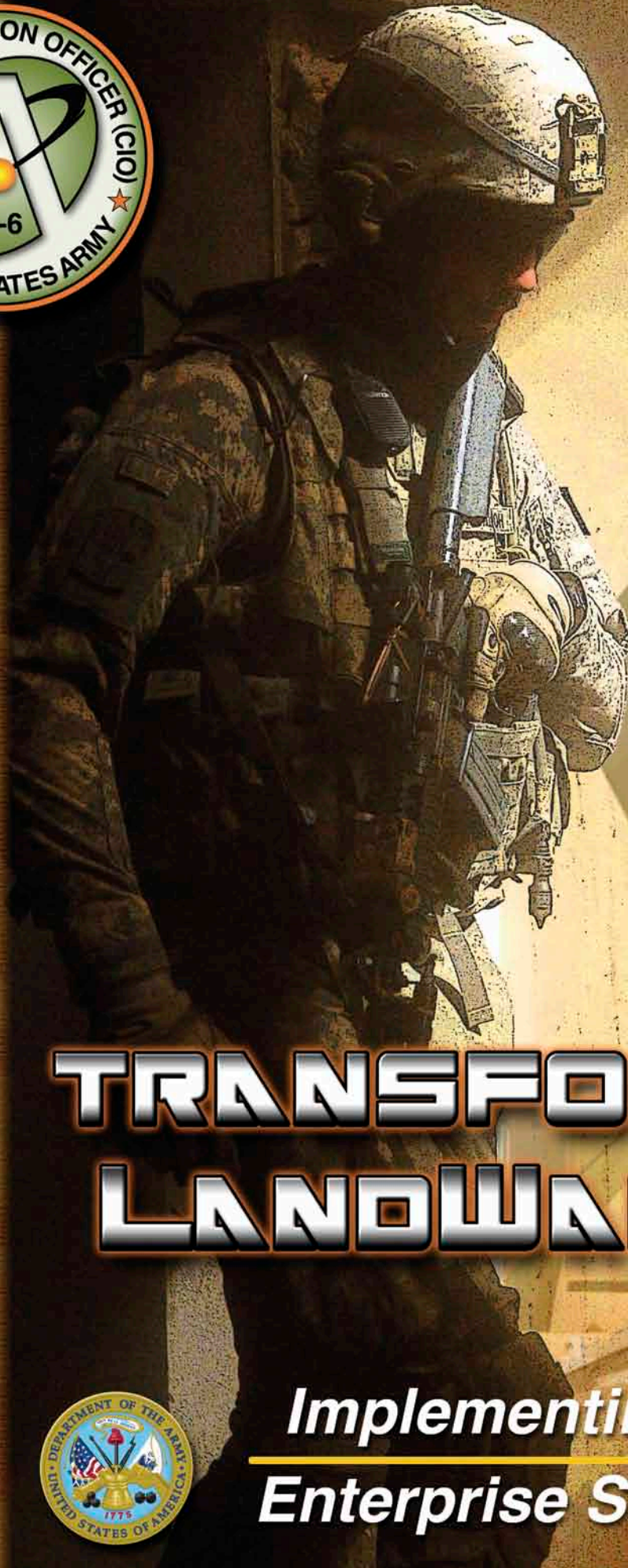




ARMY CIO/G-6



TRANSFORMING LANDWARNET

*Implementing the
Enterprise Strategy*





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: Global Network Enterprise Construct (GNEC) Update


1. On 2 March 2009, the Chief of Staff of the Army challenged the CIO/G-6 to transform LandWarNet to an enterprise architecture. We needed to lay the foundation and provide an enterprise initial operational capability in three years. This task was huge and daunting, especially given that the Army had the largest network in the world and faced an ever-changing environment. As the 2010 Army Campaign Plan notes, we are cohabiting an era of persistent conflict and complexity with an adversary who seeks to attack and destroy our nation and way of life using hybrid threats -- conventional, irregular, terrorist and criminal activity.

