

# GLOBAL NETWORK ENTERPRISE CONSTRUCT (GNEC)



The Army's Strategic Vision for the  
Transformation of LandWarNet

## MESSAGE TO OUR STRATEGIC PARTNERS



Office, Chief Information Officer / G-6


DEPARTMENT OF THE ARMY  
OFFICE OF THE SECRETARY OF THE ARMY  
107 ARMY PENTAGON  
WASHINGTON DC 20310-0107



### MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: The Global Network Enterprise Construct (GNEC) – Transforming LandWarNet

1. After eight years of war, we are a fundamentally different Army. While conducting wartime operations we are also embarking on the largest transformation of the Army since WWII. The transformation process will result in an Army that is a versatile, expeditionary force capable of full spectrum operations. The Army's responsiveness is dependent on those expeditionary capabilities and the network's ability to support the transition of our forces anywhere in the world. To support an expeditionary Army, we must also fundamentally change and adapt our institutions, including LandWarNet--the Army's portion of the Global Information Grid. The Army Chief of Staff recognized the need to transform LandWarNet and has charged the Army CIO/G6, in cooperation with our LandWarNet partners across the Army to reshape the Army's existing network and battle command components into the Army's first enterprise activity. As articulated in the Army Posture Statement and the supporting Army Campaign Plan, transforming LandWarNet is a critical Army institutional adaptation initiative.
2. Over the next three years, the Army will transform LandWarNet to a centralized, more secure, operationalized, and sustainable network using the Global Network Enterprise Construct (GNEC). Operational environment complexities and increasing demands by Army, joint, interagency, intergovernmental and multinational mission partners to receive the right information, at the right time has elevated the importance of network access, control, and utilization. Key to providing the Army with an expeditionary capability is the need to operationalize LandWarNet; transforming to deliver a global, standardized, protected and economical network enterprise that is centralized, more secure, sustainable, and capable of seamlessly delivering network capabilities and services as Warfighters transition throughout all operational phases.
3. GNEC is an Army-wide strategy to transform LandWarNet to an enterprise activity, focusing on four principle objectives: (1) Operationalize LandWarNet, (2) Dramatically improve the LandWarNet defense posture, (3) Realize economies and efficiencies while improving effectiveness, and (4) Enable Army Interoperability and collaboration with mission partners. The establishment of the Army global network enterprise requires dramatic changes to our current processes and network operations. GNEC will consolidate loosely affiliated, independent networks into a true global enterprise that transforms LandWarNet into a single information environment with global access, standard infrastructures, and common policies/standards that ultimately provide information services from the generating force to the tactical edge. In the end, all Army generating force networks will be managed by a single command (Network Enterprise Technology Command (NETCOM/9<sup>th</sup> Signal Command (Army)) organizing Army information to make it globally accessible, useful and secure for Soldiers deployed anywhere in the world.

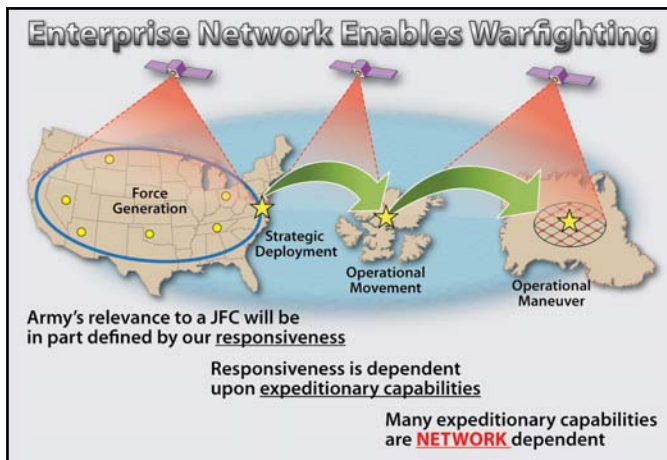
  
JEFFREY A. SORENSON  
Lieutenant General, GS  
Chief Information Officer/G-6

DISTRIBUTION:

## WHAT IS GNEC?

*"We are transforming to become a fundamentally different Army – a modular-based, expeditionary force capable of full-spectrum operations. To support an expeditionary Army, we must also fundamentally change and adapt our institutions, including LandWarNet – the Army's portion of the Global Information Grid."*  
 – CSA, 2 March 2009

The Army is operating in an era of global persistent conflict against both synchronous and asynchronous threats; and the Army's relevance to Joint Force Commanders will be judged by its responsiveness and expeditionary capability. Key to providing the Army with an expeditionary capability is the need to operationalize LandWarNet; transforming to deliver a global, standardized, protected and economical network enterprise that is centralized, more secure, sustainable, and capable of seamlessly delivering network capabilities and services as Warfighters transition throughout all operational phases of joint operations.



Operational experiences in Iraq and Afghanistan support the continued need to eliminate barriers to gain network access, establish overall control and situational awareness of LandWarNet, and ultimately utilize LandWarNet to share information across Army, joint, interagency, intergovernmental and multinational (JIIM) organizations. Additionally, DoD designated cyberspace as a warfighting domain on 12 May 2008 and the LandWarNet is the Army's application of cyberspace. With that, no other domain will experience the reality of persistent conflict more than LandWarNet. A variety of opponents will continually contest the environment with differing synchronous and asynchronous threats across the full spectrum of conflict, from stable peace to general war. The Army must ensure freedom of action in Army cyberspace, and when directed to deploy network assets, fight through a threat event when it occurs, restore normal operations after an event, and transition virtual areas of operations to other authorities if and when required.

To achieve these ends, LandWarNet must be transformed to achieve unprecedented levels of command and control (C2), interoperability and compatibility; protection; governance; standardization; and fiscal transparency. Improving LandWarNet's

response to rapidly changing, increasingly complex capability and service requirements will ensure Army forces achieve information superiority when engaged in expeditionary, JIIM operations throughout all phases of military operations.

**What is GNEC:** GNEC is an Army-wide strategy that will transform LandWarNet to an enterprise activity.

*"GNEC is the focused, timed-phased, prioritized, resource sensitive Army-wide strategy to transition LandWarNet from many loosely-affiliated independent networks into a truly global capability that is designed, deployed and managed as a single integrated enterprise."* – Army CIO/G-6, 23 January 2009

A single integrated enterprise will achieve an information environment with global access, standard infrastructures, unity of C2 across Army cyberspace and common policies/standards that ultimately provide information services from the generating force to the tactical edge.

**The GNEC is a Soldier's Story:** GNEC will ultimately facilitate mission accomplishment by providing tactical services "to the edge" in support of the Warfighter. The Warfighter tactical edge user solutions must work in austere deployed environments. Today many information services and systems are designed to work within robust networks and often do not scale down to the tactical user. This separation between home station and deployed capabilities requires the user to transition from garrison information services to tactical information services, often losing functionality in the deployed environment.

GNEC challenges the Army to deliver services that are timely, relevant, and focused on the needs of the Warfighter while providing solution sets (e.g., operational outcomes, validated requirements, and architectures) to ensure stakeholder communities move toward a common and unified end state. GNEC

## WHAT IS GNEC?

continued

centralizes control of the LandWarNet enterprise network under the single command of the Army Network Enterprise Technical Command (NETCOM)/9th Signal Command (Army) [9th SC (A)].

9th SC (A) will use the GNEC strategy to deliver a global network enterprise from desktop to foxhole, gaining resource efficiencies through single common standards and configu-

rations. The Global Network Enterprise will provide Soldiers single identity from home station to the Area of Responsibility (AOR) and back; ensuring the information is managed so the Warfighter can access information as needed from anywhere, anytime, and protect the network and information from any adversary. Together, all must do what is necessary to ensure an information advantage and give Warfighters the tools they need to accomplish their mission.

