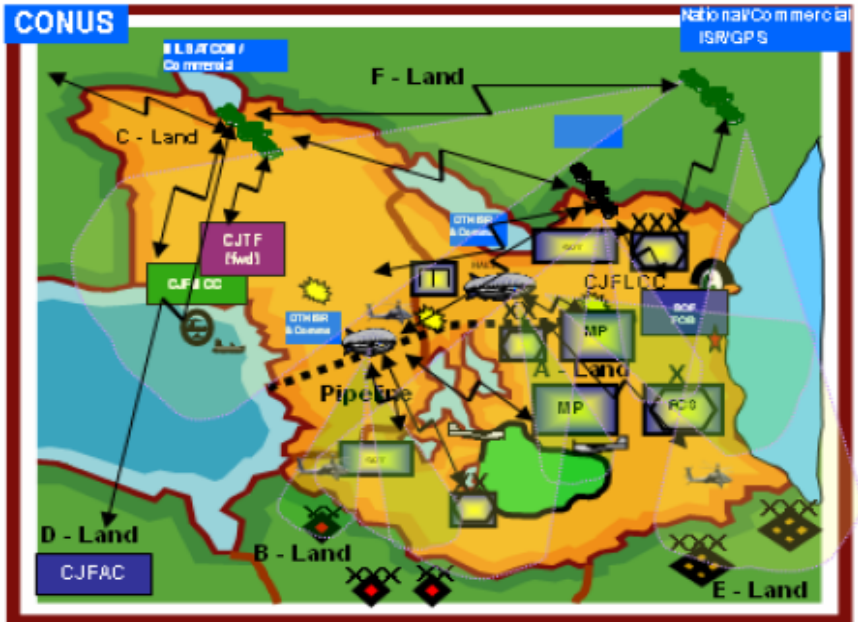

Figure 4-9. Distributed Maneuver Support and Sustainment

(a) Military Police units conduct maneuver and mobility operations supporting river crossings and route reconnaissance, conduct law enforcement activities, establish facilities for the confinement of enemy prisoners of war, and assist with population control.

(b) Engineer units enhance operational movement and maneuver by clearing and maintaining main supply route, construct bridges, and conducting de-mining operations. Engineers construct and harden base camp facilities and assist in repairing key components of the infrastructure.

(c) Aviation units coordinate and execute attack operations, conduct reconnaissance, air assault, aerial medical evacuation operations, and provide air traffic control services throughout the JOA.

(d) Chemical, biological, radiological, and nuclear (CBRN) units conduct surveillance and detection operations to identify traditional and non-traditional CBRN agent contamination. In addition, they identify and assess toxic industrial materials and toxic industrial chemicals found in the JOA.

(e) Logistics units and centers monitor unit readiness status and push tailored packages directly to consumers. Responsive replenishment and repair organizations ensure the smallest feasible deployed presence by leveraging theater and strategic logistics C2 structures.

(f) NTS capabilities are refocused and reprioritized toward more comprehensive support of theater support forces and their mission requirements. Theater signal assets are adjusted and reallocated upon completion of the decisive operations phase to enhance and fully enable planning, integration of coalition, multinational, interagency, and NGO activities with U.S. forces in preparation for the complex and wide ranging requirements of stability operations.

(4) NTS capabilities available during earlier phases of the operation are also required for maneuver support and sustainment operations. These are as follows.

(a) NTS enables commodity managers to monitor consumption across the force and direct sustainment distribution operations from national sources to theater distribution points to tactical units.

(b) In support of military police operations, NTS provides access to intelligence sources, including data bases of known terrorist and criminal organizations, enabling use of automated identification capabilities. In addition, NTS supports criminal analysis and forensic investigation through links to capabilities in the Office of the Provost Marshal General and Criminal Investigation Command.

(c) NTS capabilities enable Engineer units operating across the AO to maintain situational awareness as they maintain lines of communication. NTS permits rapid distribution of updated mapping information. Monitoring systems connected by the network to engineer Command Posts enable remote access to critical infrastructure status information. In addition, NTS supports tele-engineering.

(d) Networked intelligence resources provide critical situational information to support aviation operations.

(e) NTS capabilities provide access to information sources and national capabilities supporting CBRNE operations.

i. Network-enabled battle command (see fig 4-10). Network-enabled battle command is the keystone of future Modular Force operations. Battle command is a combination of science and art, with the commander at the focal point of decisionmaking and execution of combat operations. Battle command requires an integrated view of the operational environment that combines knowledge of self, information about the environment, and information about the enemy in order to plan, decide, and execute operations.

(1) NTS capabilities provide the critical network and information services infrastructure that ties all components of the integrated operational force together. NTS capabilities allow ready access to and sharing of information from and between national, component, and multi-national partners.

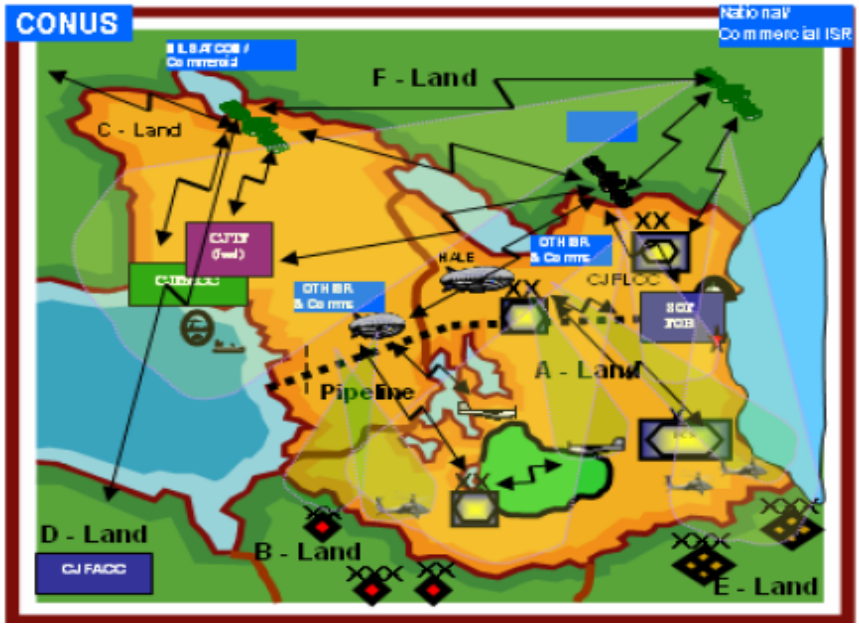

Figure 4-10. Network-enabled Battle Command

(2) Battle command enabled by NTS capabilities serves as the central nervous system of the future Modular Force. As forces flow into the JOA, the network expands and flexes to enable both inter- and intratheater flow of information. NTS capabilities allow commanders to draw from other commanders, joint resources, and home stations, and to leverage the capabilities of both live and virtual staffs. To enable a ubiquitous future Modular Force network, a layering of platforms, sensors, processors, and relays is required. These resources enable key portions of the operation such as initial ISR operations, planning and executing shaping and entry operations with the associated en route updates, plan alterations, and rehearsals. As forces flow into the JOA, demands on NTS capabilities grow, and NTS capabilities adjust to meet the demand.

4-3. Summary

a. The success of the future Modular Force will depend on NTS capabilities. The Army's dependence on the NTS facilities, personnel, organizations, and systems that bring the power of the Network to the warfighter cannot be overstated. NTS capabilities are fundamental and essential components of future Modular Force operations. Viewed in the larger construct of joint operations, Army NTS capabilities are keys to successful transformation and exploitation of the information domain.

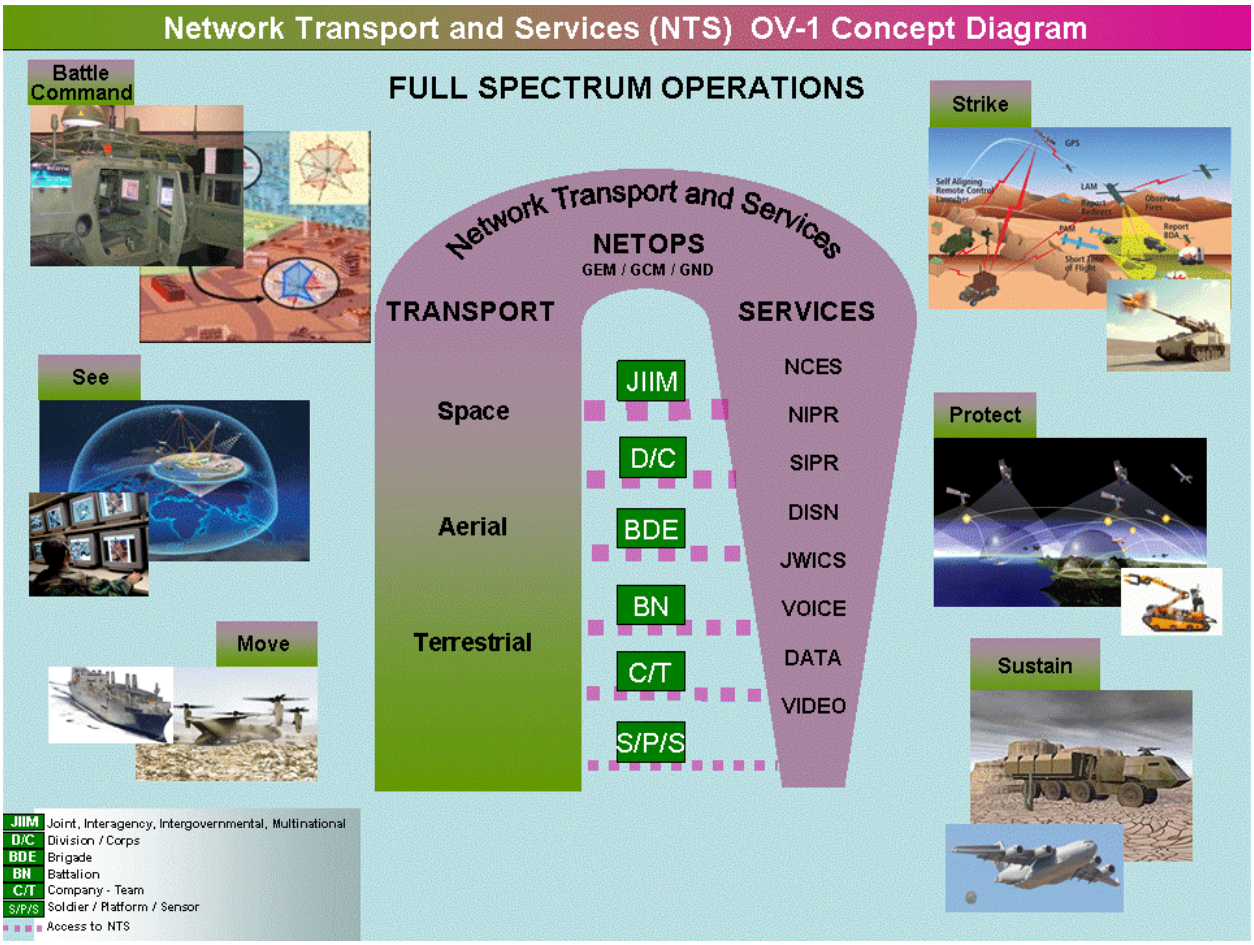

Figure 4-11. Operational View-1 Concept Diagram

b. NTS capabilities described in this CCP are part of a multitiered construct that combines advanced communications and network management technologies with the expertise, skills, and capabilities of network professionals at theater, corps, division, brigade, and battalion levels. These systems and people combined with globally positioned NTS capabilities that provide access to network services, to space communications assets, and to robust and responsive aerial and terrestrial communications layers, form the "always on" global network that enables the future Modular Force.

c. As shown in figure 4-11, NETOPS serves as the key enabler of the multi-tiered network transport and network services capabilities. NETOPS involves the functions, tasks, activities, technology, and policies that ensure the defense of the network and its components (through GND), assured availability and access to information resources and notification when new information is available (through GCM). It also involves end-to-end SA of the health of the network and the ability to diagnose and respond to issues or problems with the network based on this SA (through GEM). The transport section depicts integrated space, aerial, and terrestrial mechanisms that provides access from Soldier and sensor through joint and strategic levels. Network services are tailored to meet the needs, profile, and limitations of the user, whether it is human or machine. Combined, these elements create the network environment that relies more heavily on access than point-to-point connectivity. This access-driven environment creates the

ability to provide the pervasive Network that will enable the full integration of network-enabled C2, joint fires, joint lift, sustainment, targeting, and intelligence functions.

Chapter 5
Required Capabilities

5-1. Introduction

a. The Army's functional concepts provide explicit and implicit descriptions of the NTS-enabled functions necessary to achieve the objective state of the future Modular Force. These capabilities are integral components of a larger capability goal. The influence of a single NTS enabler is not confined to a single functional concept but will typically enable or affect several or all of the functional concepts and multiple proponent areas of responsibility. Because of this, when NTS capabilities are applied simultaneously they have the potential to deliver benefits no commander or military force has ever enjoyed.

b. These NTS capabilities should be viewed as optimum capabilities necessary to meet the requirements of the Army functional concepts during the 2015 - 2024 period. The listing is not all-inclusive, and will be further refined and developed as the Army NTS concept emerges and the JCIDS analysis is executed. Technological and threat advances may also drive changes to the listed NTS-related capability requirements.

c. These capabilities are required by elements from Soldier, platform, and sensor level to corps and JTF and ASCC and theater Army levels unless otherwise stated.

5-2. Battle Command Network Transport and Services Capabilities

a. TRADOC Pam 525-3-3, the *Battle Command* functional concept provides a visualization of how Army future Modular Force commanders will exercise command and control of operations in a unified action environment. The battle command function is a blend of the cognitive and the technical. Central to the technical component is the concept of a single, integrated Army battle command system enabled by an agile, ubiquitous communications network. Battle command is achieved by combining the art of well prepared leaders with the enabling science and technical systems of the future Modular Force.

b. All of the key ideas within TRADOC Pam 525-3-3 relate to or are enabled by NTS capabilities. The key ideas include collaborative planning; accelerated military decisionmaking process; information and decision superiority; single, integrated Army battle command system; interagency and multinational interoperability and integration; horizontal and vertical fusion; and an agile, ubiquitous communications network from space to mud.

c. Capability statement. Achievement of the capabilities described in the battle command functional concept will require the integration of a wide range of DOTMLPF factors. NTS must enable the future Modular Force to conduct battle command functions while stationary and

mobile (OTM or en-route), mounted or dismounted, in any terrain, under all environments and conditions to do the following.

(1) Provide real-time pervasive, extended range, inter- and intratheater global beyond line of sight (BLOS) communications relay and broadcast services between noncontiguous forces.