2. About two years ago, my staff and I introduced the Global Network Enterprise Construct as the way to grow and improve LandWarNet. In the past year, we've brought fidelity to the strategy, with detailed plans for: adopting industry standards and protocols; pursuing data center consolidation; utilizing common operational environments for different echelons in order to accelerate software application development; improving global network operations; continuing operational evaluations to define and refine our network doctrine, tactics, techniques and procedures; and standing up Army Forces Cyber command to oversee the operation and defense of Army networks. LandWarNet transformation will incorporate technological advances, customer demands, our national strategies and process improvements -- and will take into account our current fiscal constraints and the always adapting enemy. I want to highlight two particular shifts in our strategy.

a. First, our model for network defense has changed from one in which we build a citadel around our network to one of active defense in depth. The old model fails fast: it assumes a fixed network at a particular point in time to determine the security requirements for keeping the network safe; however, the environment is continuously changing, and our adversaries continuously adjusting, collaborating and maturing. Instead, we must actively engage the enemy at different places in the Open Systems Interconnection model and through multiple tiers of the network. We will use real-time, 24x7 monitoring, seeing the whole picture, conducting quick yet thorough analysis, and taking action to address abnormalities immediately -- before the enemy disrupts operations or gains access to our data.

b. The second shift entails pulling back on the reins of spending. LandWarNet transformation must be executed largely within existing programmed resources; in particular, we must reduce duplication and inefficiencies. Therefore, all IT expenditures will be under close scrutiny and intensively managed. No research and development effort or purchase that is not aligned with the LandWarNet transformation strategy will go forward.

3. I have every confidence in our Soldiers and civilians. I know they will take the mantle of innovation and change, and push as hard as possible to give our warfighters the sharpest tactical advantage possible. I salute their dedication and offer my thanks to the Soldiers, civilians and contractors of the IT and Signal community who work each and every day to make this vision reality.


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

Over the past decade, the United States' global defense posture has changed dramatically, remaking the forward-deployed Army of the Cold War into a force primarily based within our continental borders. At the same time, however, the demand for U.S. troops in operations overseas has increased dramatically, and the typical window to answer that call has shrunk. Under these new conditions, the Army's relevance to the joint commander is, and will be, measured largely by its responsiveness: How fast can the Army deploy, and can it bring its full suite of capabilities to bear within the required time frame?

More and more, the answer to that question is tied directly to the quality of the network – for every facet of the expeditionary Army's operations, garrison to the tactical edge, depends upon the network. Its functionality, agility, reliability and security define the chances for success. As the means for providing Soldiers and civilians critical intelligence, surveillance and reconnaissance information, situational awareness and ubiquitous command and control, the network can be the decisive advantage against any adversary – or it can be the Army's Achilles' heel. ■

☆☆☆ A Soldier's Story ☆☆☆

Today, one of the biggest challenges a Soldier faces is inconsistent access to the network and information technology resources, particularly during the transitions from training to deployment to return to home station. The ability to deploy on little-to-no notice and to fight upon arrival is essential to enabling the predominantly CONUS-based Army to respond effectively and rapidly to the new threat environment. Many expeditionary capabilities are network-dependent. Every Soldier should have universal access to his or her applications and data, critical ISR video feeds, command and control information, continuous position location information, mission updates, collaboration tools and training capability during all phases of the Army Force Generation cycle and joint operations. Even more basic, a Soldier should have but one email address and telephone number throughout his or her career.

The current suite of networks, information systems and IT resources does not fully support these hallmarks of an expeditionary Army. Many services and systems are designed to work within robust networks that often do not scale down to the tactical user or do not accommodate users accessing the network from home, training locations, temporary duty loca-

tions, National Guard armories or United States Army Reserve Readiness Centers. Email addresses and phone numbers traditionally change as Soldiers and units move through the phases of joint operations from reset to training to deployment. This separation between home-station and deployed capabilities often results in a loss of functionality in the deployed environment. If a Soldier (or civilian) cannot access his or her data, information or services, the network is "down" and the user can become operationally ineffective.