## GNEC STRATEGY

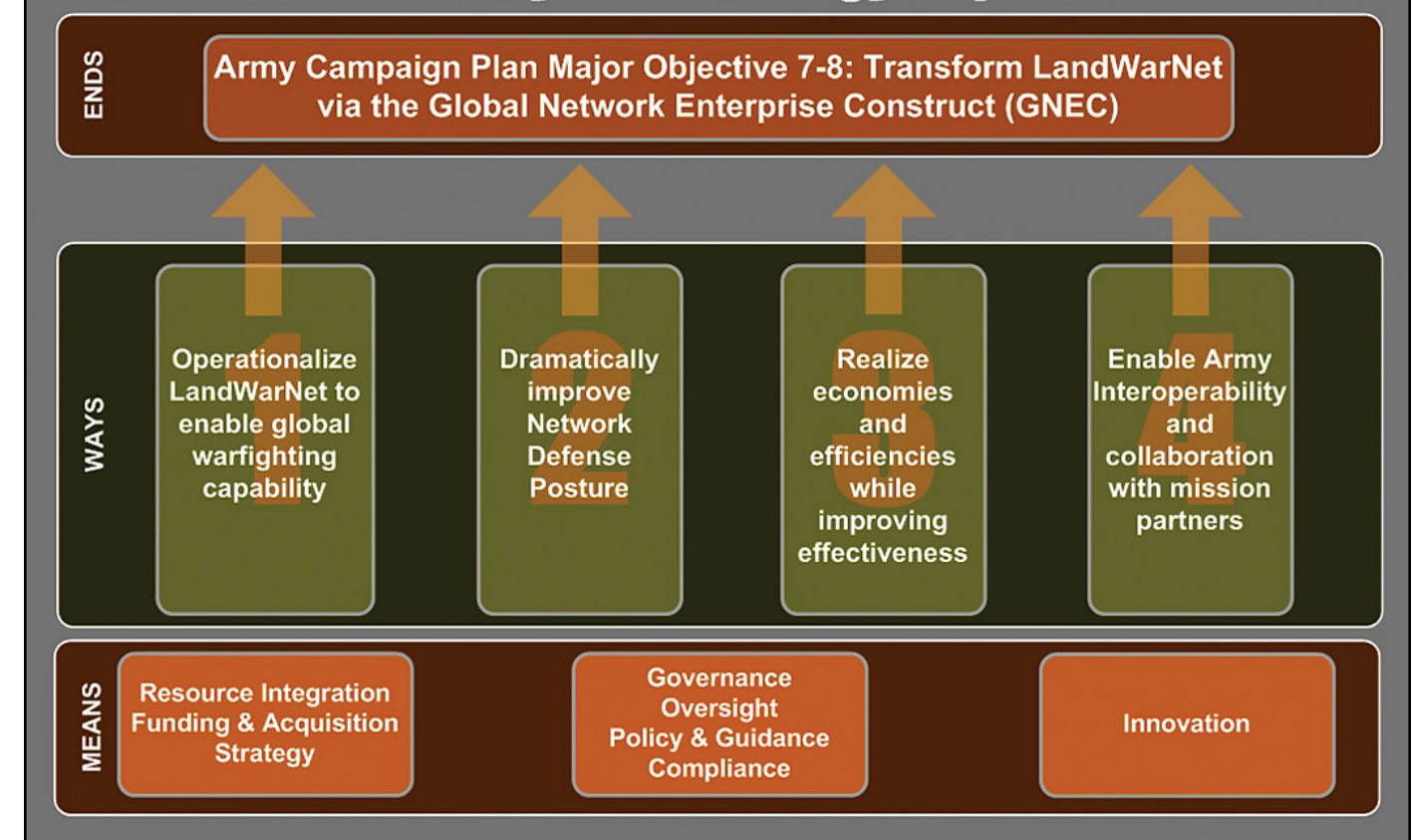
**GNEC Vision:** Operationalize LandWarNet; transforming to deliver a global, standardized, protected and economical network enterprise – effective, secure and well-managed.

GNEC transforms the current LandWarNet of stove-piped systems, processes, governance, and control to a unified net-centric environment. This Army network enterprise capability provides a single, global IT network enterprise, operating in the JIIM environment, enabling information superiority through all phases of the spectrum of operations. GNEC will

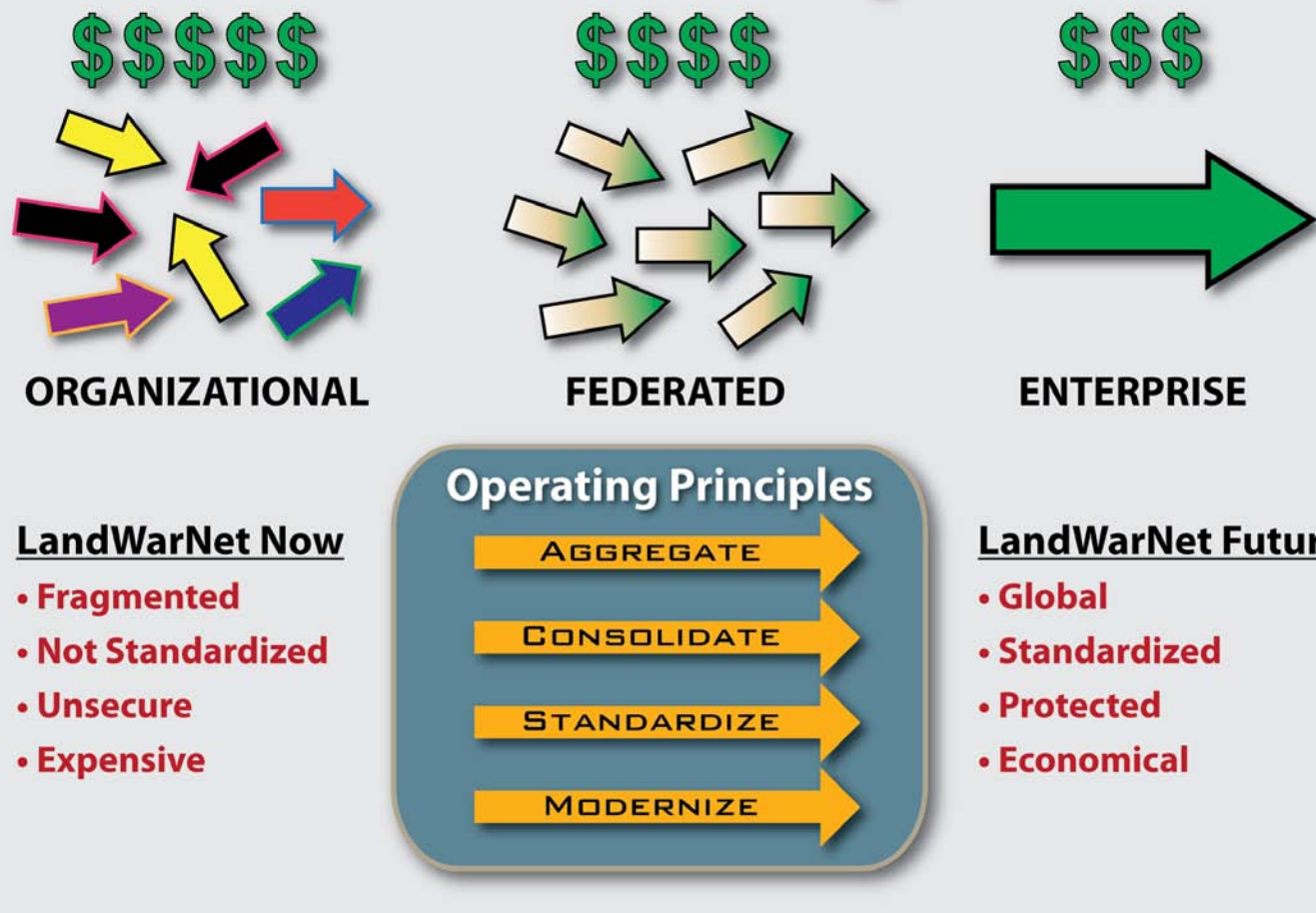
focus and integrate all Army network resources to support the Army, joint, and national strategies, such as the Army Campaign Plan, DoD GIG 2.0, and the National Military Strategy.

This vision promotes a centralized management, decentralized execution approach to operations. Ultimately, the GNEC will become an enabler by effectively linking our generating and operational forces from home station through training for and conduct of operations in the Combatant Commands' AOR and back again to home stations.

### Army GNEC Strategy Map



# LandWarNet Enterprise Plan



**GNEC Mission:** LandWarNet transformation to deliver timely, trusted, and shared information. Create an environment where innovation and service empowers Army and mission partners through an unsurpassed responsive, collaborative, and trusted information enterprise.

GNEC establishes an end state where a single, ubiquitous global network enables all dependent Battle Command and Generating Force capabilities and activities in the preparation for war, the transition to war and throughout all phases of full spectrum operations. GNEC will dramatically improve network defense, realizing efficiencies while improving effectiveness, and ensuring Army interoperability across the DoD. In the end, all Army generating force networks will be managed by a single command authority [NETCOM/9th SC(A)] organizing Army information and services that are globally accessible, useful and secure for Soldiers deployed anywhere in the world.