(2) Facilitate user connection to the network and access to services with minimal user system configuration or reconfiguration.

(3) Transport data, voice, and imagery to meet required quality of service and speed of service.

(4) Transport live full-motion video to meet required quality of service and speed of service.

(5) Provide access to net-centric enterprise services.

(6) Enable sharing of information across classification domains based on user and system profile.

(7) Move information of all classification levels across a common transport medium.

(8) Establish and maintain space, aerial, and terrestrial communication links dynamically that enable the fusion, sharing, publishing, subscribing, and updating of information from a wide variety of sensors and sources in all mission areas and classification domains.

(9) Provide access to a wide variety of sensors and sources simultaneously from multiple noncontiguous locations in order to provide timely, actionable, and relevant information in support of the planning, execution and assessment operations of the joint force and component commanders.

(10) Enable visibility of units' locations and combat readiness based on commander's priorities.

(11) Execute NETOPS functions.

(12) Enable users to access mission essential information outside DOD.

(13) Enable the dynamic allocation of frequencies during maneuver

(14) Operate unhindered by the presence of jamming and countermeasures.

(15) Provide transport for airspace C2 and airspace management.

(16) Protect the integrity of information while in transit and in storage.

(17) Connect battle command training enablers that allow integrated vertical and horizontal training, modeling and simulation, and reach.

(18) Establish and reconfigure the network and associated transport services to meet operational requirements.

(19) Manage all information network components centrally from remote locations.

(20) Enable network planners at all echelons to employ collaboratively network simulation tools that will measure network loading and the affect on network service provisioning.

5-3. See Network Transport and Services Capabilities

a. TRADOC Pam 525-2-1, the *See* concept describes how the future Modular Force will acquire and generate knowledge of itself, its opponent, and the operational environment. Without the ability to see, the Army is incapable of seeing first, understanding first, acting first, and finishing decisively.

b. Capability statement. Achievement of the capabilities described in the see functional concept will require the integration of a wide range of DOTMLPF factors. NTS must enable the future Modular Force to conduct see functions while stationary and mobile (on-the-move or en-route), mounted or dismounted, in any terrain, under all environments and conditions to do the following.

(1) Enable intelligence reach, which includes proactively and rapidly accessing information from, receiving support from, and conducting direct collaboration and information sharing with other units and agencies, both deployed in theater and outside the theater unconstrained by geographic proximity, echelon, or command. Intelligence reach requires enabling a unit to obtain the information or intelligence directly from the source without necessarily involving organizational echelons that may normally be involved.

(2) Protect the integrity of information while in transit and in storage in all operational environments and conditions.

5-4. Move Network Transport and Services Capabilities

a. TRADOC Pam 525-3-6, the *Move* concept focuses on strategic force projection and operational agility in support of joint campaign objectives. Operational maneuver from strategic distances, and achievement of the deploy-equals-employ paradigm are heavily reliant on accurate and timely situational awareness, global connectivity to information sources, and the ability to execute en route mission planning and rehearsal.

b. Capability statement. Achievement of the capabilities described in the move functional concept will require the integration of a wide range of DOTMLPF factors. NTS must enable the future Modular Force to conduct move functions while stationary and mobile (OTM or en-route),

mounted or dismounted, in any terrain, under all environments and conditions to do the following.

(1) Provide continuous information flow to enable SA, collaboration, mission planning and rehearsal for forces en route to an operation.

(2) Provide on-demand access to enable changing priorities and maintain deployment momentum.

(3) Access and disseminate time sensitive mission critical joint operational planning and execution information to meet operational requirements.

(4) Provide continuous in-transit visibility of logistics assets.

5-5. Strike Network Transport and Services Capabilities

a. TRADOC Pam 525-3-4, the *Strike* concept addresses future Modular Force fires and effects at the strategic, operational, and tactical levels. The concept explicitly describes a network that enables, "…joint C2 and joint intelligence, surveillance, and reconnaissance networks, using the CIE…" as a required capability. This capability provides near real time situational awareness, enables precision strike operations, and supports both lethal and nonlethal effects.

b. Capability statement. Achievement of the capabilities described in the strike functional concept will require the integration of a wide range of DOTMLPF factors. NTS must enable the future Modular Force to conduct strike functions while stationary and mobile (OTM or en-route), mounted or dismounted, in any terrain, under all environments and conditions to do the following.

(1) Access full spectrum of targeting information resources at all levels of command in support of strike operations, to include information supporting C2, ISR, and SA functions and processes.

(2) Provide a continuous collaborative information environment to support strike operations.

(3) Enable ISR and control data links that provide weather and meteorological information, terrain, and infrastructure updates to include imagery support for en route mission planning and rehearsal, and enemy situation updates.

5-6. Protect Network Transport and Services Capabilities

a. TRADOC Pam 525-3-5, the *Protect* concept describes how the future Modular Force will protect people, physical assets, and information against the full spectrum of threats. This concept also describes the function of protect NTS capabilities. The *Protect* concept's seven

enabling tasks—detect, assess, warn, prevent, deter, defend, and respond—are facilitated by NTS capabilities.

b. Capability statement. Achievement of the capabilities described in the *Protect* concept will require the integration of a wide range of DOTMLPF factors. NTS must enable the future Modular Force to conduct protect functions while stationary and mobile (OTM or en-route), mounted or dismounted, in any terrain, under all environments and conditions to do the following.

(1) Deter, warn, and if necessary, defend against enemy attack of NTS components; assure hostile forces cannot prevent friendly use of NTS components; ensure U.S. and allied forces ability to conduct NTS-enabled military activities.

(2) Plan and execute NTS COOP.

(3) Provide dedicated, persistent, and redundant NTS support for the protect functions (detect, assess, warn, prevent, deter, defend, and respond).

(4) Protect NTS components from deliberate or accidental interference

(5) Detect, deny, and counter adversary attempts to disrupt and exploit friendly NTS components.

5-7. Sustain Network Transport and Services Capabilities

a. TRADOC Pam 525-4-1, the *Sustain* concept describes future Modular Force logistics as a single, coherent system that senses and interprets the operational environment and responds through network capabilities. The ability to execute a logistics system from the source of support—generally CONUS—to the point of effect—generally an organization deployed in an operational theater—is heavily dependent on NTS capabilities.

b. Capability statement. Achievement of the capabilities described in the *Sustain* concept will require the integration of a wide range of DOTMLPF factors. NTS must enable the future Modular Force to conduct sustain functions while stationary and mobile (OTM or en-route), mounted or dismounted, in any terrain, under all environments and conditions to do the following.

(1) Transmit data concerning position, operational status, equipment or aircraft conditions, and maintenance diagnostics and prognostics anywhere in the JOA.

(2) Maintain in-transit and asset visibility of all supporting sustainment activities, supplies, and services.

(3) Support advanced data mining tools and decision support systems so that logistics staff elements can analyze and develop courses of action to support the maneuver commander's intent in synch with the maneuver commander's decision cycle.

(4) Establish a secure, pervasive, sustainment C2 and information infrastructure emphasizing speed, precision, accuracy, visibility, and centralized management to include sustainment requirements, distribution management, connection to industry and knowledge centers, passive radio frequency identification tags, Soldier health status, mortuary affairs, petroleum, and fuel supply. Support of a logistics COP, proactive and anticipatory maintenance, munitions, water, and logistics preparation of the battlefield.

(5) Provide continuous transport of SA data in support of convoy operations, including route reconnaissance information and convoy monitoring.

(6) Provide on-demand access to enable logistics (such as, medical logistics applications, logistics status updates, and others).

(7) Access distributed training capabilities.

(8) Enable remote modification of system software.

Chapter 6
DOTMLPF Implications and Questions

6-1. Introduction

a. The Army is pursuing the most comprehensive transformation of its forces since the early years of World War II. This transformation is happening while the nation is at war. The urgency of supporting the current fight blurs what would usually be a clear distinction between the current force and a future force. The Army seeks to accelerate incorporation of select future Modular Force capabilities into the current Modular Force to support today's fight, while simultaneously ensuring today's lessons are applied to future Modular Force developments.

b. This transformation encompasses more than materiel systems. Adaptive and determined leadership, innovative concept development and experimentation, and lessons learned during recent operations produce corresponding changes in the DOTMLPF domains. Experimentation, war games, and experience are the methods the Army uses to mitigate risk while considering and improving capabilities for the future Modular Force.

6-2. Past and Future Experimentation and War Games

TRADOC and its proponent schools have conducted extensive experimentation that has implications on the NTS CCP. Major experiments and war games conducted over the last two years involving NTS support include TRADOC Omni Fusion experimentation to include Omni Fusion Builds 0, I, II, and the Omni Fusion Build II integrating experiment; unit of action-focused experiments and events on unit of action FCS brigade operations; and the Army and Joint Forces Command Title X Transformation War Game Unified Quest 2006, 2007. They also include Air Force experimentation and wargaming conducted as part of the bi-annual Schriever war games; the Joint Forces Experiment 04 and 06; Schriever III; Thor's Hammer II; and LandWarNet I, II, and III.

6-3. Experimentation

a. Experimentation is the process of exploring innovative methods of operation to assess feasibility, evaluate utility, and determine limitations of the concepts being explored. Experiments conducted in support of JCIDS efforts use the 2015 - 2024 timeframe. The Army also conducts war games using futuristic scenarios (15 to 20 years in the future and beyond) to explore concepts in order to better define which of those concepts should be the subject of experimentation.

b. Army experimentation is usually conducted in the form of discovery (usually in a constructive modeling and simulation environment), hypothesis (also in a modeling and simulation environment, but with human-in-the-loop role players) and demonstration (live or simulated) settings.

(1) Discovery experiments are designed to inform a concept. The setting tends to lack the degree of control necessary to allow a reasonable inference of cause and effect.

(2) Hypothesis testing experiments. Hypothesis testing experiments are the traditional type used by individuals to build, confirm and advance knowledge. This occurs by seeking to falsify specific hypotheses—usually described in "if…then" statements—or by discovering their limitations. In order to conduct hypothesis testing experiments, the experimenter creates a situation in which one or more factors of interest can be observed systematically under conditions that vary the values of factors thought to cause change in the factors of interest. As this occurs, other potentially relevant factors are held constant.

(3) Demonstration experiments are used to display knowledge, and the settings tend to be somewhat orchestrated. Often the Army uses this method to display prototypes of emerging technologies that are nearing maturity and may be considered for fielding to the force.

6-4. Modeling and Simulation

Models and simulations are often used to make an informed assessment. They are also used to support training and leader development. Scenarios or vignettes are built to look at one or more sets of conditions that will best help to evaluate hypotheses. However, the raw data is often not conclusive or requires reasoned review by seasoned subject matter experts to confirm the reliability of simulation or modeling outcomes.

6-5. Concept Development and Experimentation (CD&E)

a. CD&E is fundamentally a risk reduction activity. Failure to conduct effective CD&E significantly increases developmental risk for the future Modular Force and operational risk to the current force. Specific actions are required to reduce operational risk to the current force and developmental risk for the future Modular Force.

(1) Operational risk to the current force. Increase the capabilities of the current Modular Force through prototype experiments that test the compelling solutions and develop DOTMLPF

capability packages to support the early introduction of future Modular Force capabilities to satisfy critical current force operational needs.

(2) Developmental risk for the future Modular Force. Reduce future Modular Force developmental risk by developing concepts and capabilities that meet the needs of the future joint force commander through rigorous concept development and experimentation.

b. Army efforts. Army war games and experimentation to support this CCP for NTS operations and their impact on DOTMLPF factors will be developed and studied using approved defense planning scenarios and vignettes. If required, other scenarios and vignettes may be recommended or other methods found to evaluate aspects of NTS capabilities. Experimentation will help define how the required capabilities described in chapter 5 of this CCP can best be achieved.

c. Joint efforts. Joint war games and experimentation will support this CCP. Active participation in other Service and joint events is critical to the full assessment of the Army's DOTMLPF solution sets. Army signal organizations and NTS operations will be tested, evaluated and modified as conditions (for example, scenario, vignette) change during experimentation. Scenarios and vignettes selected for experimentation will provide an illustration of how Army signal organizations and NTS capabilities will support full-spectrum operations throughout the deployment cycle.

6-6. Wargaming

Wargaming is a process of discovery and assessment. Wargaming develops insights into the impact of NTS capabilities and aids in assessing the validity of strategic visions and emerging concepts while looking 20 to 30 years into the future. War games stimulate training. Wargaming begins by attaining operational research on future warfighting systems and concepts and applying them to simulated military operations in order to prove or disprove visionary ideas and to discover gaps and seams in future Army NTS operations. Wargaming examines Army functional concepts of *Battle Command*, *See*, *Move*, *Strike*, *Protect*, and *Sustain*, and generates insights that inform experimentation and guide the development of NTS concepts, architectures, and systems that meet future Modular Force requirements. War game personnel lead participation in Army, joint, interagency, and multinational war games. They integrate NTS capabilities, concepts, and visions into war game scenarios, orders of battle, force lay-downs, and computer simulations.

6-7. DOTMLPF Questions

a. There are significant implications for the Army and for the joint community as the Army evolves NTS capabilities that will enable the net-centric environment envisioned for the future Modular Force. Interdependencies with DOD and joint forces associated with Army NTS capabilities will inevitably cause some study issues to transcend the Army's direct role; however, the Army is responsible for influencing the design and development of the range of DOTMLPF solutions for the joint force. We should examine specific NTS capabilities as the Army and the joint community move toward and embrace the net-centric operational environment.

b. The Army concepts used in the development of this CCP include a discussion of the implications of the concepts for DOTMLPF. In most cases, those implications relating to network transport and services are not explicit enough to generate action for change within the DOTMLPF domains by responsible proponents and agencies. The primary implications arising from the NTS CCP appear below. However, many of the items cited below will require additional analysis before comprehensive actionable recommendations emerge.

(1) How do NTS capabilities empower the Army to conduct net-centric operations in an integrated operations environment across the full spectrum of military operations?

(2) What are the impacts of national rules of engagement, policies, and laws on the employment of Army NTS capabilities?

(3) How does the Army manage and exploit the full range of NTS capabilities to ensure the Army can conduct operations to defeat the enemy without degrading or defeating its own capabilities?

(4) What are the limits to NTS interdependence among branch and Service functions?

c. Doctrine

(1) Emerging doctrine will focus on the necessary capabilities to engage adversaries across full-spectrum operations with a joint force that shares common systems; tactics, techniques, and procedures (TTP); and doctrine. TRADOC Pam 525-3-0 is compatible with Army doctrine contained in Field Manual (FM) 1, *The Army* and FM 3-0, *Operations*, but necessarily extends beyond current doctrine, describing new ways and means of conducting future operations. Army and joint doctrine must keep pace with new operational methods validated and introduced into the force in the form of organizational changes and new capabilities. The Army system of doctrine production and dissemination must become more responsive. For example, emerging doctrine can be captured using a special text that will be staffed and updated to FMIs and FMs as the concepts are matured. The degree of modularity envisioned requires doctrine that is more synergistic and adaptive.