To make the network a decisive advantage, rather than a vulnerability, it must be developed and implemented as a holistic enterprise system, not individual piece-parts. It must be secure and standards-based, consisting of a versatile infrastructure supported by linked, redundant transport systems, into and from which sensors, warfighting and business applications, and data are fed and drawn. To enable full-spectrum operations with our joint, coalition and interagency partners, the network also must be seamless from the sustaining base to the tactical edge, and it must give Soldiers and civilians the exact information they need, when they need it, in any environment. ■

CIO/G-6 VISION, MISSION AND GOALS

- Vision:** Ensure Army and mission partners have the right information at the right time at the right place.
- Mission:** Lead LandWarNet transformation to deliver timely, trusted, and shared information. An environment where innovation and service empower Army and mission partners through an unsurpassed agile, collaborative, and trusted information enterprise.
- Goal 1:** Operationalize LandWarNet to Enable Global Warfighting Capabilities.
- Goal 2:** Dramatically Improve Network Defense Posture.
- Goal 3:** Realize efficiencies while improving effectiveness.
- Goal 4:** Enable Joint Interoperability and Collaboration with Mission Partners.
- Goal 5:** Recruit and retain an agile workforce to support an expeditionary Army

☆☆☆ LandWarNet ☆☆☆

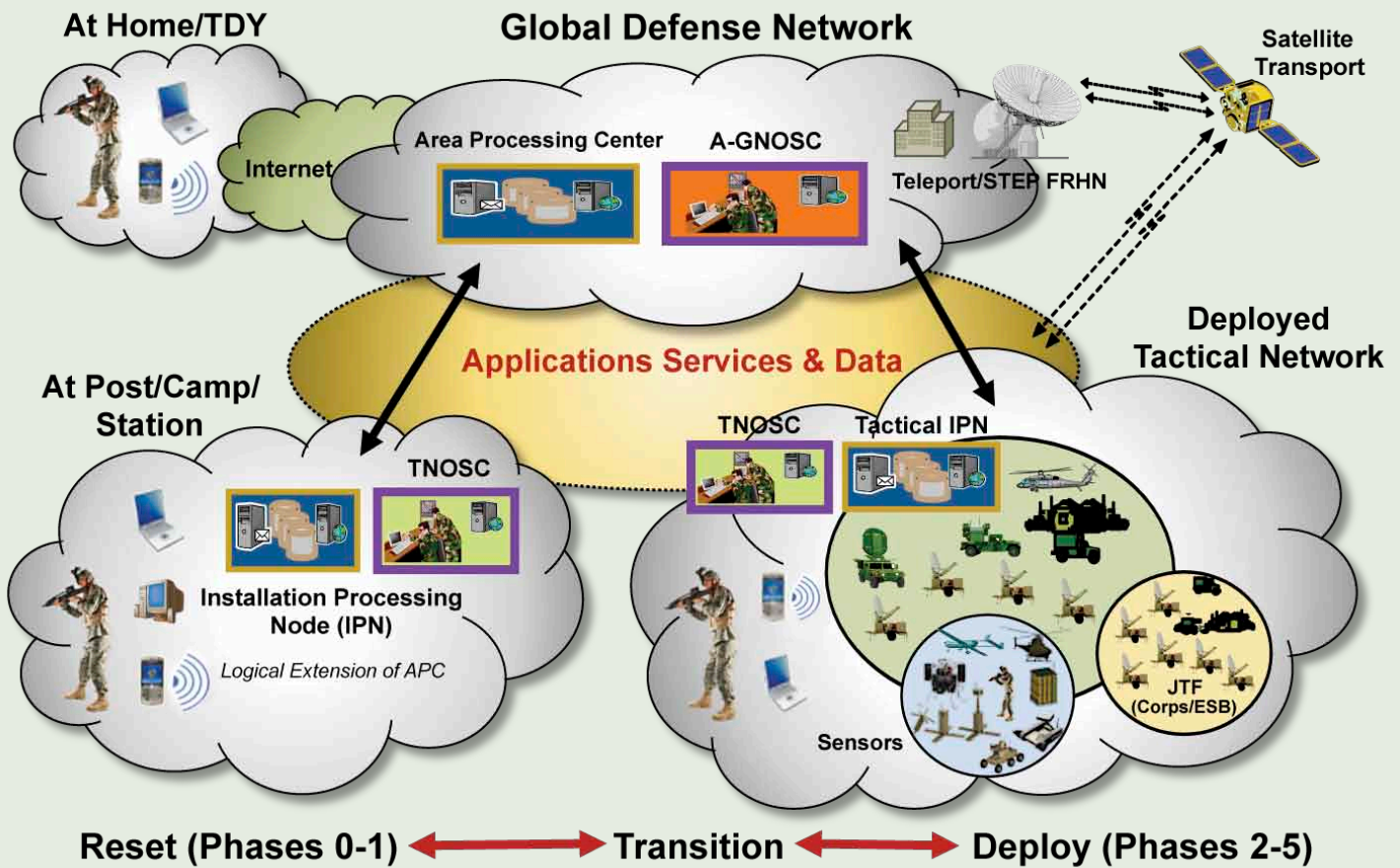
LandWarNet is the Army's solution to this enterprise network requirement, and the Army's contribution to the Global Information Grid. Though still evolving, its foundation consists of a common strategy and architecture, enterprise-wide systems engineering, a single concept of operations for network operations and configuration control. In March 2009, the Army Chief of Staff directed the maturation of LandWarNet via the Global Network Enterprise Construct (GNEC). The Army is now one-third of the way through this broad and complex three-year campaign, and the results, so far, are promising.