**GNEC Core Objectives:** GNEC near-term focus will resolve specific LandWarNet capability gaps that: (1) establish new procedures to operationalize LandWarNet; (2) improve the overall security of network services and capabilities, and dramatically improve network defense posture; (3) realize economies and efficiencies while improving effectiveness;

and (4) enable Army Interoperability and collaboration with mission partners.

Long-term, the GNEC strategy will transform the operational, security, modernization, governance, and resourcing dimensions of LandWarNet to create a network enterprise that will enable all network dependent capabilities and activities in the preparation for war, the transition to war and throughout all phases of full spectrum operations.

Transforming LandWarNet to a Network Enterprise adheres to four operating principles: (1) **Aggregate:** Collect or aggregate all data regarding IT assets, infrastructure, operations and governance (what we have now); (2) **Consolidate:** Make best use of collected data and systems by way of federation (make use of agreed standards, still allow organizations to manage their own systems and networks); (3) **Standardize:** Achieve a common technical and operational picture to ensure like-capabilities and services are delivered seamlessly across the enterprise network; and (4) **Modernize:** Systems and operations. These operating principles are not necessarily executed sequentially — these activities can and will happen in parallel.

## IV: TRANSFORMING LANDWARNET

### Operationalize LandWarNet to Enable Global Warfighting Capabilities

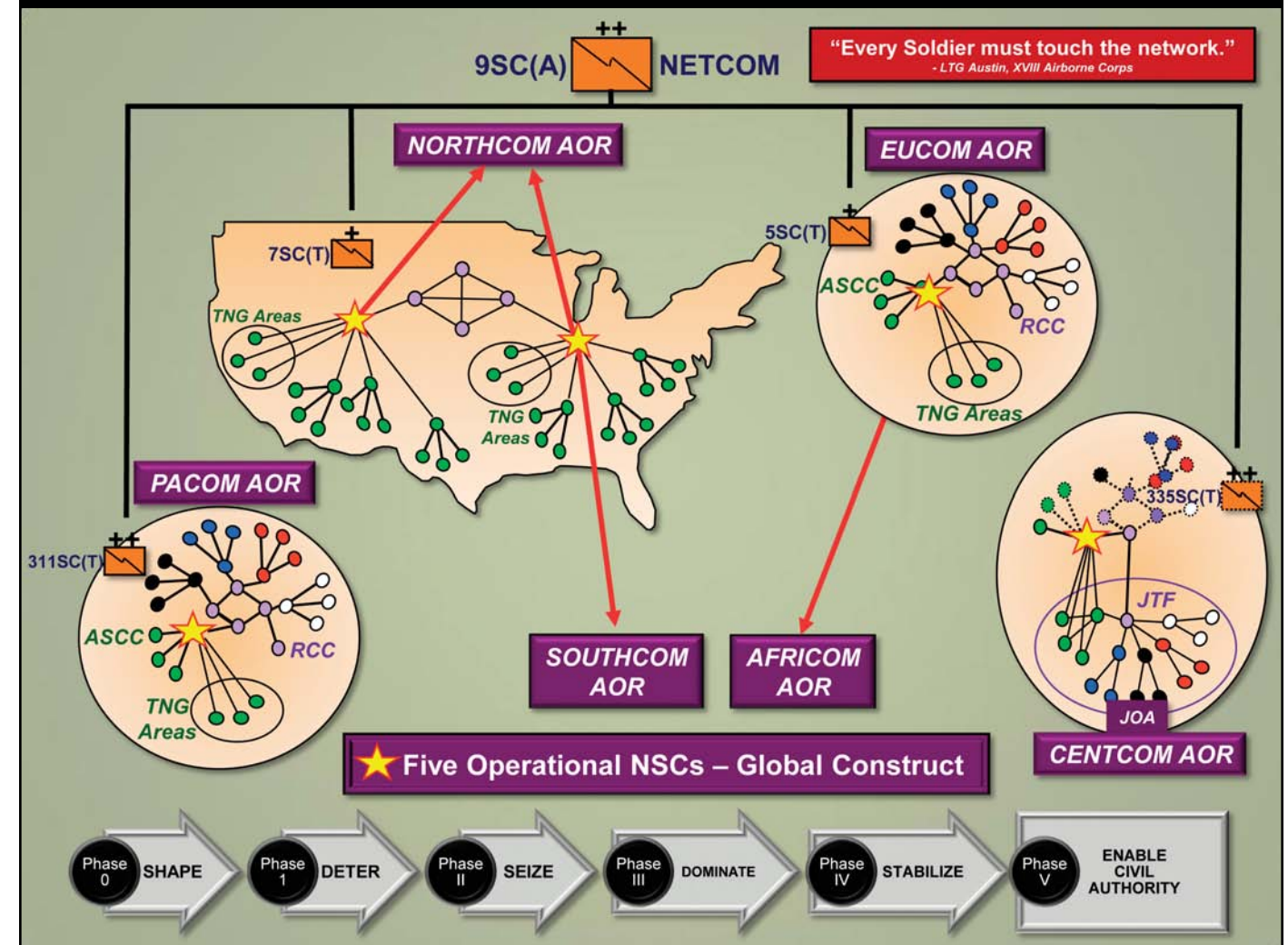
**G**NEC will operationalize LandWarNet through Army Network Service Centers (NSC). The NSC provides Warfighters connectivity — a global plug and play ability to connect to Army, Joint and commercial networks through all phases of joint operations.

The NSC also centralizes Network Operations of the LandWarNet Enterprise under a single entity to make it less vulnerable to attack and achieves IT resource efficiencies. The NSC transitions the Army's Battle Command and collaboration applications and services out of the command post and individual installation, where they are marginalized, into the enterprise where all they are available to commanders and Soldiers anywhere in the world. The NSC provides the

key connectivity interface between expeditionary operating forces and the resources of the generating forces, while GNEC provides the strategy/initiatives, including NSC, to transform LandWarNet. Supporting the NSC Construct are governance policies and activities that will create an Army-wide decision-enabling framework to ensure LandWarNet resources are managed to efficiently and effectively meet Warfighter required capabilities.

*Note: The Network Service Center itself is not a single physical place; rather, it is composed of distributed Fixed Regional Hub Nodes (FRHN), Area Processing Centers (APC) and Theater Network Operations and Security Centers (TNOSC) supported by a Service desk.*

### Enhancing Warfighting Capabilities



## NETWORK SERVICE CENTER CONCEPT

**General:** The Network Service Center (NSC) is an Army global enterprise capability that links LandWarNet to the Warfighter. The GNEC conceptual approach is a global enterprise linked by five operational NSCs (and additional NSC to support training hosted by the Signal Center at Fort Gordon).

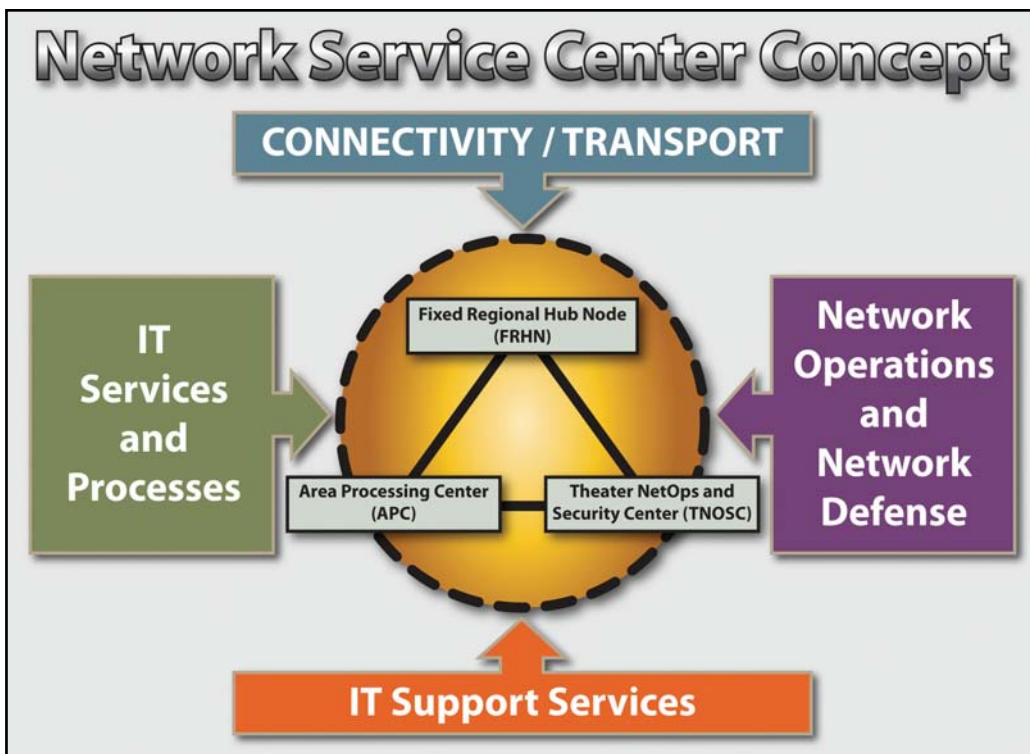
Each of the five currently planned NSCs consists of three major geographically dispersed capabilities: (1) **APC**. APCs are enterprise facilities that will provide standardized global enterprise Battle Command and collaboration services. (2) **FRHN**. FRHNs are high bandwidth satellite to fiber gateways that connect Army expeditionary operational forces to the Global Information Grid (3) **TNOSC**. TNOSCs are forward deployed, theater-based facilities that provide Network Operations (NetOps) and Service Desk functions to ensure the seamless delivery of standardized enterprise services. TNOSCs represent the Army's key LandWarNet cyber defense capability under the control of the Army's Global Network Operations and Security Center and, ultimately in support of overall DoD global network operations centers.