(2) Doctrine principles provide an authoritative guide for leaders and Soldiers, but still provide freedom to adapt to circumstances. The evolution of organizations is driven by concepts and applied through doctrine. New NTS doctrine and TTPs will be required to effectively plan and manage battles in the net-centric operating environment envisioned for the future Modular Force. Doctrine questions include, but are not limited to, the following.

(a) How will evolving NTS doctrine affect units and leaders?

(b) How does joint NTS doctrine influence the conduct of Army NTS operations?

(c) Is joint NTS doctrine adequate for full-spectrum operations?

(d) Does joint doctrine adequately address interdependence of the services in the area of NTS functions?

(e) Is Army NTS doctrine adequate for full-spectrum operations?

(f) What are the impacts of international law on joint and Army NTS doctrine?

(g) How do national rules of engagement, policies, and laws influence Army NTS doctrine?

(h) Are NTS functions adequately addressed in Army theater, corps, and division doctrinal publications?

(i) Are TTPs adequate to execute Army NTS functions in full-spectrum operations?

(j) How will Army functional proponent doctrinal publications address Army NTS capabilities?

(k) What emerging NTS technologies, processes, and capabilities need to be codified in Army doctrine?

d. Organization

(1) The future Modular Force will support future operations with organizations that are modular, scalable, and capable of being tailored for the mission with multifunctional capabilities. These forces must be versatile and agile to blend seamlessly into joint operations, and must possess capabilities to adequately support the operations of maneuver and support forces. Joint mutual support becomes a key factor in determining Service roles and missions, and mission context will determine the apportionment of Army headquarters and forces. The range of missions assigned to Army forces will force an alignment change from the traditional command echelons. The Army will support combatant commanders with the command structure appropriate for land operations.

(2) The rank of the commander and the functions of the HQ will not necessarily correspond to the numbers of forces assigned to it. In many operations, the number and composition of subordinate units will differ dramatically. As each operation unfolds, the makeup of the deployed Army force will evolve, shifting in composition as the mission and circumstances dictate. While units may align with a HQ for training and readiness, actual operational groupings will be based on mission requirements. Organizational questions include, but are not limited to, the following:

(a) What NTS capabilities are required to be organic to operational units (C2, maneuver, fire and effects, operational support and force sustainment)?

(b) What NTS capabilities are better provided from the force pool of Army signal and network organizations based on effectiveness and efficiencies?

(c) What are the second and third order affects of pushing network capabilities down to lower levels in terms of network management and sustainment requirements?

(d) Is the current organization of theater signal assets (Signal command (theater)), tactical signal brigades, and ESBs) properly organized and equipped to meet the NTS capability requirements of the units in the theater force pool?

(e) To what extent do theater signal assets contribute to the NTS tiered network? Specifically, do theater signal assets need to integrate aerial platforms to enable full utilization of the aerial network transport tier for theater force pool units and rear areas?

e. Training

(1) Training requirements must be considered to complete the full cycle of the ARFORGEN process. Active component units are training for operations 50-66 percent of the time at home station. The Army must provide the capability to network training enablers from the Battle Command Training Course to all organizations on installation training enablers and to other installations to provide a training network that meets the requirements of the (live virtual constructive (LVC) integrating architecture.

(2) Changes in NTS capabilities will drive changes to our training. Training ensures that the future Modular Force is able to conduct the operations envisioned in joint and Army concepts. By embedding NTS capabilities and effects into future Modular Force training, commanders and leaders understand the impact of applied NTS and the power of the net-centric operating environment. Training simulations that include virtual NTS capabilities and NTS planning and assessment will improve our performance in the areas of battle command, operational environment awareness, force application, strike operations, protection, and sustainment.

(3) Army training must be flexible enough to incorporate new technology-based capabilities as they mature and become available. The Army must develop Soldiers and leaders who possess a joint and expeditionary mindset and who are able to optimize the NTS capabilities available to them across all echelons and proponents. Training questions include, but are not limited to the following.

(a) How is the application of NTS capabilities integrated in training and leader development?

(b) How can the Army adapt its training to better integrate NTS capabilities into Army full-spectrum operations?

(c) How will evolving technologies and ongoing or planned changes in organization affect the ways in which Army units and leaders operate, and how will these operational changes affect the training of Army NTS operations?

(d) What training designs will develop units and leaders able to capitalize on the full range of NTS capabilities?

(e) What are the NTS operations training requirements for enlisted personnel, noncommissioned officers, officers, contractors and DA civilians?

(f) What type, scope, and frequency of Army NTS operations training must the future Modular Force conduct to achieve and sustain effective operations?

(g) What simulation capabilities are required to support Army NTS training at the institutional, tactical, operational, and strategic levels?

(h) How can NTS capabilities be leveraged to enhance training and leader development?

(i) How will NTS capabilities improve the ability of Army forces to train for future conflicts?

(j) Will NTS capabilities facilitate realistic training in conjunction with other services and government agencies, both U.S. and multinational?

(k) What are the training requirements and what capabilities can be provided to enhance the integration of theater signal support units, specifically ESBs, with theater force pool units they will be tasked to support upon notification of mobilization and deployment? Additionally, how are the Active Reserve components ESBs integrated in this training program?

f. Materiel

(1) Resources are always limited, and the joint interdependence of NTS operations makes the selection and development of NTS materiel demanding and difficult. Modernization and sustainment ensure that baseline capabilities are maintained and future Modular Force capabilities are pursued. Realization of the Army NTS concept depends on the development and incorporation of advanced technologies that will enable NTS capabilities that, in turn, will provide the net-centric operating environment envisioned for the future Modular Force across the full spectrum of military operations.

(2) The development of NTS-related materiel solutions must proceed along a top-down, joint-driven path. Materiel questions include, but are not limited to the following.

(a) What NTS capabilities are required to support rapid connection of user systems to the network (plug and play)?

(b) What NTS capabilities are required to support the expanding presence of sensor systems and platforms on the battlefield?

(c) What are the maintenance impacts of NTS systems?

(d) How will terrestrial, aerial, and satellite systems enable a net-centric operating environment for multi-echelon and multidimensional ISR, fires, maneuver, and logistics?

(e) How will terrestrial, aerial, and satellite systems be integrated into a seamless network transport system of systems that provides a net-centric operating environment?

(f) How will terrestrial, aerial, and space-based systems enable dominant SU?

(g) How will terrestrial, aerial, and space-based systems contribute to the establishment of a single, integrated, network-enabled joint battle command system?

(h) What terrestrial, aerial, and satellite systems are required to support the expanding presence of unmanned systems on the battlefield?

(i) What terrestrial, aerial, and space-enabled sensor-to-shooter linkages are needed to support future Modular Force in full-spectrum operations?

(j) How will common data link (CDL) capability be integrated into NTS?

(k) What MILSATCOM systems are needed to enable NTS for the future Modular Force?

(l) What commercial SATCOM assets are needed to enable NTS for future Modular Force?

(m) What aerial layer systems are necessary to enable NTS to support future Modular Force operations?

(n) What ground terminal systems are needed to enable space and aerial capabilities?

g. Leadership and Education

(1) One of the keys to enabling effective Army operations will be the development of leaders and staffs that can perform effectively across the full spectrum of military operations in a complex, uncertain, and dynamic operational environment. Leaders must be educated, trained, and developed to be self-aware, innovative, and adaptive throughout training and operations. In the area of NTS operations, leaders must think strategically as well as tactically, possess a joint and expeditionary mindset, and successfully apply the joint and Army aspects of the net-centric operating environment enabled through NTS.

(2) Leaders also will need integrated operations education and experience early in their careers. Doctrine will provide an operational foundation. Educational opportunities will provide intellectual growth that will prepare leaders for the unified action-oriented, net-centric operating environment enabled by NTS capabilities. Leader development questions include, but are not limited to the following

(a) How can the Army develop adaptive theater Army, corps, division, brigade, and battalion leaders who understand NTS-enabled capabilities?

(b) How does the Army provide world-class leader development in the area of NTS operations in a joint and multinational construct?

(c) How does the Army prepare leaders to deal with the complexity of NTS, the associated net-centric operating environment, threats, and interagency implications?

(d) What NTS-related leader development programs are needed in the non-commissioned officer education system, the warrant officer education system, and the officer education system?

(e) What civilian leader development programs are needed?

h. Personnel

(1) Soldiers are the Army's greatest resource and the most important factor in achieving and maintaining unit readiness. The integration of NTS capabilities into future Modular Force operations will increase the demands on an already stressed population. Selecting and assigning the right Soldiers to NTS-related positions and occupational specialties are difficult tasks. The personnel management system must provide the career paths needed to utilize fully the NTS expertise of the force. New organizational constructs may rely on experienced civilian personnel to provide the skills needed to support training readiness and global NTS operations.

(2) The right combinations of active and reserve component Soldiers, Army civilians, and contract personnel can only be determined through research and experimentation. Personnel questions relating to NTS operations include, but are not limited to the following.

(a) How does the Army recruit and retain the personnel (Soldiers and civilians) with the skills necessary to perform Army NTS functions?

(b) What skill sets are required by Army civilian and contract support personnel?

(c) What is the best means of selecting Army NTS officers, warrant officers, and non-commissioned officers?

(d) Should pre-commissioning programs include a component on NTS capabilities?

(e) What is the right mix of personnel between NTS professionals and other personnel selected to serve in NTS-related positions?

(f) How will NTS affect the signal military occupational specialty and additional skill identifier structure?

(g) How will NTS affect non-signal military occupational specialties?

(h) How will NTS affect Soldier security clearance requirements?

i. Facilities

(1) As the role of NTS in Army operations continues to grow, so does demand for a supportive facilities infrastructure. The joint nature of NTS operations will require secure communications facilities capable of supporting training and operations. These facilities will have varying capabilities to support training, force projection, reach, and knowledge access. Installation information facilities will enable units to train as they fight, and to share information among sustaining base organizations and deployed forces during all phases of operation.

(2) Prior to deployment, fixed facilities on the installation can collect, process, and analyze large volumes of data such as terrain databases. Installations will require suitable facilities for skilled civilian personnel supporting a military staff. NTS training ranges, test laboratories, and modeling and simulation facilities will be needed. Facilities questions include, but are not limited to the following.

(a) Are adequate facilities available to Soldiers, leaders, battle staffs, non-uniformed personnel, and units to attain and maintain acceptable levels of NTS operating and maintenance proficiency?

(b) What infrastructure is required at local, national, regional, and global locations to adequately support NTS operations in training, maintenance and operational constructs consistent with Army, joint, and multinational requirements?

(c) What infrastructure is required in a theater of operations to support Army NTS functions?

(d) What installation infrastructures are needed to support home station NTS functions?

(e) What NTS test and training facilities are necessary?

6-8. Plan for Assessment

a. Introduction. NTS capabilities are essential to successful future Modular Force operations. Currently, there are no U.S. Army documents that provide a concept for future NTS capabilities. This CCP is the first Army-specific document that attempts to provide a concept for future integrated NTS operations. The concepts referenced in the development of this document reflect the capabilities researched and the mission areas studied either prior to or during the formulation of this CCP.

b. Assessment Options

(1) Future CCP and JCIDS Efforts

(a) The intent of the NTS CCP is to provide a holistic view of the NTS capabilities required to enable the future Modular Force in full-spectrum operations. The integrated capabilities development team preparing this CCP consisted of 13 core members and 10 supporting members (listed in appendix B). Each of these proponents has or likely will develop its own concept or plan for how it will operate in the future. The number of proponents involved and the range of their proponent responsibilities indicate that the development of additional CCPs, which include NTS-enabled capabilities, is likely.

(b) The span of required capabilities identified in the CCP indicates the need for a CBA to determine if current and projected DOTMLPF solutions are adequate, identify capability gaps, and determine possible solutions to mitigate gaps.

(2) Network Representation and Scenario and Vignette Scope

(a) Network challenges generally revolve around two distinct groupings of users. Warfighters engaged in serious and relatively high intensity operations, placing a high demand on the network for voice, video, data, and imagery but with a significant capability in multiple communications means and options. Users whose initial requirements for network support center on pure connectivity, but grow over time and become as vital to the sustained operations of the force, as a whole, as the normal operations traffic of the former group. The challenge for the NTS CBA is to identify and select the most appropriate scenario and vignettes that can present these two groups of users at their most challenging size, geographical location and limitations, operational demands, and realistic mixture of blended U.S. component and coalition and multinational forces and communications capabilities, and interagency and non-governmental players.

(b) The question quickly centers on the MDMP-like issue of most likely versus most dangerous and challenging scenario choices. The larger the overall scenario and associated force structure, the more likely the following issues need to be handled.

- Multiple component units alerted and mobilized for deployment, bringing varied sets of modernized and capable signal equipment, from widely dispersed locations and commands.
- A theater support structure large enough to represent the full suite of capabilities and organizations required to deploy and support in a relatively austere host nation operational AO (units without organic signal support that tax force pooled theater signal support assets).
- Significant deployment timelines in which signal and network assets must compete for priority with combat and other vital support units. Sufficient host nation and even interim staging base considerations to enable complete and timely deployment of the force.
- A ROMO being conducted concurrently in the same theater, requiring varying network support capabilities (such as, humanitarian relief, displaced civilian control, stability operations, and outright combat operations, and others).
- Involvement and presence of U.S. and non-U.S. military forces, civilian and private agencies.

- Breadth and depth of joint forces supporting Army forces, or requiring Army support.
- Dispersion and geographic distribution, revealing the limitations of communications capabilities and requiring greater effort to assure communications of the force as a whole as well as the individual units.
- Greater impacts by environment on more widely dispersed forces in varying geographic locations.
- More opportunity and incidence of threat operations across the spectrum of threat capabilities.
- Complexity and network implementation and management challenges required of the larger and more complex force.
- Limitations of available communications systems and capabilities–available and leasable SATCOM, local phone networks, capacity of commercial cables and fiber, and others.

(c) The vignettes presented in this CCP are indicative only of the kinds of communications challenges faced in each of the operational phases. A scenario and vignettes associated with locations and forces that do not have a historical basis of U.S. operations (such as, Southwest Asia, Northeast Asia) would expose lack of capabilities if more austere, less established infrastructure and interoperability locations and forces were chosen. Much of the network support in current Northeast Asia and Southwest Asia is a combination of developed infrastructure (such as, cable and fiber, local host nation network, commercial leased or purchased equipment bought for and now operated by the host nation, transitional government, or even U.S. units). Distinguishing the pure military network requirements and capabilities becomes more complex (the forward operating base-centric complex).