GNEC is best described as the focused, time-phased, resource-sensitive, Army-wide (active, Reserve and National Guard) strategy to transition LandWarNet from many loosely affiliated independent networks into a truly global capability that functions as a single integrated enterprise. In response to today's operational complexity and the growing demand

by the Army and its partners to get the right information at the right place at the right time, GNEC is particularly concentrated on network access, utilization, security and control.

Under GNEC, the desired LandWarNet end-state configuration is composed of three major components: the Global Defense Network, post/camp/station campus area networks and deployed tactical networks. The Global Defense Network includes Fixed Regional Hub Nodes, Standardized Tactical Entry Points, teleports to connect to the deployed tactical networks, Area Processing Centers that host data and applications, and the Army Global Network Operations and Security Center, which has overarching responsibility to operate and to defend LandWarNet. Campus area networks and deployed tactical networks comprise capabilities to provision and host data and applications locally, connections to the Global Defense Network, and Theater Network Operations and Security Centers to help operate and defend the network.

Army Enterprise Architecture



ALWAYS ACCESSIBLE BY THE SOLDIER

To form a truly unified enterprise network, demarcated only by classification enclaves, the Army must change its approach to information technology development, acquisition and integration. Historically, the Army has not maintained uniform technical standards to guide material development and to keep it in sync with industry. As a result, the Army has in the past produced stove-piped systems, which ultimately stymie the effort to institute an enterprise network, and fielded technology far behind the latest that industry can provide – and which our adversaries use. Under GNEC this practice will stop. For LandWarNet, standardization is a fundamental principle; everything will conform to the underlying Everything over Internet Protocol (EoIP) architecture.