The NSC addresses a key capability gap between the Army's operational and generating forces and delivers seamless LandWarNet capabilities to each during day-to-day operations, training, simulation, emergency response, and wartime operations.

### NETWORK SERVICE CENTER (NSC) OPERATIONAL CONSTRUCT

The NSC leverages current and future enterprise resources, including network access, equipment, and personnel to deliver a synchronized, seamless, information capability in support of the Army's transformation to a network-enabled, modular, expeditionary force. NETCOM/9th SC(A) is the Army's global Network Enterprise command and provides authoritative oversight and coordination to ensure intra- and inter-theater support and synchronization. 9th SC(A) will implement a NSC construct through the respective Signal Command (Theater). NSCs provide the Command and Control to enable, manage, and protect the Army's LandWarNet Joint Information Environment.

As future combat operations are likely to be executed by task-organized joint military forces in a Coalition environment, it is critical that Army network enterprise solutions sup-



port this role. The NSC will provide direct support to Army, Joint, and Coalition forces, Agencies, and Nongovernmental Organizations (NGO) in order to enable the Combatant Commander's plan through information superiority.

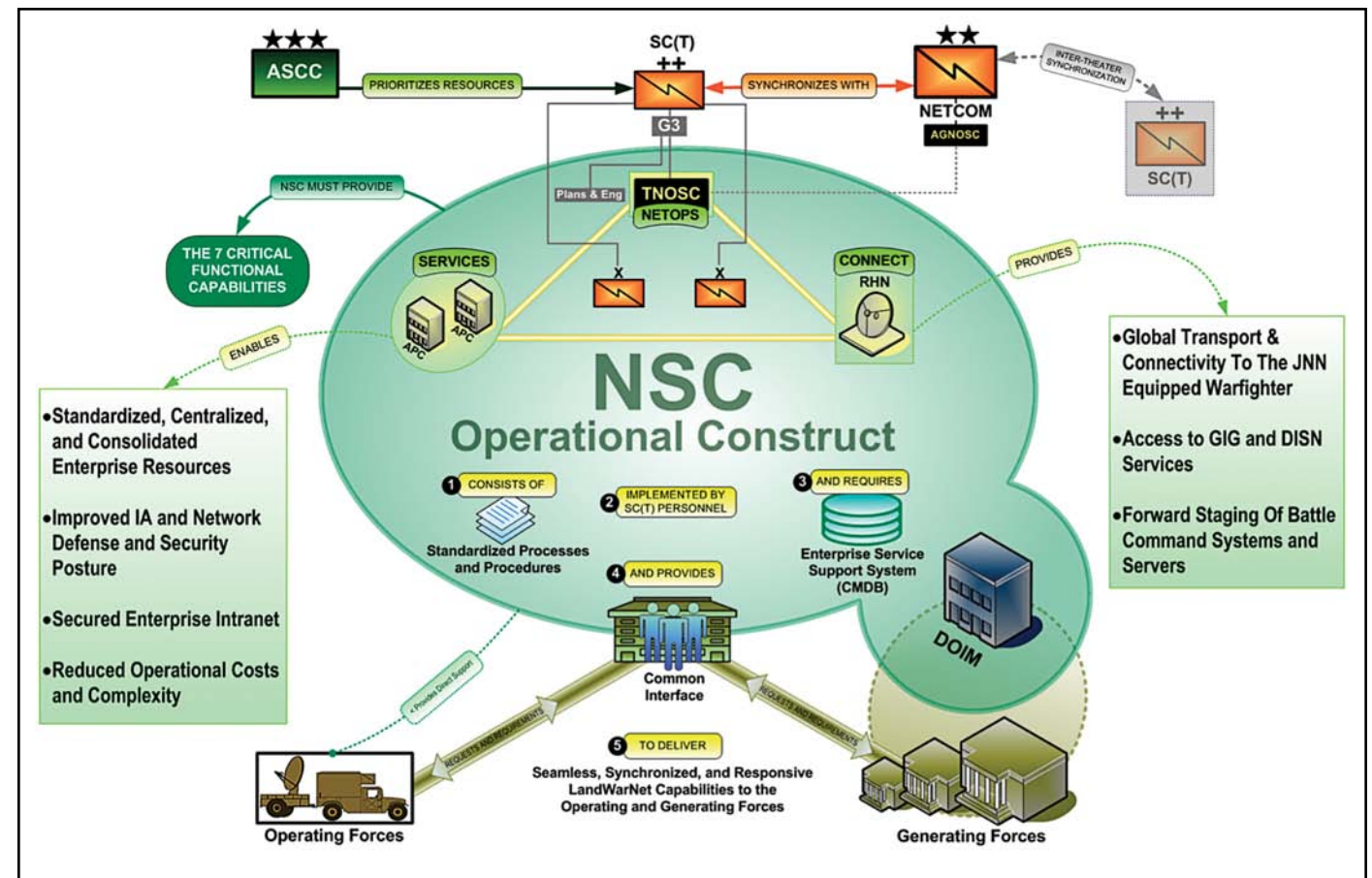
The implementation of the NSC Construct will increase operational performance and reliability, provide needed agility to respond efficiently and effectively to change, and allow for economies of scale in terms of operations and maintenance costs.

The Army will achieve a number of distinct operational benefits and improvements when NSCs are implemented with the GNEC approach. These include:

- A single point of contact within each theater for access to LandWarNet enterprise services and functional or mission-specific generating force information resources.
- Reduced forward-deployed equipment footprint, enabled by the ability to reach-back both in theater and across theater for network enterprise services and capabilities.
- Enhanced operational and generating force network information security posture.
- A single global service support capability to assign and track actions taken to provision IT services that support the Warfighter mission.
- Use of standardized, common, and repeatable applications that are designed to increase speed and responsiveness of the network through processes.
- Enhanced battle command capabilities through improved delivery of services in all locations and phases of operation.

## IV: TRANSFORMING LANDWARNET

continued



- A synchronized, seamless, information capability that effectively and efficiently supports the transition of operational army units across deployment phases and locations.
- A true "plug-and-play" environment developed from common standards ensuring interoperability that is globally accessible to the Warfighter.
- A consistently available, "always on" connect capability dramatically increasing operational force responsiveness to the JFC.
- Network modeling and simulation capabilities and services provided to operational units in support of both the planning and execution of their missions.

### AREA PROCESSING CENTER (APC)

The APC is a global enterprise information processing component of the NSC construct and is critical to the successful implementation of the NSC. Establishing APCs is the initial step in maturing the LandWarNet Enterprise that includes enhanced enterprise data management and application and services warehousing initiatives. APCs are located in sanctuary areas and extend common enterprise and mission services globally

### FIXED REGIONAL HUB NODE (FRHN)

The FRHN is a global enterprise component of the NSC construct and provides the Warfighter a satellite to fiber interface that connects deployed operational forces to global Army, Joint and commercial network capabilities. The FRHN is the deployed force conduit to enterprise Battle Command and network service capabilities. Each of the planned five FRHN facilities is capable of supporting up to three Army divisions, or two divisions and five separate organizations (e.g., expe-

## Area Processing Centers (APC): Currently Active / Others TBD



ditionary Brigade Combat Teams (BCT), support brigades, or Marine Air Group Task Force (MAGTF) Marine Corps Enterprise Information Technology Services (MCEITS) units.