(d) Scenarios and vignettes centered on South America, Africa, or Horn of Africa, or Southeast Asia and the Pacific offer more opportunity to examine the extreme lengths the U.S. would have to go to establish the future network envisioned in support of our forces. Further, a scenario of sufficient sized force structure, including one or more corps and JTFs, with one half or more of the U.S. combat and support force requiring deployment and network support, would enable the CBA to examine the challenges of scale and utilize the full suite of warfighting functions and U.S. joint and coalition support forces.

(3) Future experimentation, wargaming, and simulation. Experiments and war games will facilitate the exploration of required capabilities and answering questions that will further develop the ideas from this CCP and facilitate the CBA process. These include Unified Quest, and those programmed through the TRADOC 2008 Army Concept Development and Experimentation Program including Omni Fusion 08; ISR Warfighter 08. The recurring annual exercise; Earth Wind and Fire 08, Complex Web Defense simulation exercise; Air Assault Expeditionary Force; Coalition Radio Interoperability; the Air and Ground Distribution computer aided exercise; the Logistics C2 Seminar; Operational Movement from Strategic Distance; and the LandWarNet wargame.

Chapter 7
Risk and Mitigation

7-1. Introduction

This chapter examines potential risks associated with implementation of required NTS capabilities. It also considers possible risks related to alternatives, the most significant of which would be insufficient resourcing of required NTS capabilities. These risks expand on risks described in the earlier discussion of the operational environment (chapter 3), and are grouped into three categories: operational risk, expectation risk, and adversary action risk. In each case, the potential for mitigation is included.

7-2. Operational Risk

a. Failure to provide required NTS capabilities will restrict the ability of the future Modular Force to execute warfighting functions, limit the utility of information systems (including battle command), constrain the sharing of critical information, limit collaboration, etc. This will affect all aspects of operations, including mission preparation during the ARFORGEN process, C2 of forces en route to the AO, speed of maneuver and operational agility, achievement of decision superiority, and sustainment at every level. This will require changes in warfighting doctrine and training, may drive increases in force structure to accommodate manual performance of tasks, and will generally force a lower operational tempo than that envisioned for the future Modular Force. Mitigation: Revise warfighting doctrine to reflect capabilities compatible with reduced information exchange, limited collaboration, and slower decisionmaking; constrained maneuver over shorter distances; and limited on-the-move battle command.

b. The future Modular Force may become dependent on NTS capabilities to the point of being incapable of operating in a degraded network state. The ability of commanders and staffs to conduct effective operations with limited network services may diminish as network capabilities become more reliable and pervasive. Mitigation: The conduct of operations in a degraded network environment must be addressed in doctrine, trained in service schools, and exercised frequently.

7-3. Expectation Risk

a. Achieving required NTS capabilities may create an expectation that unlimited bandwidth will be available throughout an operation. Such an expectation could offset “appetite suppression” efforts, and lead to wasteful or trivial use of network assets. Mitigation: Training, supervision, and enforcement by commanders of network policies and standards are keys to ensuring sufficient bandwidth is always available to satisfy real operational requirements.

b. A related risk is the assumption that NTS capabilities eliminate the need to carefully engineer user applications to operate efficiently on the network. Such an assumption could lead to the acceptance of poorly crafted applications that require inordinately large amounts of network bandwidth to accomplish functions that could be achieved in more bandwidth-efficient ways. Mitigation: Include network efficiency and bandwidth utilization criteria in application

requirements documents; require network certification during the design of applications to ensure bandwidth efficiency parameters are incorporated.

7-4. Adversary Action Risk

a. The most significant risk associated with NTS capabilities is a security breach of the Network. While security features can be designed into NTS systems, poor compliance with and enforcement of security and IA procedures could allow an adversary to penetrate the network, halt, slow, or misdirect information flow, and/or alter information used in the decisionmaking process. All of these actions can have both immediate and long-term detrimental impacts on future Modular Force operations. Mitigation: Maximize reasonable security design in NTS systems; train and enforce IA policies and procedures.

b. Direct action may be taken by adversary elements against NTS capabilities. This may occur both within the AO and in areas that host NTS facilities outside the AO. Direct action may take the form of either physical attacks against facilities or people, or electronic attacks against NTS systems. Direct action may result in the complete or partial loss of NTS support to operational forces. Mitigation: Where operationally feasible, locate NTS capabilities in sanctuary; provide adequate physical security; include redundancy and continuity of operation plan as a key system and network design parameters.

Appendix A
References

Section I
Required Publications
(ARs, DA Pams, FMs, and DA forms are available at Army Publishing Directorate (APD) - Home Page. TRADOC publications and forms are available at TRADOC Publications. Joint Concepts are available at http://www.dtic.mil/futurejointwarfare/concepts)

Net-Centric Environment Joint Functional Concept

Net-Centric Operation Environment Joint Integration Concept

Net-Centric Enterprise Services Warfighter Concept of Operations (Available at https://www.us.army.mil/suite/doc/5895380)

TRADOC Pam 525-2-1
The U.S. Army Functional Concept for See 2015-2024.

TRADOC Pam 525-3-3
The U.S. Army Functional Concept for Battle Command 2015-2024.

Section II
Related Publications

Army Concept Capability Development Plan.

Army Concept Development and Experimentation Plan.

Army Strategic Planning Guidance.

Capstone Concept for Joint Operations.

Chairman Joint Chief of Staff Instruction (CJCSI) 3170.01B
Joint Capability Integration Development System Manual.

CJCSI 3170.01E
Joint Capability Integration Development System Instructions.

Chairman Joint Chief of Staff Manual (M 3500.04D
Universal Joint Task List.

DA Pamphlet 25-40
Army Publishing: Action Officers Guide.

Defense Information (DI)-1577-33-06
Information Operations Capstone Threat Assessment, (S//NF//20300804).

DI-2710-25-01
Information Operation Threat to Military Use of Commercial Satellite Communications, (S/NF//XI) Declassify X1, X3.

Defense Planning Guidance. (Available at http://www.defenselink.mil/dodcmsshare/briefingslide/138/020510-D-6570C-001.pdf.)

DOD-1574-0727-06
Space Capstone Threat Assessment (S//FGI//NF//MR).

FM 7-15
Army Universal Task List.

Future Combat System, System Threat Assessment Report, (S//NF).

Global Broadcast Service Operational Requirements Document.

Initial Capabilities Document for Department of Defense Transformational Communications.

Joint Publication 6-0
Joint Communications System.

Joint Publication 6-02
Joint Doctrine for Employment of Operational/Tactical Command, Control, Communications, and Computer Systems.

National Military Strategy. (Available at http://www.defenselink.mil/news/Mar2005/d20050318nms.pdf.)

National Security Strategy. (Available at http://www.whitehouse.gov/nsc/nss.html.)

NAIC (North American Industry Classification) -1574-0731-04
Electronic Warfare Threat Environment Description, (S//NF//MR).

NAIC-1574-0367-05
Military Satellite Communications System Threat Assessment Report, (S//NF//MR).

Office of Naval Intelligence-1573-001-03
Worldwide Foreign Information Operations Threats to U.S. Naval Systems, (S/NF).

The Joint Operational Environment-Into the Future White Paper.

The Joint Operational Environment "The World through 2030 and Beyond." United States Joint Forces Command.

TRADOC Pamphlet 525-3-0
The Army in Joint Operations: The Army Future Force Capstone Concept.

TRADOC Pam 525-3-1
The Army Operating Concept for Operational Maneuver 2015-2024.

TRADOC Pam 525-3-2
The Army Concept for Tactical Maneuver 2015-2024.

TRADOC Pam 525-3-4
The U.S. Army Functional Concept for Strike 2015-2024.

TRADOC Pam 525-3-5
The U.S. Army Functional Concept for Protect 2015-2024.

TRADOC Pam 525-3-6
The U.S. Army Functional Concept for Move 2015-2024.

TRADOC Pam 525-4-1
The U.S. Army Functional Concept for Sustain 2015-2024.

TRADOC Pam 525-5-600
LandWarNet Concept of Operations.

TRADOC Pam 525-7-4
Concept Capability Plan for Space Operations 2015-2024.

TRADOC Regulation 10-5
U.S. Army Training and Doctrine Command.

TRADOC Regulation 25-35
Preparing and Publishing U.S. Army Training and Doctrine Command Administrative Publications.

Appendix B
NTS CCP Integrated Concept Development Team Members

ICDT Chair:

Mr. Alton D. Morrison,
Deputy Chief, Concepts and Doctrine Branch (CDB); Concepts, Requirements, and Doctrine Division (CRDD); Capabilities Development and Integration; Directorate (CDID); U.S. Army Signal Center

Project Team:

Mr. Ron Higgins, Ms. Mona Strickland, Mr. Jeff Wells,
Concepts Section; CDB, CRDD, CDID, U.S. Army Signal Center

Core Members:

HQ TRADOC ARCIC
U.S. Army Space and Missile Defense Command
U.S. Army Maneuver Support Center
U.S. Army Combined Arms Support Command
U.S. Army Air Defense Artillery Center
U.S. Army Armor Center
U.S. Army Aviation Warfighting Center
U.S. Army Intelligence Center
U.S. Army Infantry School
U.S. Army Field Artillery School
U.S. Army Signal Center

Supporting Members:

Defense Information Systems Agency
Department of the Army: G-3 and G-6
U.S. Forces Command
U.S. Army Materiel Command (Communications and Electronic Life Cycle Management Command)
U.S. Army Special Operations Command
U.S. Army Combined Arms Center
U.S. Army Medical Department
U.S. Army Network Enterprise Technology Command/9th Signal Command (Army)

Appendix C
Bridging Current to Future Capabilities

C-1. Introduction

a. This appendix is provided as a tool and a starting point for the CBA study team. It provides a "snapshot in time" of current NTS capabilities, addresses the development of near- and mid-term future capabilities, and identifies potential NTS capabilities under development. The appendix identifies known gaps between current and mid-term NTS capabilities, and describes programmed NTS capabilities that address those gaps and may meet requirements outlined in the future Modular Force concepts. As stated, this is a start point for future JCIDS analysis.

b. NTS capabilities are essential to all Army functional concepts. The NTS capability descriptions in this chapter are common to all functional concepts and are organized along functional concept lines. Within those discussions the CCP expands on specific capabilities relating to leader-Soldier-sensor requirements; en route command and control; joint, coalition, interagency, and non-governmental functions; the aerial transport layer; battle command OTM; network operations; and full-motion real time video requirements.

c. Each functional category is viewed in three timeframes: current and near-term (2007 - 2009), mid-term (2010 - 2015) and far-term (2016 - 2024). Figure C-1, Capability Development Blocks, represents the incremental steps associated with enabling the future Modular Force's network with required NTS capabilities. These blocks are defined by the timeframes of the DOD program objective memorandum, and coincide with the incremental development schedule defined in the Warfighter Information Network-Tactical (WIN-T) Acquisition Decision Memorandum. Current and mid-term capabilities are based on the NTS capabilities integration map, the bridge to future networks (BFN) capabilities production document (CPD), the WIN-T capabilities development document, TRADOC Pam 525-5-600, and other approved program documents.

d. Bridging the gap between current and future NTS-enabled capabilities will be a complex task involving national and civil agencies, the joint community, and all Army proponent schools and centers. NTS required capabilities will be driven continually during the concept period by emerging technologies that influence warfighting functions and the reliance of those functions and supporting systems on NTS capabilities. The future capabilities described in this chapter and the associated solution components reflect a "best possible" scenario—the optimum NTS-enabling facilities, personnel, organizations, and materiel solutions considering the timeframe, the threat, and the ROMO.

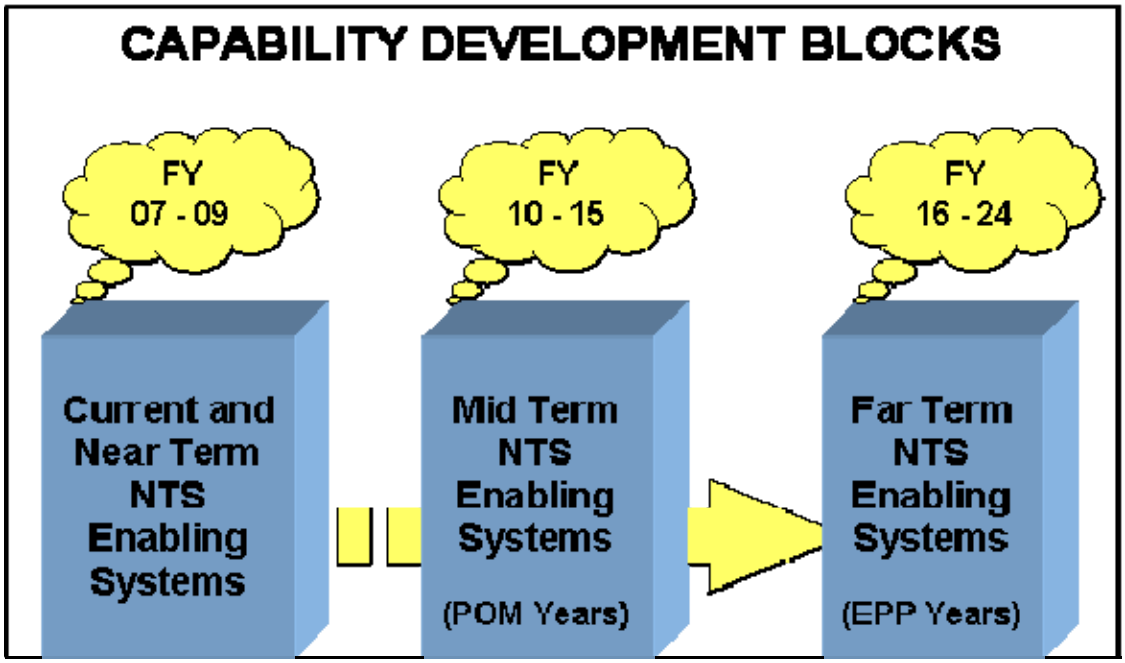

Figure C-1. Capability Development Blocks

C-2. Battle Command Related NTS Required Capabilities

a. Battle command encompasses a commander's need to continually address changing situations and missions by dynamically linking functions within and across the joint operation environment. Fundamental to meeting this need is a secure global communication and information infrastructure employing a robust set of systems, facilities, and organizations comprised of well-trained Soldiers. Table C-1 depicts the current, mid term, and far term NTS blocks that support the *Battle Command* concept.

b. Near and Mid Term Capabilities

(1) NTS capabilities supporting current force battle command functions consist of many related but often disparate solutions that cover a broad span of technologies. They include the mobile subscriber equipment (MSE) and tri-service tactical (TRI TAC) systems, joint network node (JNN) and command post node, and blue force tracking (BFT). They also include the TROJAN program's special purpose integrated remote intelligence terminal (SPIRIT), combat service support (CSS) very small aperture terminal (VSAT), medical network, PA network, and others. Several of these systems have emerged to provide a single-purpose or "stovepipe" communications capability to support a specific application. In addition, each system has brought its own unique management infrastructure. These unique management systems do not support emerging integrated NETOPS and OTM ad hoc networking constructs. Current networks rely heavily on commercial satellite, narrowband tactical satellite, and single-channel line-of-sight (LOS) radio systems. The Army does not have assured information pathways because these transport systems do not function as a single network, but instead operate independently with differing services and levels of service quality.