In this same vein, LandWarNet will possess an unprecedented level of adaptability in order to react to changes in technology. The network is not like a tank; as the Internet has taught us, networks should be the most dynamic entities on the planet. The Army, therefore, must allow faster, more efficient introduction of new capabilities that are tested against a certified, accredited architecture. To enable such a process, the Army will establish in the next year a Mission Command Center of

Excellence to certify new technologies against the network's standard architecture and to determine operational viability, with the pass-fail mark set by the user experience. The Center of Excellence also will tap the user perspective to develop operational tactics, techniques and procedures for new technological advances.

To maximize the operational benefit of the network, the Army is abandoning the traditional "horizontal" insertion of new technology according to echelon in favor of "vertical" deployment – where the individual user is the key component. The Army will align programs of record (PORs) to push the network down from the enterprise to the Soldier at the tactical edge. If a particular POR system or technology is not ready, the Army will employ commercial-off-the-shelf solutions to fill the 'gap' – as long as that solution fits within the standardized architecture. In addition, fielding of new capabilities into the network enterprise will be synchronized with the Army Force Generation cycle. The Army will focus funding by fiscal year in order to equip units that are in the reset and preparing-to-deploy phases. ■

★★★ The Practical Impacts ★★★

GNEC and LandWarNet will streamline, to an unprecedented extent, numerous aspects of Army information technology and services. Today's multiple enclaves – among them those of the Army National Guard, Army Reserve, Corps of Engineers, Medical Command, Inspector General Network and Accessions Command – will be consolidated into a single enterprise network with common identity management and security services. The Active Directory redesign will standardize and collapse the Army's current 22 AD forests into two: one for users and the other for applications. CIO/G-6 has finished the architecture for this redesign, which will be completed in 2012. To provide baseline support for the forest consolidation, the Army has established three Enterprise Service Desks: two for the NIPRNet and one for the SIPRNet.

CIO/G-6 also intends to reduce the number of Army Data Centers by 75 percent, from more than 250 to 65. This effort will not only bring about efficiencies in our ability to store data and applications, but will also improve security by significantly reducing the number of points of presence on the network. Overall effectiveness also will increase as our ability to pre-stage data and applications for deploying forces improves.

With a common architecture, the Army will, for the first time, be able to establish common operating environments (COEs). The Army COE strategy identifies three conditions necessary to develop and rapidly deliver software applications to Soldiers: standardized end user environments and software development toolkits; streamlined enterprise software pro-

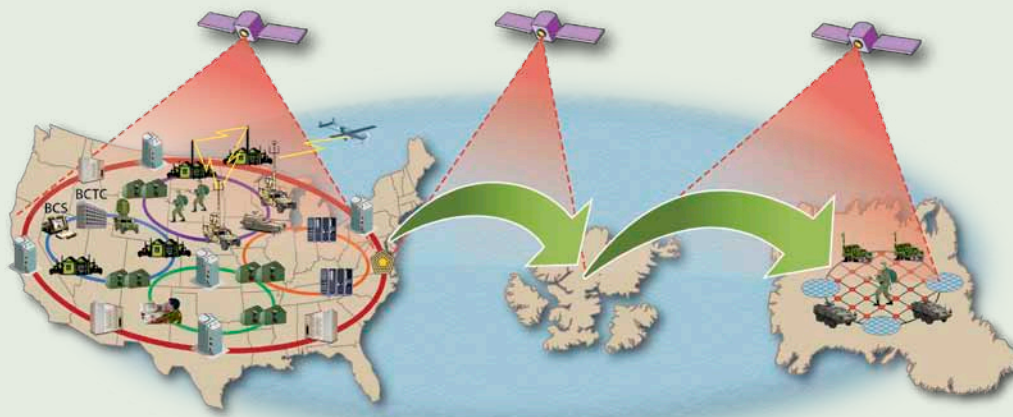
cesses; and creation of an Army Software Marketplace. The Army will apply a common operating environment to each of five categories of computing environments: vehicles, tactical servers, enterprise servers, small form factor (sensors and PDAs) and desktop users. The COEs, combined with a common architecture, will not only align the Army with industry best practices but, perhaps most importantly, will enable the rapid development of secure and interoperable applications that satisfy emerging operational requirements.