Five FRHNs are currently planned at strategic locations to provide worldwide coverage. Locations for the FRHNs are Europe, SWA, Pacific, and two in the Continental United States. The Army currently has two operational FRHNs. The Army currently has two operational FRHNs in support of CENTCOM,

either global or regional network technical oversight (enterprise content, spectrum and help desk management); NetOps situational awareness, bandwidth management and the management of Information Assurance and network security for the theater. The Army's modular force structure has flattened the Army's NetOps architecture and the TNOSC is the lynchpin of Army global NetOps, management and security through all phases of operations. The TNOSC is the centerpiece of the Army's *Cyber Operations Defend the Network Strategy* and

## Fixed Regional Hub Nodes (FRHN): 5 Planned Locations World Wide



ECUOM, and AFRICOM AORs that support deployed Army and USMC forces. The CONUS FRHNs and the Pacific FRHN are scheduled to attain IOC by FY10 and FY11 respectively.

### GLOBAL/THEATER NETWORK OPERATIONS AND SECURITY CENTERS

Network Operations and Security Centers (NOSC) are a global enterprise component of the NSC construct. It represents the Army's primary LandWarNet NetOps capability with strategically placed TNOSCs supporting their respective COCOMs. Organized under NETCOM/9th SC(A), each NOSC provides

works in concert with other Army, Joint and agency Cyber Operations centers of excellence to defend LandWarNet.

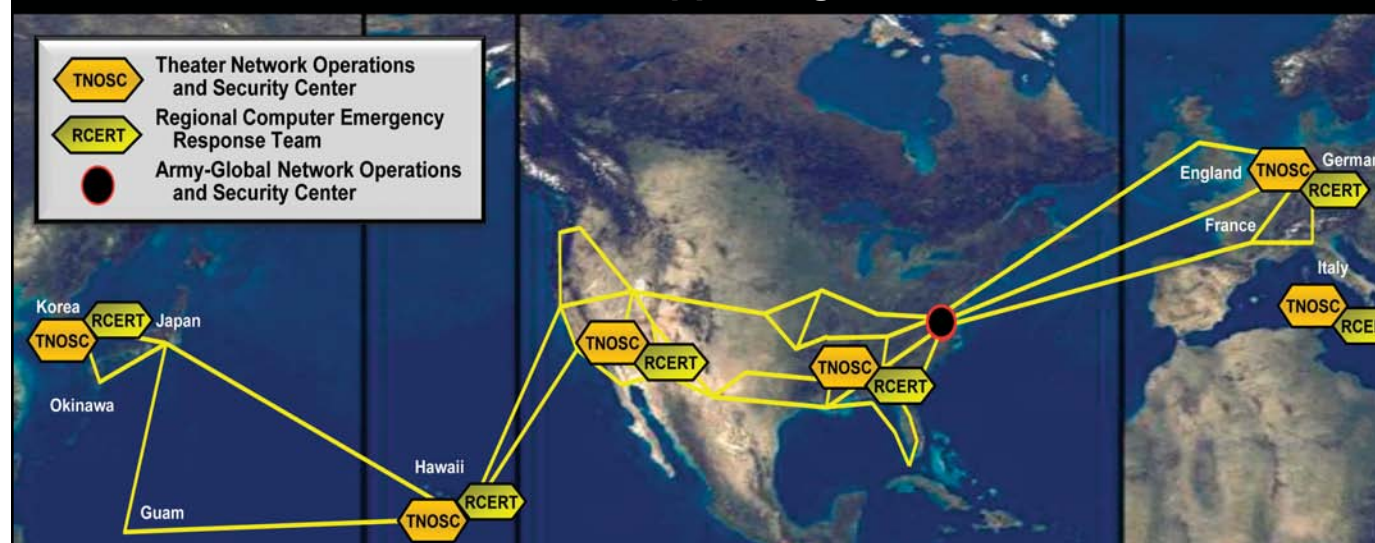
The global NOSC structure is a tiered construct with the top tier being the Army-Global Network and Security Center (A-GNOSC). The A-GNOSC is the entry point for execution of Global NetOps.

The second tier consists of six TNOSCs, (2) in CONUS, (1) Europe, (1) Pacific, (1) in Korea, (1) in SWA and are under the operational control of an Army Service Component Command with NetOps responsibility under the control of

## IV: TRANSFORMING LANDWARNET

continued

### 6 TNOSC / RCERT Locations Supporting COCOM AORs World Wide

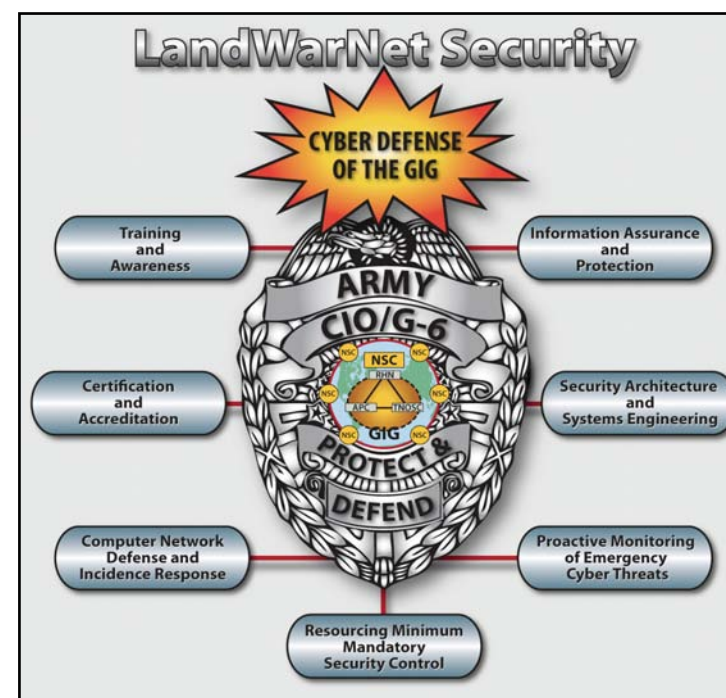


the A-GNOSC. Each of these NOSCs is directly supported and integrated with Army Computer Emergency Response

Teams (CERT) creating a consolidated Cyber NetOps Center.

## IV: TRANSFORMING LANDWARNET

### Dramatically Improve Network Defense Posture



LandWarNet Protection: Numerous threats to LandWarNet exist in the operational environment. Protection of the LandWarNet is achieved through the active and passive measures that protect against, monitor for, detect, analyze, and respond against malicious and non-malicious, unauthorized activity through Army cyberspace. It denies adversaries and others the opportunity to exploit vulnerabilities for their own purposes. The secure and uninterrupted flow of information allows Army forces to multiply their combat power and synchronize with other Joint capabilities.

Protection is one of the main activities mentioned as part of the 8 October 2008 official DoD definition of Cyberspace Operations and it is intrinsically linked to another major component of Cyberspace Operations – those activities required to operate the LandWarNet. Protection activities include: 1) budgeting for and implementing minimum mandatory security controls; 2) training and awareness; 3) certification and accreditation; 4) security architecture and systems engineering; 5) Information Assurance and protection; 6) computer network defense and incident response; and 7) proactively monitoring emerging cyber threats in coordination with the intelligence community.

Through LandWarNet Protection, the Army CIO/G-6 sets direction and strategy for the development and implementation of Army-wide Network Enterprise security and privacy policy, standards, guidelines and procedures to ensure delivered services are in accordance with federal laws and policies. Championing LandWarNet protection as a tenet of GNEC ensures that the transformation of LandWarNet leads the way in enabling Army cyberspace operations efforts, and complies with mandated and legislated requirements.

In this new cyberspace battlefield, new operational thinking is required. The Army is actively developing plans to support the U.S. Strategic Command's Implementation-Plan (I-Plan) to execute the National Military Strategy for Cyber Operations.

The I-Plan identifies 42 tasks (10 critical) and the responsible organizations and milestones that will lay the groundwork for achievement by the Department of Defense of its strategic goal of U.S. military superiority in cyberspace.