(2) The current force is being enhanced with commercial technologies to ensure operational relevance and interoperability with future capabilities. The ongoing infusion of COTS hardware, software, training, and elements of network management, information assurance, and information dissemination management capabilities into brigades, divisions, corps, warfighting platforms, strategic reachback sites, and Signal formations is designed to effectively and efficiently enhance warfighting capabilities. NETOPS will provide users at all levels with end-to-end connection and visibility of strategic, theater, operational, and tactical network management, IA, and information dissemination management (IDM) resources.

(3) Multiple advancements have been approved at joint and Army levels to facilitate the creation of communication and information networks for the near and mid-term NTS construct. The BFN CPD initially identified communications capabilities relevant to several TRADOC proponents that enabled the transforming Modular Force to begin employing internet protocols technology in BLOS communication systems, primarily the JNN. The BFN replaced the area common user system modernization plan and took advantage of existing and directed transmission capabilities to recapitalize the current MSE and TRI TAC systems. The WIN-T program has joint-approved requirements to provide Army warfighters with a state-of-the-art ground, aerial, and space layered information network that enables the exchange of all types of information (voice, data, and video) throughout tactical echelons and span across and connect the near-, mid-, far-term NTS networks. The WIN-T acquisition decision memorandum directs four increments (INCs) of the WIN-T program to account for evolution of warfighters' urgent network needs and allow maturation of the technologies to meet those needs. Technological and doctrinal changes will also require NETOPS functionality to enable a shared SA of the Network and the ability to employ technologies, procedures, and collaborative organizational structures to rapidly assess and respond to system and network degradations, outages, or changes in operational priorities. The INCs are defined below.

(a) INC 1. Networking at-the-halt. Increment 1a: former JNN program with military Ka satellite capability. Increment 1b: selected warfighting JNN-equipped brigades receive WIN-T BLOS SATCOM waveform (NCW) and migrate to WIN-T's security architecture.

(b) INC 2. Initial networking OTM–WIN-T NETOPS capabilities for division G-6 and brigade S-6; new LOS (ground-to-ground) and BLOS (ground-to-space) waveforms and transmission systems; new "colorless" (totally encrypted) security core.

(c) INC 3. Full networking OTM capabilities fielded broadly; NETOPS capabilities further integrated; supports FCS.

(d) INC 4. Addition of protected SATCOM OTM.

(4) Transport

(a) WIN-T will be the core transport and information networking capability that enables future Modular Force capabilities. WIN-T will provide communications transport capabilities across all Army warfighter echelons, enabling full spectrum operations in an integrated LandWarNet environment. WIN-T leverages seamless multi-tiered transport layers enabling

ground-to-ground, ground-to-air, air-to-ground, air-to-air, and space-to-ground communication paths. The Network will transport warfighting, intelligence, and business mission area information requirements, which negates the need for mission area-specific transport systems. Dynamic spectrum management and bandwidth allocation supporting these multi-tiered, integrated transport layers improves network connectivity and availability across all echelons, and allows the Network to flex in support of developing requirements. Transparent to the user, the Network will provide access via the most expeditious/available transport layer given requirements and established policies. Additionally, through WIN-T mobile Army forces will collaborate and access GIG resources (databases, knowledge centers, collectors, and national agencies) to exchange critical and timely information. Information systems will compete for the limited resources of spectrum, bandwidth, and network access. NETOPS provides the means to manage the infrastructure and provide assured system and network availability, information protection, and information delivery.

(b) Army units require the same joint connectivity whether in garrison or tactical locations. Operational commanders require access to joint and Army systems such as Global Command and Control System-Army (GCCS-A), Global Combat Support System-Army (GCSS-A), Joint Operation Planning and Execution System (JOPES), Army Battle Command System (ABCS), Force XXI Battle Command Brigade and Below, joint BFT, and other current information systems that rely on Internet protocol to interconnect across the AO and throughout the GIG. The network transport capabilities outlined in WIN-T facilitate the Army's JTF role with installation-based commercial capabilities plus the security and battle command OTM capabilities to meet tactical information requirements.

(c) Enterprise systems management and network management of the LandWarNet will assure effective and efficient availability of information systems, elements and services across all echelons and warfighting, intelligence and business domains. Dynamic spectrum management in turn will enable self-forming, self-healing connectivity to support fluid operations.

(d) WIN-T will enhance the staff planning process and the ability of commanders to execute operations. WIN-T will give warfighters joint communication services, such as Secret Internet Protocol Router Network, National Security Agency Network, NIPRNET, joint worldwide intelligence communications system, and Defense Red Switch Network whether they are in garrison, en route to an operation, or deployed. Network-enabled enterprise services will support dynamic collaboration and ad hoc task organization, with content discovery, delivery, and storage, providing automated access to relevant information in accordance with commanders' priorities.

(e) WIN-T will transport all classifications and types of information, and will replace MSE, and TRI TAC. It will replace the communications functionality of Trojan SPIRIT, CSS VSAT, and PA network employed at BCT and below, medical network, and interim mounted battle command OTM systems.

(f) The Joint Tactical Radio System (JTRS) will bring the voice and data network to brigade and below, mounted and dismounted, Soldiers by providing a networked, interoperable, LOS and BLOS, narrowband and wideband, voice and data tactical communications capability.

The JTRS lays the foundation for achieving network connectivity down to the individual Soldier at brigade and below. It provides the means for digital information exchanges, both vertically and horizontally, between joint war fighting elements, while enabling connectivity to civil, national authorities, and coalition forces as applicable. The JTRS will support joint missions by enabling network connectivity, network interoperability (both Internet protocol and legacy), sensor fusion, voice and data dissemination, cooperative position location information, and other multi-platform applications. JTRS will enable network-centric operations by providing narrowband and wideband tactical communications capability and seamless connectivity throughout air, ground, and space domains for the simultaneous command and control and exchange of ISR information.

(5) SATCOM. SATCOM systems available to the joint force provide the foundation for current space-based inter- and intratheater communication enablers. These systems are generally organized into five groups: protected (Milstar-(military strategic and tactical relay satellite), narrowband (ultra high frequency (UHF) fleet satellite or UHF follow-on (UFO)), wideband (Defense SATCOM System (DSCS)), GBS, and commercial SATCOM systems.

(a) Protected. Protected SATCOM provides the U.S. military's communications requirements with worldwide, anti-jam, scintillation resistant, low probability of detection communications services. Milstar meets the minimum essential command and control communications requirements of senior governmental leaders, strategic and tactical military forces. The first advanced extremely high frequency (AEHF) launch is scheduled for fiscal year (FY) 2008 and will provide five to eight times the current protected capacity.

(b) Narrowband. The UFO constellation is the primary source of UHF SATCOM. UFO is augmented by the aging fleet satellite system, a commercially owned and operated system the military leases for UHF SATCOM services. The UFO constellation is a Navy owned and operated system that provides worldwide operational communications for aircraft, ships, submarines, and ground stations. The Mobile User Objective System (MUOS), a next-generation narrowband tactical SATCOM system, will significantly improve ground communications for U.S. forces OTM. Slated for first launch in FY 2010, MUOS will provide ten times more throughput than the current UFO System, and will provide U.S. forces a much more reliable way to communicate.

(c) Wideband. The DSCS provides super high frequency wideband communications for worldwide long-haul communications to fixed station and mobile critical national, strategic, tactical, and other designated governmental users. DSCS includes the GCCS and broadcasts between early warning sites, operations centers, unified and specified commands, and tactical forces. DSCS provides substantial worldwide capacity of high quality voice and wideband data circuits. Worldwide global satellite (WGS) had its initial launch in October 2007. WGS will provide the same capacity as the entire DSCS constellation today.

(d) GBS. The GBS system provides a high-data-rate link for the flow of information from the U.S. or rear echelon to deployed forces. GBS provides information in a dynamically reconfigurable format rapidly adaptable to peace and wartime circumstances, and delivers it to theaters of operation worldwide. GBS is an extension of the Defense Information Systems

network (DISN) and includes GBS theater injection points and receiver terminals. The GBS broadcasts to small, mobile, tactical terminals, and brings high-power satellite transponders, high speed wideband, and simplex broadcast capabilities. Typical products include video, mapping, charting and geodesy, imagery, weather, and digital data.

(e) Commercial SATCOM. DOD SATCOM systems do not have the capacity to satisfy all warfighter requirements for network connectivity. Commercial SATCOM systems provide a flexible means to provide additional or surge capabilities. Administrative and logistics traffic as well as peacetime operations can be satisfied by commercial means. International marine or maritime satellite (INMARSAT), Iridium, Globalstar and Telesat represent some of the better known commercial SATCOM systems. Commercial leases of C-, L- and Ku-band capacity have long been an accepted part of the MILSATCOM architecture; however, commercial SATCOM is often expensive and does not offer the security of DOD systems. Also, the long-term availability of commercial SATCOM bandwidth is subject to business influences. SATCOM capabilities supporting the future Modular Force are described in detail in TRADOC Pam 525-7-4.

(6) Aerial layer. Aerial communications relay programs today are limited to local short-range radio relay in support of lower level tactical commanders (platoon to battalion) via a JTRS or Soldier radio waveform (SRW) radio package on Raven, Shadow, or similar size and function UASs with JTRS relay capability. This could include the FCS Class IV unmanned aerial vehicle (UAV), and a combat net radio and JTRS package on an extended range multipurpose (ERMP). The UAS assets are often dedicated to ISR and strike missions, providing incidental network extension, but could be launched with communications relay as the primary mission with approval of the owning commander. Dedicated or non-dedicated wideband WIN-T communications payload (WCP) may be available as an FCS Class IV UAV or ERMP objective requirement. A high altitude, long loiter (HALL) platform capable of prolonged stratospheric flight with persistent station-keeping ability capable of hosting a communications payload that can provide high capacity communications range extension for the WIN-T network is possible in this timeframe, but has not had its requirement validated , and is currently not programmed or funded. An NTS CBA could investigate the capabilities of the high altitude airship and HALL relay platform and provide the underpinnings for a future requirement.

(7) Commercial fiber-optic network. Army organizations down to brigade level have a limited capability to exploit the extensive bandwidth available in the global commercial fiber-optic network.

(8) NETOPS

(a) GCM involves the following NETOPS critical capabilities to support the core enterprise services previously discussed. These capabilities for GCM must be employed along with the core enterprise services at the strategic, operational, and tactical levels across all DOD warfighting, intelligence, and business domains.

- Visibility involves knowing the status of the information flowing across the GIG and of those systems used to collect, store, process, secure, discover, and disseminate information.

- Monitoring and analysis involves viewing information flows and access, determining impact to network capacity, and is satisfied with a reasonable quality of service. Planning occurs in establishing prioritized information requirements, identifying sources responsible for providing that information, and staging information content throughout the GIG in support of a given operation. Contingency planning for disseminating information is a critical aspect of GCM operational planning.
- Coordinating and responding tracks and maintains knowledge of the various requests and user profiles for information; coordinates changes in the operating parameters of GIG assets; identifies new products; reviews and validates user-profile database; and develops joint policies and procedures governing information. The GIG integrated architecture will enable user data pulls, which will minimize the need for central coordination and administration.
- Management includes establishing the priorities for information gathering and reporting through the commander's critical information requirements and developing policy and procedures to govern information flow; directing subordinate forces to develop mission information exchange requirements and user profiles; and incorporating expected information requirements into communications capacity planning.
- Control involves developing mission information exchange requirements, developing user profiles, and updating and customizing established user profiles.

(b) GND involves the following NETOPS critical capabilities to support the fundamental attributes previously discussed. These capabilities for GND must be employed along with the fundamental attributes at the strategic, operational, and tactical levels across all DOD warfighting, intelligence, and business domains.

- Visibility involves knowing the status of the GIG security. This includes the configuration of each device and current threats to the GIG.
- Monitoring and analysis involves receiving and viewing all GND events and incidents to determine the impact on current operations and providing trend analysis.
- Planning occurs in establishing defense-in-depth configurations, assigning monitoring responsibilities, anticipating contingency operations for a given set of cyber attacks or failures, and coordinating NETOPS priority intelligence requirements with combatant command priority intelligence requirements.
- Coordinating and responding involves receiving, compiling, and disseminating GND events and incidents. This creates a common GND picture and coordinates and directs response to major GND events and incidents that could have an operational impact.
- Management and administration involves collecting and consolidating intrusion detection reports and data, assessing the compiled data, and reporting the results to the appropriate command authorities. Management involves coordinating the efforts of subordinate network control and operations centers to detect, isolate, and contain GND events and incidents. Management establishes policies and procedures to govern GND rules of engagement for subordinate centers. It also maintains and oversees implementation of network defense initiatives and compliance with information assurance vulnerability alert procedures.

(c) GEM involves the following NETOPS critical capabilities to support the IT services previously discussed. The critical capabilities for GEM must be employed along with the IT services at the strategic, operational, and tactical levels across all DOD warfighting, intelligence, and business domains.

- Fault, configuration, accounting, performance, and security are required for computing hosts, software applications, and connected transmission systems, both wired and wireless, that carries voice, video, data, and imagery.
- Monitoring and analysis involves receiving and viewing relevant fault and performance data to determine the impact on current operations and provide trend analysis.
- Planning occurs in establishing the computer and communications configurations for an operation: allocating circuits, calculating loads, ensuring spectrum non-interference, and establishing applications to be used in the operation. Contingency planning, including backup resources and restoration resources, is a critical aspect of GEM planning.
- Coordinating and responding involves receiving, compiling, and disseminating fault and performance data for systems and networks. This creates a common network picture and coordinates response to major network outages that could have an operational impact.
- Management and administration includes establishing restoration priorities for assigned systems and networks, and developing and overseeing implementation of policies, procedures, and special instructions to subordinate network control centers. It involves planning, coordinating, and obtaining approvals for SATCOM access, request for service release, telecommunication service request, tactical telecommunication release, communications system tasking, and obtaining frequency allotments and assignments from the electromagnetic spectrum manager.
- Control involves the ability to perform fault, configuration, accounting, performance, and security management over all assigned systems and networks. Control also involves the ability to maintain and direct automated intrusion detection systems and devices. It also involves the implementation of information assurance vulnerability alert on systems.