The Army's Network Operations and Security Centers, both Global and Theater, directly supported by their respective Regional Computer Emergency Response Teams (RCERT), are the centerpieces of the Army's Cyberspace Operations "Operate and Defend the Network" strategy. The Network Operations and Security Centers work in concert with other Army, DoD, and National Cyberspace Operations Centers of Excellence to defend LandWarNet.

## IV: TRANSFORMING LANDWARNET

### Realize Economies and Efficiencies While Improving Effectiveness

#### GNEC – "INFORMATION SERVICES TO THE EDGE"

As stated in FM 3-0, "Information is a powerful tool in the operational environment. In modern conflict, information has become as important as lethal action in determining the outcome of operations." In the physical realm, every engagement, battle, and major operation requires complementary information to both inform and influence audiences within the operational area; it is an element of combat power against enemy command and control and is a means to affect enemy morale. It is both destructive and constructive.

Warfighter information services must work in austere, tactical environments in the same fashion they work at home station; yet today many information services are designed to work in robust network architectures and often do not scale down to the deployed user. This separation between home station and deployed capabilities requires the user to ineffectively and inefficiently transition from garrison IT services to tactical IT services, often losing functionality in the deployed environment.

Achieving and maintaining an information advantage down to the tactical edge as a critical element of combat power requires a concentrated effort in order to provide a single, seamless information environment optimized for the Warfighter. For example, 7th SC(T) will implement GNEC by providing CONUS-based operating and generating forces assured availability to and reliability of core enterprise information services throughout full spectrum operations. Core enterprise information services consist of collaboration, applications, messaging, discovery, mediation, enterprise service management, user assistance, and storage.

One component of GNEC "Information Services to the Edge" is Army enterprise data management and warehousing. Enterprise data management and warehousing will allow the Army to achieve a single authoritative source for all data

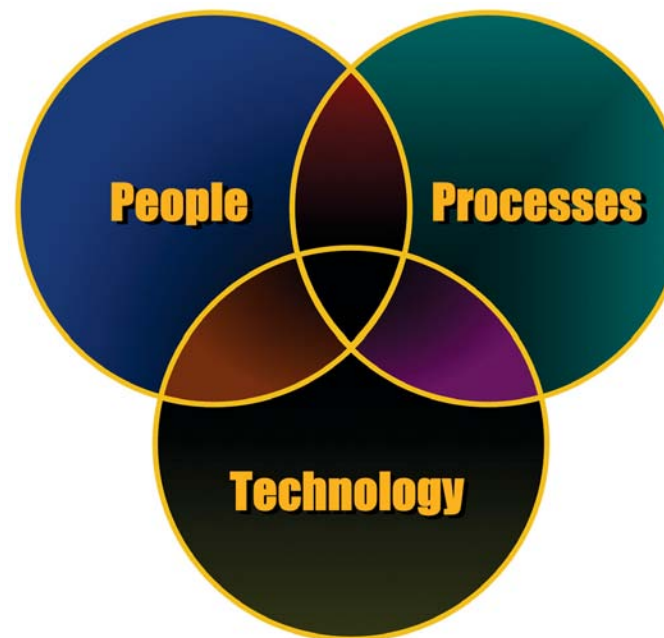
while reducing the number of data centers and computer rooms — reducing risk, providing improved service, and subsequently better defending Army data. It will move the Army to a single standard set of technologies and facilitate the retirement of legacy systems and applications. Providing "information services to the edge" will enable seamless interaction and knowledge transfer across functional, tactical, institutional, and organizational units; and support the goal of the GNEC strengthening the Army's ability to operate in JIIM environments.

#### GNEC – COMMON POLICIES/STANDARDS AND GOVERNANCE

The CIO/G-6 is responsible and accountable for the standardization, compatibility, interoperability, security and fiscal discipline of LandWarNet. Establishing strong, unwavering strategic partnerships is essential as LandWarNet capabilities and services impact all business processes, warfighting capabilities, and subsequently, all Army organizations. The strategy objective is to deliver LandWarNet capabilities and services for policy makers, Warfighters, and other decision-makers by improving Army IT business operations and their integration with Army and DoD business processes within the Joint enterprise.

**Common Policies and Standards:** GNEC will initiate common policies and standards that ensure the LandWarNet provides seamless end-to-end information services. These common standards will ensure systems are developed, tested, certified and deployed with end-to-end enterprise commonality. This concept does not imply a one size fits all approach to IT systems but rather one set of technical interface standards to ensure seamless interoperability of IT systems across the force. This effort will provide effective enterprise direction for data standards, information service standards, acquisition, certification, and enforcement to ensure the seamless flow of information between all Army and mission partner users and systems.

## IV: TRANSFORMING LANDWARNET continued



IT Service Management – People, Processes and Technology

To meet this challenge the Office of the Army CIO/G-6 is adopting best business processes that enhance the management of the Army's information enterprise to improve LandWarNet capabilities delivery. We must collectively strive to raise the bar in obtaining a new gold standard for Federal CIO organizations. Through GNEC, the Army is pursuing unprecedented levels of enhance warfighting operational effectiveness by enforcing *standardization, compatibility, interoperability, security, compliance, and fiscal discipline* of the Army's LandWarNet capabilities and services.

GNEC will: (1) deliver structured, controlled, repeatable, measurable processes that drive accountability and compliance for the management of the Army's information enterprise; (2) provide data-driven decision-making; (3) deliver LandWarNet capabilities and services to Army leadership and Warfighters; and (4) enable rapidly changing operational requirements for Army and Joint missions. The value to the enterprise will be disciplined IT investments, integrated enterprise activities, increased LandWarNet security, and synchronized capabilities delivery.

Information Technology Service Management (ITSM) is the management and execution of all activities required to provide enterprise IT services. The emphasis is on alignment of IT services to the warfighting and business objectives in an optimally cost effective manner. ITSM is an all-inclusive, holistic approach to managing IT components, processes, and services Army-wide. The focus of the Army CIO/G-6 IE Strategy is enterprise ITSM — *People, Processes and Technology* — that improves the Army's ability to reconcile current to future force

LandWarNet capabilities and services and optimizes critical IT resources. People, processes, and technology aspects must be integrated with a holistic approach. They are not mutually exclusive and their components must all receive equal consideration to be successful.

The LandWarNet components including; user access and display devices and sensors, networking and processing, applications and services, and related transport and management services will be governed by common policies and standards.

**Governance:** GNEC includes five Enterprise IT Governance focus areas: (1) *Strategic Alignment* synchronizes Army LandWarNet strategies and policies to Army operating and generating force required network capabilities. (2) *Value Delivery* requires decision-makers to provide to the Network Enterprise disciplined LandWarNet investments, integrated enterprise activities, increased LandWarNet security, and Army Force Generation (ARFORGEN) synchronized capabilities delivery and services: (3) *Risk Management* requires implementation of a continuous process that identifies risks (impact on assets, threats and vulnerabilities); and once identified, mitigates the risk by countermeasures (control). The performance of the risk mitigation process (including risk acceptance) should be managed, i.e., measured and monitored; (4) *Resource Management* guides the Army when providing quality human and non-human resources, which increase the effectiveness of personnel hiring and retention, and IT



procurement right sourcing; (5) *Performance Measurement* enhances the Army's ability to measure and manage its budget, services, delivery capabilities, and generally promote effective and efficient operations.

Using an Enterprise IT "Tiered Decision Model" Governance Framework enables the Army to strengthen IT decision-making and align IT strategy, systems, and processes to the Army's operating and generating force strategies and capabilities. *IT Enterprise Governance is not a standalone IT process; it is syn-*

# IV: TRANSFORMING LANDWARNET

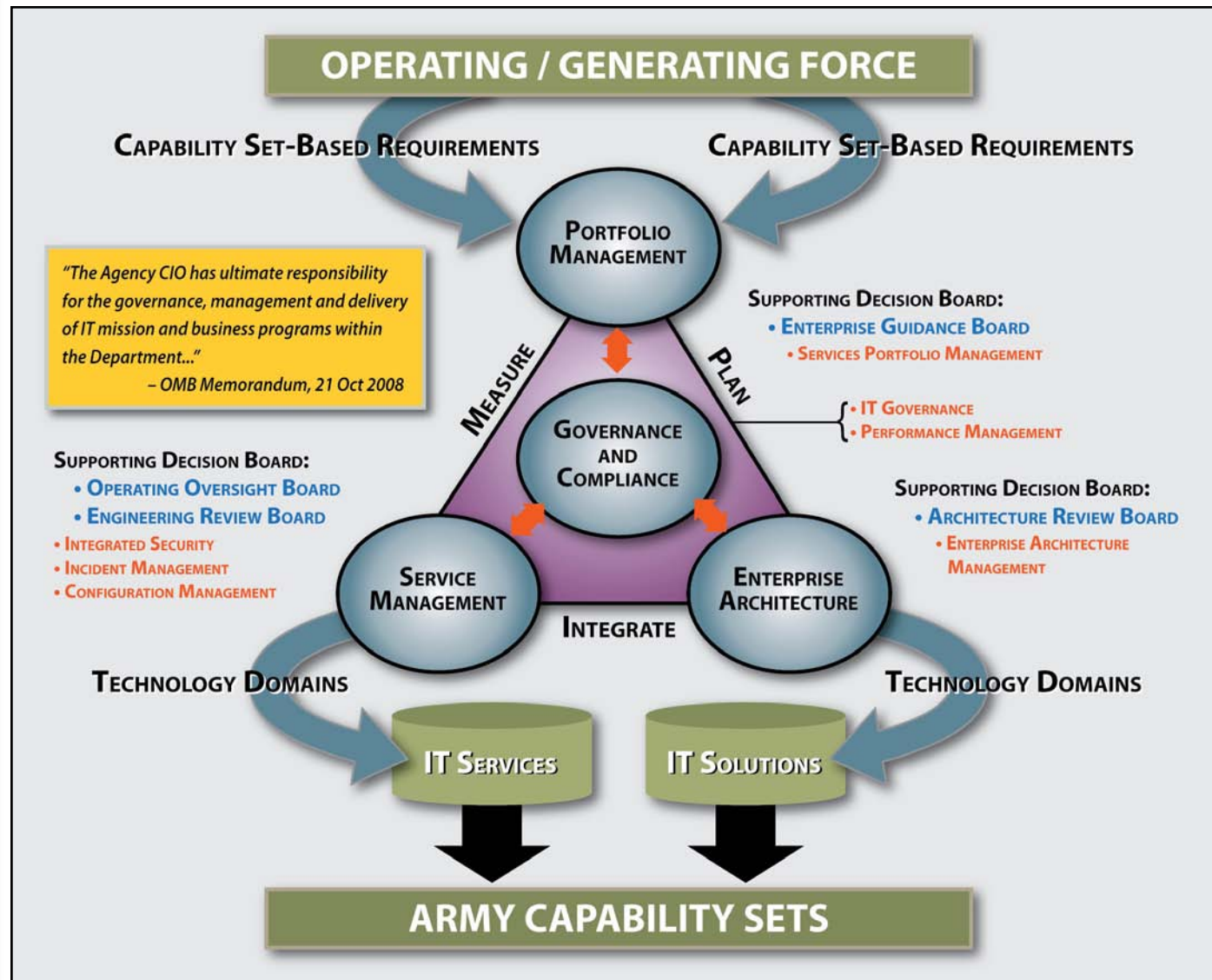
## Enable Army Interoperability and Collaboration with Mission Partners

In this era of persistent global conflict, Army Warfighters must freely exchange information routinely with joint, interagency, intergovernmental and multinational (JIIM) partners that span from the generating force to the tactical edge. The Warfighter must deploy and connect no matter where they are located, pull information needed for their missions, and be given timely, accurate information on any threats they may face. A Warfighter's ability to leverage the right information at the right time is the difference between mission success and mission failure. Therefore, it is no longer sufficient for the Army Network Enterprise to provide segments of the network that are independently developed and managed if these conditions are to be met. The network enterprise must be seamless between the sustaining base and the tactical edge to enable operational agility. This translates into the need for enterprise wide systems engineering, a common strategy and architecture, a single concept of operations for network operations, configuration control, and situational awareness that comprehensively spans the sustaining base to the tactical edge. This requires the Army to adopt innovative ideas and processes to deliver capabilities and services that our forces are able to use with agility. Through GNEC, the

Army will enforce standards, processes, and architecture for data accuracy; increase the speed and flexibility of delivering capabilities and services; and tailor oversight and governance to be commensurate with risk. The intent of transforming LandWarNet is simple — close the gaps between the availability of technologies; field them for warfighting advantage; and sustain the advantage for Warfighter decision superiority.

As we transition to a single network enterprise authority, Network Enterprise, NETCOM/9th SC(A) will aggressively develop and implement measures to manage and defend LandWarNet to ensure warfighting forces, including partners and allies, can deploy and connect globally, and share timely, trusted, and accurate information needed for their missions. LandWarNet will design, implement, operate, and sustain LandWarNet for maximum mission assurance in the face of kinetic or cyber attack. Policy and implementation instructions for security certification and accreditation will support the fast paced, often ad hoc, on demand nature of net-centric operations and warfare. The GNEC strategy to transform LandWarNet will provide a single, seamless information environment optimized for the Warfighter.

*"We, as a MEU, had very diverse missions during this deployment, [which] separated the commander from the combatants ashore, but by using the Arifjan Earth Terminal Complex we were able to ensure reliable, fast communications between the commander and his Marines." — SGT Daniel Finein, USMC, 13th MEU*



chronized with and compliments the Army's existing governance structure.

Enterprise IT Governance is the component of GNEC that ensures direction-setting, decision-making, and that Information Enterprise oversight boards are established; and, if necessary realigned, to ensure the Army LandWarNet Enterprise objectives are achieved. The integration of governing and advisory bodies will improve: (1) guidance on Army LandWarNet activities; (2) accountability and effectiveness of Army Network Enterprise programs and operations; (3) issue resolution that assures representation of operating and generating force customers; and (4) improve the effectiveness and efficiency of the Army's LandWarNet enterprise activities and service delivery within GNEC. The key objective is to achieve a synchronized approach and execution of Network Enterprise activities and services Army-wide.

### GNEC – RESOURCE MANAGEMENT

In recognition of the importance of GNEC, the Army made an initial investment in NetOps capabilities during the 2009 mid-

year review. This investment provides significant resources to close Computer Network Defense (CND) gaps in the CONUS network, and to provide for standardizing critical network management tools to facilitate the further federation and consolidation of the LandWarNet. As the Army moves forward toward fully realizing the benefits of GNEC, resourcing will often be based on our ability to identify off-setting costs in existing programs and more efficient delivery of services based on transformed business processes. Efficient transformation will not occur without a concerted effort from the C4/IT community focused on adopting best business practices and building a "trusted services environment."

The CIO/G-6 will utilize a series of Business Case Analyses (BCA), focused at the initiative level, that will identify current business processes and resources, and contrast this "as is" case with the future "to be" case for guiding the Program Objective Memorandum (POM) 12-17 resourcing process. Our BCA process will rely heavily on the continuing efforts with the Army Budget Office, Army Audit Agency, and NETCOM/9th SC(A) to aggregate IT asset, contracting, and resourcing the current information network enterprises.



## GNEC – FORCE GENERATION

The future Modular Force will fight as a part of a networked joint force, integrated at every level, and interdependent in the joint areas of battle command, force projection, air and missile defense, sustainment, and fires. The strategic environment and demands of Soldier-centric, network-enabled expeditionary operations will significantly increase network reliance.