(9) Services

(a) Net-centric enterprise services become the joint standard throughout the near- and mid-term. Net-centric enterprise services consist of multiple services, each of which is found in one of nine product families. The product families are further defined as a consumer-facing or enterprise environment service. The descriptions below define each of the nine product families grouped according to their classification as consumer-facing or enterprise environment services.

(b) Consumer-facing services provide a direct interface and capability to warfighters and other DOD end users.

- Messaging service. This service grouping provides the ability to exchange information among users or applications on the enterprise infrastructure, such as e-

mail, DOD-unique message formats, message-oriented middleware, instant messaging, and alerts.

- Discovery service. This service provides processes for discovery of information content or services that exploit metadata descriptions of IT resources stored in directories, registries, and catalogs (includes search engines).
- Mediation service. This set of services helps broker, translate, aggregate, fuse, or integrate data, including accessibility services to support broad user-based requirements in the DOD community.
- Collaboration service. These services allow users to securely work together and jointly use selected capabilities on the network; for example, chat, online meetings, and work group software.

(c) The enterprise environment services support DOD system developers and community of interest service providers.

- Enterprise systems management. This set of services provides end-to-end GIG performance monitoring, configuration management, and problem detection and resolution, as well as enterprise IT resource accounting and addressing; for example, for users, systems and devices. Additionally, this service area, similar to civil 911 and 411 services, encompasses general help desk and emergency support to users.
- Application service. This service grouping provides infrastructure to host and organize distributed on-line processing capabilities.
- Storage service. These services provide physical and virtual places to host data on the network with varying degrees of persistence, such as archiving, continuity of operations and content staging.
- Information assurance and security service. This set of services provides capabilities that address vulnerabilities in networks, infrastructure services, or systems. Further, these services provide characterizations of the risk strength of components as well as the risk posture of the hosting run-time environment in support of future dynamically composed operational threads.
- User assistant service. This service provides the set of automated or manual capabilities that learn and apply user preferences and patterns to assist users to efficiently and effectively utilize network resources in the performance of tasks. In the context of the network, a user represents any person, object, or entity that has the authority to interact with the network. User Assistant shall provide presentation capabilities, decision aids and tools, as necessary, to maximize user efficiency and performance of their task, with operator aids designed to support specific user tasks and tailored to the information needs of the targeted user.

(10) En Route C2

(a) Force commanders must exercise C2 of deploying forces, continue mission planning, and communicate with other elements of the Army and other service components while en route to an AO. When fully matured, WIN-T will have the bandwidth and throughput necessary to provide communications support to deploying forces for EMPR when in transit to an AO.

EMPR requirements include, but are not limited to, situational awareness (enemy and friendly forces), COP, maps, digital images, and visualization of terrain, and collaborative planning.

(b) An en route C2 capability directly influences reaction and deployment times in an environment where potential enemies have the ability to alter rapidly the battlespace before forces arrive in the AO. Force commanders and staffs must be able to continue mission planning and rehearsal that they began at home station once aboard aircraft or theater support vessels during the deployment phase of an operation.

(11) Battle command OTM. OTM transport capabilities are addressed in INCs 2-4 of the WIN-T program. While WIN-T will support battle command OTM requirements, future battle command applications, down to the lowest level platforms, must be capable of adapting to varying levels of transport capacity and providing support to battle command functions in the absence of network connectivity.

(12) Full-Motion Real Time Video

(a) Requirements to transport real-time or near-real- time full-motion video over the Army's enterprise network are increasing. In addition to the requirement to support secure and non-secure video teleconferencing, many new technologies such as sensors carried on UAS deliver capabilities such as target observation in the form of video. Video streams pose a unique challenge compared to the movement of text or graphics over the Internet protocol-based digital networks, which are today's standard. The Network requirements associated with providing real-time, full-motion video media closely approximate those related to voice over Internet protocol service because both media are inherently analog in nature. Conversion from analog to digital for transport and then the conversion back to an analog presentation is just the first technical requirement to be met. As noted earlier in this CCP, the DOD is continuing to rely on COTS products and COTS standards, and these standards are still evolving.

(b) A few critical tenets must be understood with respect to the transport of full motion video media. First, the nature of the media does not allow true real time transport due to the need to provide compression and de-compression of the video stream (Note: current technology usually buffers video streams before display occurs, which creates a time delay.) Second, quality is a direct function of bandwidth availability; the greater the bandwidth available, the greater the quality of the video stream. Quality is usually put in terms of frames per second. Commercial video teleconferencing, the gold standard of quality, is 30 frames per second, and requires 384 kilobits per second when using compression. The uncompressed bit rate is 36.45 megabits per second. As a result, real-time, full-motion video bandwidth demands are likely to exceed transport capacity. Therefore, a third tenet to consider when transporting full-motion video over an Internet protocol network is the imperative to identify the mission that is being supported and determine if 30 frames per second is actually required to meet the capability of the sensor system. For example, if a target being videoed is a stationary target (such as a bridge), then a frame rate of 8 frames per second would be sufficient. If the mission is to support a surgeon supervising an operation from a remote location, then the demand for 30 frames per second would be justified. For most ISR missions, subject matter experts indicate 15 frames per second

would be an appropriate standard. Verifying the mission requirement can preclude unnecessary consumption of bandwidth.

(c) NTS capabilities that will exist at the threshold of the far term period (2015) include the following.

- Convergence of many (but not all) diverse network extension assets into an integrated WIN-T network transport and services capability.
- Improved military SATCOM access with limited commercial SATCOM to support command post mobility.
- Quad-band, high capacity communication capability (HC3) SATCOM terminals that provides access transformational satellite (TSAT) and other military and commercial SATCOM systems.
- Limited narrowband C2 and voice aerial communications relay.
- Wideband broadcast on the move.
- Upgraded high-capacity line-of-sight radios with greater bandwidth and range.
- High frequency (HF) radio waveforms upgraded and integrated into JTRS.
- Improved narrowband on-the-move connectivity via MUOS and JTRS.
- Improved and integrated NETOPS capabilities across the enterprise, progressing toward common operating environment objectives.
- Regional network service centers and Teleports providing DISN services and reach-back capability.

(d) The following capability gaps will exist at the threshold of the concept years (2015).

- Lack of a single, unified network.
- Lack of an integrated CDL WIN-T capability.
- Lack of a single, integrated NETOPS capability.
- Insufficient military SATCOM capacity and coverage.
- Nonexistent all-weather, continuously available aerial communication relay capability
- Limited protected & narrowband communications.
- Limited wideband capability OTM.

d. Far Term Required Capabilities

(1) NTS capabilities must enable command and control. The dependence of Army and joint forces on information, vertically and horizontally integrated from strategic to tactical levels, will continue to grow as technologies supporting situational awareness, decision support, and collaboration tools are advanced. NTS capabilities must provide the means for forces at all levels to achieve SU; establish, maintain, and distribute a COP; create a commander-centric C2 environment; leverage advanced data mining and decision support tools; and conduct high-tempo operations across an expanded, noncontiguous battlefield. At the same time, NTS capabilities must enhance the lethality, survivability, agility, versatility, and sustainability of the force, enabling more effective and timely application of the elements of combat power.

(2) The capability objective of the NTS CCP is to enable warfighter, business, intelligence, and network mission area functions through a single, integrated tactical network that gives Soldiers, units, sensors, weapons, and systems worldwide access to the GIG through communications links that are unconstrained by terrain, weather, or distance. Objective NTS capabilities must ensure future Modular Forces can share relevant information at the right time and place, commanders can maneuver forces without network constraints, and commanders and leaders can utilize automated, collaborative decision support tools to effectively plan, synchronize, and virtually rehearse missions no matter where they are in the battlespace. Integrated NETOPS will provide the global "always on," accessible network and protected information services required in an increasingly dynamic and fluid environment. Network-enabled global identity and tailored permission and policy-based services will enable operations across the warfighting spectrum.

(3) NTS capabilities must provide the means to disseminate information at all levels of classification (unclassified to top secret and sensitive compartmented information) and must enable commanders to maintain situational awareness and control forces while on the move, either mounted or dismounted. NTS capabilities must support offensive operations in a joint environment, giving geographic combatant commanders the ability to conduct tactical operations using information provided by increased network interoperability among DOD, joint, and coalition networks. NTS capabilities must help reduce the forward deployed footprint of network-related forces while increasing effectiveness of the network.

(4) NTS capabilities must enhance ISR functions; provide access to business systems and improved analytical tools; enable the joint exchange of friendly and enemy force tracking down to the tactical level; and increase synergy between and within all echelons.

(5) In the end state, NTS capabilities must enable a robust and integrated network that provides sufficient bandwidth, access, operational flexibility, and the full range of network-centric enterprise services to support forces at all echelons through all phases of an operation in a fluid integrated operations environment. To achieve this, the Army requires the capabilities below.

(a) SATCOM systems that provide dynamically assignable, high-capacity bandwidth for reach and reach-back, from Soldier and platform to strategic levels.

(b) Aerial platforms and payloads that provide flexible, responsive, dedicated, high throughput BLOS communications capability as part of a multitiered network architecture that supports all operational echelons in any condition.

(c) Terrestrial high-capacity wireless systems that leverage dynamic self-organizing and self-healing high-capacity waveforms, to include optical capabilities.

(d) A robust, protected installation infrastructure that enables training, readiness, and home station operation center capabilities.

(e) The ability to employ available fiber-optic bandwidth.

(f) Establishment of globally positioned regional network service centers.

(g) Deployable capabilities that are modular, "tailorable," and capable of connecting platforms from the dismounted Soldier level to the GIG infrastructure.

(h) An integrated, coherent, synchronized network that supports LandWarNet and warfighting functions at all levels.

(i) An integrated NETOPS package that supports the GIG, LandWarNet and the warfighting functions at all levels.

Table C-1.
NTS Battle Command Related Capability Migration Plan

Battle Command-Related NTS Enablers			
Required Capabilities	**Current Enablers FY 07-09**	**Mid Term Enablers Migration FY 10–15**	**Far Term Enablers Migration FY 16–24**
Ability to provide pervasive, extended range, inter- and intratheater global BLOS communications relay and broadcast services between noncontiguous forces, even on the move, in all operational environments and conditions.	Warfighter Information Network-Tactical (WIN-T): Not available Satellites: Ultra-high frequency (UHF), military strategic tactical relay (Milstar), defense SATCOM system (DSCS), commercial L/C/Ku, advanced extremely high frequency (AEHF) (2009) Terminals (representative sample): joint network node (JNN) very small aperture terminal (VSAT), tactical satellite communications (TSC)- 85/93, Trojan special purpose integrated remote intelligence terminal (SPIRIT), mounted battle command on-the-move (OTM),	WIN-T: INC 2 WIN-T Satellites: Mobile user objective system (MUOS), UHF, Milstar, DSCS, Commercial L/C/Ku, advanced extremely high frequency (AEHF), worldwide global satellite (WGS) Terminals (representative sample): Phoenix, SMART-T, SCAMP, GBS, MUOS in joint tactical radio system (JTRS), AN/PRC-117, AN/PSC-5, joint tactical terminal, Tacticomp, ARC-231, WIN-T point of presence (PoP), TCN, Army Navy/field satellite communications (AN/FSC)-78, Army Navy/ground satellite communications (AN/GSC)-52/39/	WIN-T: INC 3WIN-T Satellites: MUOS, WGS, transformational satellite (TSAT), AEHF, Commercial L/C/Ku Terminals (representative sample): High capacity communications capability (HC3), WIN-T PoP TCN, MUOS in JTRS, modernization of enterprise terminals, C & Ku Band, E-6 TACAMO Communications relay package (CRP), Hunter CRP, Shadow CRP Light, FCS Class IV and Class I, ERMP UAS w/CRP-Medium & WIN-T communications payload (WCP), Objective Gateway, high altitude, long

	Phoenix, secure mobile anti-jam reliable tactical terminal (SMART-T), Army Navy portable satellite communications (AN/PSC)-11 single channel anti-jam man portable terminal (SCAMP), global broadcast system (GBS), Iridium/ International Maritime Satellite (INMARSAT), Army/Navy portable radio communications (AN/PRC)-117, Army Navy portable satellite communications (AN/PSC)-5, joint tactical terminal, tactical computer (Tacticomp). airborne radio communication (ARC)-231, Army Navy Fixed Satellite Communications (AN/FSC)-78, Army Navy ground satellite communications (AN/GSC)-52/39/49/70, AN/TSC-86, C & Ku Band, E-6 TACAMO, CPR, Hunter CRP, Shadow CRP Light JTRS: UHF SATCOM-demand assigned multiple access (DAMA) HF	49/70, AN/TSC-86, C & Ku Band E-6 take charge and move out (TACAMO) Comms Relay Package (CRP), Hunter CRP, Shadow CRP Light, future combat systems (FCS) Class IV and Class I, extended range multi-purpose (ERMP) unmanned aerial system (UAS) w/CRP-Medium & WIN-T communications payload (WCP), Objective Gateway JTRS: Ultra-high frequency (UHF) SATCOM-demand assigned multiple access (DAMA) high frequency	loiter (HALL) JTRS: JTRS INC 2 with MUOS
Ability to provide uninterrupted transport of data, voice, and imagery in near-real time.	WIN-T: Not available JTRS: enhanced position location and reporting system (EPLRS) single channel ground to air radio system	WIN-T: INC 2 WIN-T JTRS: JTRS handheld, manpack and small form fits (HMS) with Soldier radio waveform (SRW)	WIN-T: INC 3 WIN-T

	(SINCGARS) Tacticomp	JTRS airborne, maritime, fixed (AMF) with wideband networking waveform (WNW) and SRW	
Ability to transport full-motion-video in real time.	WIN-T: Not available		WIN-T: INC 3 WIN-T
Ability to access net-centric enterprise services.	WIN-T: INC 1 WIN-T JTRS: EPLRS UHF SATCOM-DAMA	WIN-T: INC 2 WIN-T JTRS: JTRS ground mobile radio (GMR) with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: INC 3 WIN-T
Ability to share information across classification domains.	WIN-T: Not available	WIN-T: Partial INC 2 WIN-T	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2
Ability to dynamically establish and maintain space, aerial, and terrestrial communication links that enable the fusion, sharing, push, pull and update of information from a wide variety of sensors and sources in all domains.	WIN-T: Not available	WIN-T: Not available JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2 adds MUOS
Ability to provide access to a wide variety of sensors and sources simultaneously from multiple noncontiguous locations in order to provide timely, actionable, and relevant information in support of the planning, execution and assessment operations of the joint force and component commanders.	WIN-T: Not available JTRS: EPLRS	WIN-T: Not available JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2 adds MUOS
Ability to enable real-time visibility of units' combat readiness and locations.	Blue force tracker (BFT) JTRS: EPLRS	BFT JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2
Ability to seamlessly and pervasively execute	WIN-T: Not available	WIN-T: Not Available	WIN-T: INC 3 WIN-T

NETOPS functions.		JTRS: JTRS enterprise network manager (ENM)	JTRS INC 2 ENM
Ability to reach outside DOD to rapidly obtain information (knowledge centers, national agencies) in all operational environments and conditions.	WIN-T: Not available distributed common ground system – Army (DCGS-A) Trojan	WIN-T: Not available DCGS-A Trojan	WIN-T: INC 3 WIN-T DCGS-A
Ability to dynamically assign frequencies during maneuver operations across a wide range of environments, to include complex and urban terrain.	WIN-T: Not available	WIN-T: Not available	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2 ENM
Ability to operate NTS capabilities unhindered by the presence of jamming and counter- measures.	WIN-T: Not available Satellites: Milstar Terminals : SCAMP, SMART-T JTRS: Single channel ground and airborne radio system (SINCGARS) EPLRS	WIN-T: Not available Satellites: Milstar Terminals : SCAMP, SMART-T JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: Beyond line-of-site (BLOS) (SATCOM with HC3) INC 4 WIN-T Satellites: AEHF/TSAT Terminals: SMART-T, HC3 JTRS: JTRS INC 2

C-3. See Related NTS Required Capabilities

The *See* concept focuses on the contribution to the future Modular Force of data acquisition, the transformation of data into information and knowledge, and the sharing of that information and knowledge. The continuous acquisition and synthesis of data and information from joint and interagency sources, coalition partners, and non-traditional sources permits the future Modular Force to maintain an accurate understanding of the operational environment. Table C-2 depicts the current, midterm, and far-term NTS enablers that support the *See* functional concept.