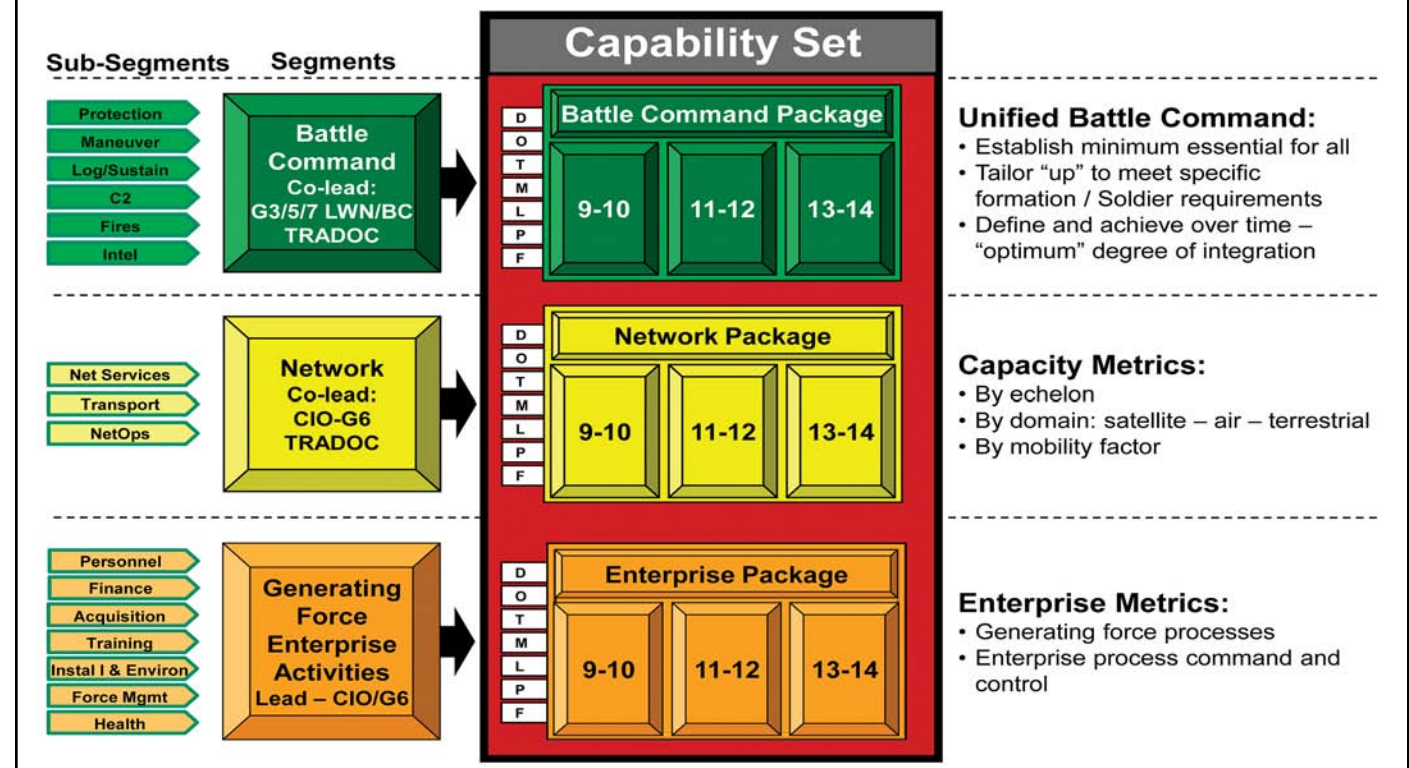
Although LandWarNet currently enables various operational and generating force capabilities, there are significant capability gaps for Army units as they prepare and deploy during the Joint Phases of Operations. LandWarNet enterprise enabling capabilities are limited because of multiple networks, applications and services that are independently managed, and tied to fixed base infrastructure. Several Army networks are not integrated either in the same infrastructure or at the operational command post. This not only complicates C2 for the commander but limits the capability to share information such as common operating picture (COP) and Situation Awareness (SA) with Joint forces and coalition partners. Additionally, LandWarNet operational functionality currently does not fully support the commander's critical needs such as joint distributive planning, virtual task organization and sharing vital mis-

sion critical information while preparing for and deploying to a theater of operations.

The ARFORGEN process when fully implemented across the entire Army will allow GNEC to introduce new LandWarNet infrastructure capabilities to a unit during a "Reset" period. Once these new LandWarNet enterprise capabilities are fully incorporated into the unit, the unit then progresses to a "Train/Ready" state, and finally an "Available" state at which time the unit is fully mission ready and can be deployed to execute an operation or mission. To meet these challenges, LandWarNet is integrated into a portfolio construct that facilitates the synchronization, coordination and prioritization of all LandWarNet and Battle Command activities across the entire force.

The Army CIO/G6 [and NETCOM/9th SC(A)], in conjunction with the Deputy Chief of Staff, G-3/5/7 LandWarNet/Battle Command (LWN/BC), and TRADOC, is transforming Army processes to deliver relevant, affordable, and interoperable LandWarNet/BC infrastructure capability sets to the Generating and Operational Forces within the ARFORGEN process – modernizing net-enabled capabilities over time. The LWN/BC Capability Sets Development Strategy estab-

## Capability Set – Portfolio Framework



## ARFORGEN IS THE "DRIVE TRAIN"



lishes deliberately planned capability increments or sets, transforming LandWarNet into an enterprise managed activity that effectively and efficiently delivers trained and ready expeditionary forces in a deliberate, synchronized method within the ARFORGEN process.

The challenge is to effectively synchronize its systems engineering activities to deliver affordable and interoperable infrastructure capabilities to the designated ARFORGEN units as a Capability Set. LWN/BC Capability Sets are designated in two year increments and will be the basis for fielding capabilities to the Army within the ARFORGEN. A LWN/BC capability set portfolio is comprised of all the new and existing DOTMLPF solutions inclusive of all LandWarNet segments.

GNEC's role is to ensure delivery, relevant, affordable, and interoperable LWN/BC capabilities sets to the Generating and Operational Force within the ARFORGEN process — over time. This System of Systems portfolio approach built on the development of Capability Sets for modular formations to synchronize and integrate all generating force processes to incrementally deliver improved capabilities over time.

### GNEC – DATA MANAGEMENT AND DATA WAREHOUSE

The need for centralized data processing arose from the realization that Army's predominantly decentralized computing environment had reached unsustainable levels from operational, financial, technological, and security perspec-

tives. Implementing enterprise data management and warehousing will increase operational performance and reliability; introduce standardization, provide needed agility to respond efficiently and effectively to change, enhance security, and allow for economies of scale in terms of operations and maintenance costs. Centralized data processing will also enhance cyber security and information protection, secure and non-secure, and will enable the Army to more effectively implement continuity of operations and disaster recovery planning.

Army enterprise data management and warehousing allows the Army to achieve a single authoritative source for all data while reducing the number of data centers and computer rooms to more effectively manage IT operations. Enterprise data management and warehousing will move the Army to a single standard set of technology, facilitate the retirement of legacy systems and applications, and allow for standardize, compatible and interoperable connectivity to the GIG.

Due to the size and scale of the Army's LandWarNet, It is crucial that that the Army implements a more efficient data processing environment that maximizes opportunities for knowledge transfer and security. Managed virtual data and information architectures must be provided and storage architecting strategies are required to present mission data and information in effective and consumable ways to Army and partnering joint, interagency, intergovernmental and multinational (JIIM) warfighting and business communities. Traceable data elements must be available to both communities to enable decision superiority.

## V: LANDWARNET IN THE 21<sup>ST</sup> CENTURY

### GNEC – LOOKING FORWARD

The Army has made tremendous progress in transforming LandWarNet to an enterprise capability and improving its ability to provide battle command and collaboration capabilities to our deploying and deployed Soldiers. This is largely due to our combined efforts and those of our strategic partners across the Army. As always, our Army is globally deployed and operating in a period of constant change politically, fiscally, and operationally. That is not going to change in 2010 and beyond. We must be vigilant, involved, and flexible to build on the momentum we achieved in 2009 and provide the best network capability available to our Army and our soldiers. In 2010, we will operationalize LandWarNet as the Army Enterprise Network to function across the operational, resource, and governance dimensions enabling network dependent capabilities as our Warfighters transition through all phases of joint operations across the full spectrum of conflict. Beyond 2010, LandWarNet will continue on the path to providing the Army a secure global cyber environment that provides seamless information superiority to support the Army's Joint, Interagency, Intergovernmental, Multi-National operational and business missions.

GNEC will position NETCOM/9th SC (A) to gain situational awareness, understanding, and unity of C2 across Army cyberspace in order to centrally manage intelligence, protection, sustainment, and information movement and maneuver warfighting functions within the LandWarNet. Network Services Centers are required to provide Warfighters anytime, anywhere, global access to the network in order to receive the right information, at the right time, and in the right format. Core enterprise information services must function as well in austere environments as they do at home station and over standard infrastructures that enable interoperability with Army and JIIM organizations. Lastly common policies and standards are necessary to enable universal processes and procedures that in the end result in the effective and efficient operation and defense of the network.

The GNEC strategy lays the foundation for a holistic environment that provides for unified communications, computing infrastructure, core enterprise services, specialized services, service delivery, and information assurance. Finally, the GNEC strategy will support all Army missions and functions in war and peace, along with supporting Army's involvement with interagency, coalition, state, local, and NGO mission partners.





Department of the Army  
**Chief Information Officer/G-6**  
107 Army, Pentagon  
Washington, DC 20310  
[www.ARMY.mil/CIOG6](http://www.ARMY.mil/CIOG6)