Table C-2.
NTS See Related Capability Migration Plan

See-Related NTS Enablers			
Required Capabilities	**Current Enablers FY 07-09**	**Mid Term Enablers Migration FY 10–15**	**Far Term Enablers Migration FY 16–24**
Ability to rapidly access, process, and analyze national and commercial imagery from archive and	tactical exploitation system (TES) and tactical exploitation of national capabilities	Warfighter Information Network Tactical (WIN-T): (Partial transport	WIN-T: (Partial transport processed data only) INC 3 WIN-T

databases in theater.	(TENCAP) distributed command ground system – Army (DCGS-A)	processed data only) INC 2 WIN-T DCGS-A	DCGS-A
Ability to rapidly obtain needed data and transfer to the proper location in accordance with the commander's needs and policies.	WIN-T: Not Available Joint tactical radio system (JTRS): EPLRS Trojan Common data link (CDL)	WIN-T: Partial INC 2 WIN-T JTRS: JTRS ground mobile radio (GMR) with WNW and SRW JTRS hand-held, manpack, and small form fit (HMS) with Soldier radio waveform (SRW) JTRS airborne, maritime, fixed (AMF) with wide-networking waveform (WNW) and Soldier radio waveform (SRW)	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2
Ability to protect the integrity of information while in transit and/or in storage in all operational environments and conditions.	WIN-T: Not Available DCGS-A	WIN-T: Not Available JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW DCGS-A	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2

C-4. Move Related NTS Required Capabilities

The *Move* functional concept describes future requirements for strategic responsiveness and operational agility of the future Modular Force. NTS capabilities are essential to both strategic responsiveness and operational agility. Table C-3 depicts the current, midterm, and far-term NTS enablers required to support the *Move* functional concept.

Table C-3.
NTS Move Related Capability Migration Plan

Move-Related NTS Enablers			
Required Capabilities	**Current Enablers FY 07-09**	**Mid Term Enablers Migration FY 10–15**	**Far Term Enablers Migration FY 16–24**
Ability to provide seamless information flow to enable SA, collaboration, mission planning and rehearsal for forces en route to an	Warfighter Information Network- Tactical (WIN-T): Not available Joint tactical radio	WIN-T: Not available JTRS: JTRS ground mobile radio (GMR) with	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2 adds mobile user objective

operation.	system (JTRS): Ultra-high frequency (UHF) SATCOM-designated assigned multiple access (DAMA)	wide-network waveform (WNW) JTRS airborne, maritime, fixed (AMF) with WNW UHF SATCOM-DAMA	system (MUOS)
Ability to access uninterrupted communications links that enable small teams of experts (unit movement Non-commissioned and commissioned officers) to react to changing priorities and maintain deployment momentum.	WIN-T: Not Available JTRS: Enhanced position location and reporting system (EPLRS) Single channel ground and airborne radio system (SINCGARS)	WIN-T: Partial INC 2 WIN-T (Company level) JTRS: JTRS GMR with WNW and Soldier radio waveform (SRW) JTRS hand-held, manpack, and small form fit (HMS) with Soldier radio waveform (SRW) JTRS AMF with WNW and SRW	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2 adds MUOS
Ability to rapidly access and disseminate information through the JOPES.		JTRS: JTRS GMR with JTRS AMF with WNW	JTRS: JTRS INC 2 adds MUOS
Ability to provide seamless in-transit visibility of sustainment assets.		WIN-T: (Partial Transport Only) INC 2 WIN-T JTRS: JTRS GMR with WNW JTRS AMF with WNW	WIN-T: (Partial Transport Only) INC 3 WIN-T JTRS: JTRS INC 2 adds MUOS

C-5. Strike Related NTS Required Capabilities

The *Strike* functional concept focuses on future Modular Force networked fires and effects at strategic, operational, and tactical levels, to include aviation interdiction attack. The *Strike* functional concept incorporates the effects of fires capabilities as well as effects achieved by other means such as information operations, to include the IO core capabilities of EW, computer network operations, psychological operations, military deception and operations security, and the IO-related capabilities of PA, civil-military operations, defense support to public diplomacy, plus other effects related to space control. Table C-4 depicts the current, midterm, and far-term NTS enablers required to support the *Strike* functional concept.

Table C-4.
NTS Strike Related Capability Migration Plan

Strike-Related NTS Enablers			
Required Capabilities	**Current Enablers FY 07-09**	**Mid Term Enablers Migration FY 10–15**	**Far Term Enablers Migration FY 16–24**
Ability to access full spectrum of targeting information resources at all levels of command in support of strike operations, to include information supporting C2, ISR, and SA functions and processes.	Joint tactical radio system (JTRS): Enhanced position location and reporting system (EPLRS) Ultra-high frequency (UHF) SATCOM designated assigned multiple access (DAMA) Single channel ground and airborne radio system (SINCGARS)	Warfighter Information Network-Tactical (WIN-T): Partial INC 2 WIN-T JTRS: JTRS ground mobile radio (GMR) with wideband networking waveform (WNW) and Soldier radio waveform (SRW) JTRS hand-held, manpack, and small form fit (HMS) with SRW JTRS airborne, maritime, fixed (AMF) with WNW and SRW	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2 adds mobile user objective system (MUOS)
Ability to provide a continuous collaborative information environment to support strike operations.	JTRS: EPLRS UHF SATCOM DAMA SINCGARS	JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: (Partial Transport Only) INC 3 WIN-T JTRS: JTRS INC 2 adds MUOS
Ability to provide ISR and control data links that provide: weather forecasting, terrain and infrastructure updates to include imagery support for en route mission planning and rehearsal, and enemy situation updates.	JTRS: EPLRS	JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: (Partial Transport Only) INC 3 WIN-T
Ability to provide continuous transport for over-the-horizon and BLOS airspace C2 and airspace management in support of dynamic re-tasking of aviation missions.	JTRS: UHF SATCOM DAMA	JTRS: AMF with WNW	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2 adds MUOS

C-6. Protect Related NTS Required Capabilities

The *Protect* functional concept describes how the future Modular Force will protect people, physical assets, and information against the full spectrum of threats. NTS capabilities are key enablers of the protect function. Table C-5 depicts the current, midterm, and far-term NTS enablers required to support the *Protect* functional concept.

Table C-5.
NTS Protect Related Capability Migration Plan

Protect-Related NTS Enablers			
Required Capabilities	**Current Enablers FY 07-09**	**Mid Term Enablers Migration FY 10–15**	**Far Term Enablers Migration FY 16–24**
Ability to deter, warn, and if necessary, defend against enemy attack of NTS capabilities; assure hostile forces cannot prevent friendly use of NTS capabilities; ensure U.S. and allied forces ability to conduct NTS-enabled military activities.		Joint tactical radio system (JTRS): JTRS enterprise network manger (ENM) JTRS global mobile radio (GMR) with wideband networking waveform (WNW) and Soldier radio waveform (SRW) JTRS hand-held, manpack, and small form fit (HMS) with SRW JTRS airborne, maritime, fixed (AMF) with WNW and SRW	Warfighter Information Network-Tactical (WIN-T): (Partial Transport Only) INC 3 WIN-T
Ability to plan and execute NTS COOP.		JTRS: JTRS ENM	JTRS: JTRS INC 2 ENM
Ability to provide dedicated, persistent, and redundant NTS support for the Protect functions (detect, assess, warn, prevent, deter, defend, and respond).		JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	JTRS INC 2 ENM
Ability to detect jamming operations conducted as part of the anti-access efforts.		JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	

Ability to protect NTS capabilities from deliberate or accidental interference.		JTRS: JTRS ENM JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2 ENM
Ability to detect, deny, and disrupt adversary attempts to disrupt friendly NTS capabilities.		JTRS: JTRS ENM	WIN-T: (Partial Transport Only) INC 3 WIN-T JTRS: JTRS INC 2 ENM

C-7. Sustain Related NTS Required Capabilities

The *Sustain* functional concept establishes the overarching framework for logistics support to the future Modular Force. The concept seeks to answer the challenges that flow from the joint operating environment of the future Modular Force. Table C-6 depicts the current, midterm, and far-term NTS enablers required to support the *Sustain* functional concept.

Table C-6.
NTS Sustain Related Capability Migration Plan

Sustain-Related NTS Enablers			
Required Capabilities	**Current Enablers FY 07-09**	**Mid Term Enablers Migration FY 10–15**	**Far Term Enablers Migration FY 16–24**
Ability to transmit data concerning position, operational status, equipment or aircraft conditions, and maintenance diagnostics, and prognostics anywhere in the JOA.	Manual file transfer from tester to standard army management information system (STAMIS) Joint tactical radio system (JTRS) Enhanced position location and reporting system (EPLRS) Single channel ground and airborne radio system (SINCGARS)	CSS Automated Information System interface (CAISI) very small aperture terminal (VSAT) JTRS: JTRS ground mobile radio (GMR) with wideband networking waveform WNW and Soldier radio waveform (SRW) JTRS hand-held, manpack, and small form fit (HMS) with SRW JTRS airborne, maritime, fixed (AMF) with WNW and SRW	Warfighter Information Network-Tactical (WIN-T): INC 3 WIN-T JTRS Future combat system (FCS) platform mission readiness system (PSMRS)
Ability to maintain in-transit visibility of all supporting logistical activities, supplies, and	WIN-T: INC 1 WIN-T combat service support automated information	WIN-T: INC 2 WIN-T CAISI-VSAT (unclassified)	WIN-T: (Partial Transport Only) INC 3 WIN-T

services.	system interface (CAISI)-very small aperture terminal (VSAT)(unclassified) mobile tracking system (MTS)	Mobile tracking system (MTS)	
Ability to establish a secure, pervasive, logistics C2 and information infrastructure emphasizing speed, precision, accuracy, visibility, and centralized management to include: logistics requirements, supply distribution and management, connection to industry and knowledge centers, passive radio frequency identification tags, Soldier health status, petroleum and fuel supply. Support of a logistics COP, proactive and anticipatory maintenance, munitions, water, and logistics preparation of the battlefield.	WIN-T: INC 1 WIN-T CAISI VSAT (unclassified) MTS SINCGARS Working with Logistics STAMIS systems, and Army battle command sustainment support system (ABCS3) JTRS: EPLRS SINCGARS	WIN-T: INC 2 WIN-T CAISI VSAT (unclassified) MTS Working with logistics STAMIS systems, transition to global combat support system-Army (GCSS-A) fixed/tactical (F/T) and GCSS-A product lifecycle management plus (PLM+), and logistics modernization program (LMP) and ABCS3 JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: (Partial Transport Only) INC 3 WIN-T JTRS Working with GCSS-Army (F/T), GCSS-Army (PLM+), LMP, and the Army battle command system (ABCS) logistic component, logistics decision support system (LDSS), PSMRS
Ability to provide seamless transport of SA data in support of convoy operations, including route reconnaissance information and convoy monitoring.	WIN-T: INC 1 WIN-T CAISI VSAT (unclassified) MTS SINCGARS Working with ABCS3 JTRS: EPLRS	WIN-T: INC 2 WIN-T CAISI VSAT (unclassified) MTS Working with ABCS3 JTRS: JTRS GMR with WNW and SRW JTRS HMS with SRW JTRS AMF with WNW and SRW	WIN-T: INC 3 WIN-T JTRS Working with ABCS logistic component, LDSS
Ability to share information across classification domains.	WIN-T: Not Available Manual transfer	WIN-T: Partial INC 2 WIN-T	WIN-T: INC 3 WIN-T JTRS: JTRS INC 2

Appendix D
NETOPS

D-1. Introduction

a. This appendix describes NETOPS, network operations functions, and the relevance of NETOPS to NTS capabilities.

b. NETOPS is the operational construct consisting of the essential tasks, SA, and command and control that the commander, U.S. Strategic Command (USSTRATCOM) will use to operate and defend the GIG, and the Commander 9th Signal Command (Army). The goal of NETOPS is to provide assured and timely network-enabled services across strategic, operational, and tactical boundaries. This supports the DOD's full spectrum of warfighting, intelligence, and business missions. NETOPS provides tactical units the ability to harness the power of GIG enterprise services and bring this power to the battlefield where it is needed most, thus increasing the lethality of Army tactical units.

D-2. GEM

a. GEM is the technology, processes, and policy necessary to effectively operate the systems and networks that comprise the GIG. This essential task merges IT services with the NETOPS critical capabilities. GEM is a joint and global network term. GEM at the LandWarNet level of the global network is referred to as enterprise systems management and network management.

b. GEM, as it relates to the LandWarNet, is enterprise systems management and network management. Enterprise systems management is the management of technologies, processes, and policy necessary to provide end-to-end SA and management of the LandWarNet through performance monitoring, configuration management and problem detection/resolution, enterprise IT resource accounting and addressing, facilitating the effective operation of the systems and networks that comprise the LandWarNet supporting net centric operations. Enterprise systems management combined with network management provides enterprise systems management and network management for the LandWarNet. Network management provides the services of a networked system with the desired level of quality and guaranteed availability.

c. IT services. There are five major IT services within GEM. Theses services manage the GIG services and technologies to ensure the effective and efficient operations, performance, availability, and security of GIG information systems, elements of systems, and services. These services must be employed at the strategic, operational, and tactical levels across all DOD warfighting, intelligence, and business domains. The five services are discussed below.

(1) Enterprise services management provides the services for end-user applications, web-based services, remote hosted applications, discovery, storage, operating systems, and other IT components of applications. Applications management provides the services for end user applications, local area network environment, web-based services, remote hosted applications, storage, operating systems, and other IT components of applications; focuses on higher layer protocols.

(2) Systems management provides the day-to-day management of computer-based information systems, elements of systems, and services to include software applications, operating systems, databases, and hosts of the end-users. System management comprises all the measures necessary to ensure the effective and efficient operations of GIG information systems and elements of systems and services.

(3) Network management provides the services of a networked system with the desired level of quality and guaranteed availability. Networks included within GEM are located on all three means of communication (terrestrial, airborne, or SATCOM), and they include switched networks, data networks, video teleconferencing networks, SATCOM networks, and wireless networks.

(4) SATCOM management is the day-to-day operational management of all apportioned and non apportioned SATCOM resources. SATCOM Management includes appropriate support when disruption of service occurs; provision of global SATCOM system status; maintenance of global SA to include each combatant command's current and planned operations as well as space, control, and terminal segment asset and operational configuration management; radio frequency interference resolution management; satellite anomaly resolution and management; and SATCOM interference to the GIG.

(5) Electromagnetic spectrum management and planning involves the efficient employment of the electromagnetic spectrum, including international planning; frequency allocation; coordination with civilian and other government departments, agencies, military services and components, and allies; frequency assignment, allotment, and approval; protection; frequency de-confliction; interference resolution; and coordination with EW activities. Spectrum management ensures that the combatant commanders and subordinate commanders have cognizance of all spectrum management decisions that impact accomplishment of their missions.

D-3. GIG Network Defense

a. To convey the global dimension of USSTRATCOM's mission to defend the GIG, the term GND is used in this document to encompass USSTRATCOM's operational responsibilities for IA, CND, critical infrastructure protection, and other GIG defense tasks in an effort to more clearly define the scope of this NETOPS essential task. This is not intended to replace the terms of IA and CND. Additionally, GIG constituent systems that meet the definition of a National Security System must follow the appropriate IA guidelines and policies for a National Security System. GIG systems that are not designated a National Security System must provide adequate IA so the security of other GIG National Security systems will not be jeopardized. GND is a joint and global network term. GND at the LandWarNet level of the global network is referred to as IA and CND.

b. IA includes IO that protect and defend information and information systems to ensure their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

c. CND provides defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.

d. Fundamental attributes. There are five fundamental attributes within GND. These attributes help protect friendly information and information systems while denying adversaries access to the same information and information systems.

(1) Protection involves prior actions taken to counter vulnerabilities in GIG information transport, processing, storage, service providers, and operational uses. Protection activities include emission security, communications security, computer security, information security, and critical infrastructure protection. In addition, this will incorporate physical protection, access control, cryptography, network guards, and firewall systems.

(2) Monitoring involves the examination of information systems to sense and assess abnormalities and the use of anomaly and intrusion detection systems.

(3) Detection is instrumental to initiating system response and restoration actions. Timely detection, identification, and location of abnormalities include attack, damage, or unauthorized modification.

(4) Analyzing involves assessing pertinent information to determine indications and warnings, providing SA, evaluating system status, identifying root cause, defining courses of action, and prioritizing response and recovery actions. These steps are taken in order to conduct the necessary reconfiguration of GIG assets.

(5) Responding requires that direct action is taken to mitigate the operational impact of an attack, damage, or other incapacitation of an information system. Response also includes restoration. This is the prioritized return of essential information systems, elements of systems, or services to pre-event capability. CND response actions include defensive and restoration actions. Response actions are deliberate, authorized defensive measures or activities. These actions protect and defend computer systems and networks under attack or targeted for attack or exploitation by adversary computer systems and networks. Response actions extend DOD's layered defense-in-depth capabilities and increase DOD's ability to withstand adversary attacks or exploitations. Objectives for using CND response actions include strengthening DOD's defensive posture and operational readiness, halting or minimizing attack and exploitation effects or damage, and supporting rapid, complete attack, or exploitation characterization.

D-4. GCM

a. GCM is defined as the technology, processes, and policy necessary to provide awareness of relevant, accurate information; automated access to newly revealed or recurring information; and timely, efficient, and assured delivery of information in a usable format. As GCM becomes more mature, the complete complement of its services will be available for use by all authorized DOD GIG users as a network-enabled service. This essential task merges core services with the

NETOPS critical capabilities. GCM is a joint and global network term. GCM at the LandWarNet level of the global network is referred to as IDM core services.

b. IDM core services is the final component of NETOPS. It provides awareness of relevant, accurate information; automated access to newly discovered or recurring information; and timely, efficient delivery of information based on the commander's priorities. It seeks to achieve the right information, arriving at the right place, at the right time, and in a usable format. IDM uses specific processes, services, and applications to provide this information to Soldiers at the strategic, operational, and tactical military operational levels.

c. Core services. The core services necessary to implement GCM are content discovery, content delivery, and content storage. These core services are envisioned to be enterprise wide services used by the entire DOD to ensure our information is available to all authorized users. The GIG enterprise service effort and the network enabled enterprise services program will deliver these core services:

(1) Content discovery provides the ability to quickly search for information throughout the GIG. Using any Web browser, whether on a desktop computer or wireless device, operational staffs can search across multiple sources from one place. Once the product is located, the access service permits the users to pull in the needed product.

(2) Content delivery provides the user the capability to replicate files and directives, publish and subscribe to information based on roles and responsibilities, and provide assured, timely transport of the information, to include notification of when the information was read by a distant user. Information that is received in the area of responsibility by the information manager is delivered using the core services delivery service. Items are delivered across multiple, heterogeneous communications systems. All information has a delivery and read receipt notification to provide assured delivery of information products.

(3) Content storage provides physical and virtual places to host data on the network with varying degrees of persistence. These information storage capabilities will be located throughout the GIG.

Glossary

Section I
Abbreviations

ABCS	Army battle command system
ABCS3	Army battle command sustainment support system
ACC	air component commander
AEHF	advanced extremely high frequency
AFATDS*	advanced field artillery tactical data system
AMF	airborne, maritime, fixed
AN/FSC	Army Navy fixed satellite communications
AN/GSC	Army Navy ground satellite communications
AN/PRC	Army Navy portable radio communications
AN/PSC	Army Navy portable satellite communications
AO	area of operations
AOC*	air operations center
APOD	aerial port of debarkation
ARFORGEN	Army force generation
ASCC	Army service component command
BSC3*	battle command sustainment support system
BCD*	battlefield coordination
BCT	brigade combat team
BFN	bridge to future networks
BFT	blue force tracking
BLOS	beyond line of sight
C2	command and control
C3D2	camouflage, cover, concealment, denial, and deception
CAISI	combat service support automated information system interface
CBA	capabilities based assessment
CBRN	chemical, biological radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosive
CCP	concept capability plan
CDB	concepts and doctrine branch
CDL	common data link
CD&E	concept development and experimentation
CDID	capabilities development and integration directorate
CENTCOM*	Central Command
CIE	collaborative information environment
CJCSI	Chairman Joint Chief of Staff instruction
CJFLCC*	coalition/joint forces land component commander
COCOM*	combatant commander
CONUS	continental U.S.
COP	common operating picture
COOP	continuity of operation plan
COTS	commercial off-the-shelf

CNA	computer network attack
CND	computer network defense
CNE	computer network exploitation
CNO	computer network operations
CPD	capabilities production document
CRDD	concepts, requirements, and doctrine division
CRP	communications relay package
CSS	combat service support
DA	Department of the Army
DAADC	deputy area air defense commander
DAMA	demand assigned multiple access
DCGS-A	distributed common ground system Army
DI	defense information
DISN	defense information systems network
DNS*	domain name service
DOD	Department of Defense
DOTMLPF	doctrine, organization, training, materiel, leadership and education, personnel, and facilities
DSCS	defense satellite communications system
DTSS	digital topographical support system
EA	electronic attack
EMPR	en route mission planning and rehearsal
EMSO	electromagnetic spectrum operations
ENM	enterprise network manager
EPLRS	enhanced position location and reporting system
ERMP	extended range multipurpose
ESB	expeditionary signal battalion
EUCOM*	European Command
EW	electronic warfare
FBCB2*	FORCE XXI battle command brigade and below
FCS	future combat system
FM	field manual
FY	fiscal year
GBS	global broadcast service
GCCS(A)	global command and control system (Army)
GCM	global content management
GCSS(A)	global combat support system (Army)
GEM	global enterprise management
GIG	global information grid
GMR	ground mobile radio
GND	global network defense
GPS	global positioning system
HALL	high altitude, long loiter
HC3	high capacity communications capability
HF	high frequency
HMS	handheld, manpack and small for fit

HQ	headquarters
IA	information assurance
IDM	information dissemination management
IMETS*	integrated meteorological system
INC	increment
INMARSAT	international maritime satellite
IO	information operations
ISR	intelligence, surveillance, reconnaissance
IT	information technology
JCIDS	joint capabilities integration and development system
JFAC*	joint force air component
JFACC	joint force air component commander
JFC	joint force commander
JFLC	joint force land component
JFLCC	joint force land component commander
JFMCC	joint force maritime component commander
JMOC	joint martime operations center
JNN	joint network node
JOPES	joint operation planning and execution system
JOA	joint operations area
JSOTF	joint special operations task force
JTF	joint task force
JTRS	joint tactical radio system
JTT	joint tactical terminal
JVMF*	joint variable message format
LDAP*	lightweight directory access protocol
LOC	lines of communication
LOS	line of sight
LVC	live virtual constructive
MCS*	maneuver control system
MDSC	Medical Deployment Support Command
MEF*	Marine expeditionary forces
MILSATCOM	military satellite communications
Milstar	military strategic tactical relay
MSE	mobile subscriber equipment
MSS*	mobile subscriber service
MUOS	mobile user objective system
MTS	mobile tracking system
NAIC	North American industry classification
NATO*	North Atlantic Treaty Organization
NCOE	net-centric operation environment
NECC*	network-enabled command capability
NETOPS	network operations
NGO	nongovernmental organization
NIPRNET	non-secure Internet protocol router network
NORTHCOM*	Northern Command

NSCs	network service centers
NTS	network transport & services
OTM	on-the-move
PA	public affairs
PACOM*	Pacific Command
PoP	point of presence
PSMR	platform mission readiness system
RF*	radio frequency
ROK*	Republic of Korea
ROMO	range of military operations
SA	situational awareness
SATCOM	satellite communications
SCAMP	single channel anti-jam man portable terminal
SINCGARS	single channel ground to air radio system
SMART-T	secure mobile anti-jam reliable tactical terminal
SOCOM*	Special Operations Command
SOF*	special operations forces
SOUTHCOM*	Southern Command
SPIRIT	special purpose integrated remote intelligence terminal
SPOD	seaport of debarkation
SRW	Soldier radio waveform
SU	situational understanding
TAADCOORD	theater Army air and missile defense coordinator
TACAMO	take charge and move out
Tacticomp	tactical computer
TAIS*	tactical airspace integration system
TCDL*	tactical command data link
TES	tactical exploitation system
TENCAP	tactical exploitation of national capabilities
TRADOC	training and doctrine command
TRI TAC	tri-service tactical
TSAT	transformational satellite
TSC	theater sustainment command
TTP	tactics, techniques, and procedures
UAS	unmanned aerial systems
UAV	unmanned aerial vehicle
UFO	ultra high frequency follow-on
UHF	ultra high frequency
UK*	United Kingdom
U.S.	United States
USMTF*	U.S. message text format
USSTRATCOM	U.S. Strategic Command
VSAT	very small aperture terminal
WCP	WIN-T communications payload
WGS	worldwide global satellite
WIN-T	warfighter information network – tactical

WMD	weapons of mass destruction
WNW	wideband networking waveform

* Denotes and acronym found only in the figures.

Section II
Terms

collaborative information environment
CIE is a suite of integrated, network-enabled tools, organizations, business rules, processes, and trained personnel that enables simultaneous, collaborative planning and execution.

global enterprise management
GEM is defined as the technology, processes, and policy necessary to effectively operate the systems and networks that comprise the GIG. This essential task merges IT services with the NETOPS critical capabilities. GEM is a joint and global network term. GEM at the LandWarNet level of the global network is referred to as enterprise systems management and network management.

LandWarNet
The Army's portion of the GIG. It encompasses all Army information management systems and information systems that collect, process, store, display, disseminate, and protect information worldwide. It enables execution of Army C2 processes and supports operations through wide dissemination of relevant information. It facilitates rapidly converting relevant information into decisions and actions. It allows commanders to exercise command and control from anywhere in their area of operations.

live, virtual, and constructive integrating architecture
The LVC IA is a network-centric linkage that collects, retrieves, and exchanges data between and among LVC instrumentation, simulators and simulations, and joint and Army command, control, communications, computers, intelligence, surveillance, and reconnaissance systems. It supports DOD training transformation and Army training doctrine by providing the required integrated LVC mission rehearsal and training environment that allows commanders, leaders, battle staffs, and units to train as they expect to operate as part of the joint force.

network management
Network management focuses on the people, technology, processes, policy, and capabilities necessary to operate effectively the systems and networks, including their configuration, availability, performance, manageability, and enterprise connectivity.

network services
Network services generally associated with network operations such as connecting all assets, sharing information among interagency, coalition, IO commercial, NGO participants, archiving large volumes of data, maintaining network status, keeping all nodes informed, supporting separate constellations of community of interest, and supporting geographically transitioning nodes.

network transport
For the purpose of this CCP, network transport is a system of systems including the people, equipment, and facilities that provide **e**nd-to-end communications connectivity for network components.

operational base
Within this concept, the term operational base refers to the fixed station communications and information system infrastructure and related organizations that support deployed operational forces.

quality of service
Measures of network performance include prioritization, response time, precedence, reliability, and latency. Quality of service management tools enable the allocation of network resources to meet priorities established by the commander.

speed of service
The time between the release of information by the originator and the receipt of that information by the addressee.