The COEs also will help the Army execute information technology acquisition in a more efficient yet less expensive manner. For instance, the Army intends to pursue smaller programs, separating data from applications, and the use of common modules to accelerate software development. The Software Marketplace will provide an open software development environment that encourages innovation from industry and Army personnel; and, combined with the software development toolkits and common modules, should streamline application development and delivery.

The Army will adopt a Defense Information Systems Agency plan to provide Exchange 2010-managed email service for 1.4 million NIPRNet users and 200,000 SIPRNet users. The base service will exceed current standards, enabling the Army to skip a generation of Microsoft email capabilities, substantially reduce hardware and storage expenses, and eliminate email and spam-filtering redundancies. Ultimately, all non-tactical Exchange servers will be retired and 1.4 million

CONUS-based and Expeditionary

...continued from page 5



"We're building an Army that is a versatile mix of tailorable and networked organizations operating on a rotational basis ... to provide a sustained flow of trained and ready forces for full-spectrum operations ... and to hedge against unexpected contingencies ... at a tempo that is predictable and sustainable for our all-volunteer force." — GEN George Casey, Chief of Staff of the Army

Common Access Card holders removed from AKO mail. This effort will bring significant efficiencies that will generate savings in excess of \$150 million.

The Army also is modernizing its Network Operations tools. By the end of the fiscal year, 9th Signal Command (Army)/Network Enterprise Technology Command will have deployed the Host-Based Security System to 82 percent of the NIPRNet and 40 percent of the SIPRNet, and completed the Secure Configuration Compliance Validation Initiative. ■

☆☆☆ Defending the Network ☆☆☆

The cyberspace domain is a critical enabler for U.S. land component forces. Intelligence, fires, maneuver, command and control, situational awareness, collaboration, logistics, air traffic control, medical evacuation – in the last nine years, they have moved to reside primarily in cyberspace.

The Army's use of COTS equipment and industry standards for LandWarNet increases the number and types of capabilities available to those on the battlefield. However, it also increases risk. U.S. adversaries will not only attempt to jam the spectrum, but also will seek to exploit vulnerabilities in routers, to activate logic bombs, to conduct denial-of-service attacks, and to change the data and information within U.S. systems. Network outages or hostile tampering with data results in confusion, incorrect information and delayed decision making at best. At worst, people die.

The Army believes that mitigating this risk requires unity of command and effort. The first element is Army Forces

Cyber (ARFORCYBER), a new Army Service Component Command that combines 9th Signal Command (Army)/Network Enterprise Technology Command and its subordinate units with Intelligence and Security Command under a three-star command and staff. ARFORCYBER will be responsible for ensuring that Army information is accessible, useful and secure for Soldiers deployed anywhere in the world. It will provide the unified NetOps structure necessary to operate and defend LandWarNet, execute technical authority over the network, and supply the Soldiers and civilians capable of attacking and exploiting threat networks.

The second element is a communal Signal effort, at all levels and segments of the network, to ensure consistent global enforcement of standards and policies (the definition of which will remain the purview of the CIO/G-6). All users must be properly trained, and all commanders must make informed decisions that take into account the potential second- and third-order effects of assuming risk on their portions of the network. ■

☆☆☆ Into the Future ☆☆☆

Earlier this year, the Army conducted the second GNEC validation exercise, OPVAL II, to test further and to refine core concepts and systems. Using a real-world brigade, the 75th Fires at Ft. Sill, Oklahoma, OPVAL II simu-

lated a Stryker Brigade Combat Team's transition through all phases of a joint operation as part of 2010 Austere Challenge. The exercise also served as the primary dress rehearsal for GNEC operational, technical and training-related tactics,

techniques and procedures. The preliminary assessment indicates that GNEC is on the right track.

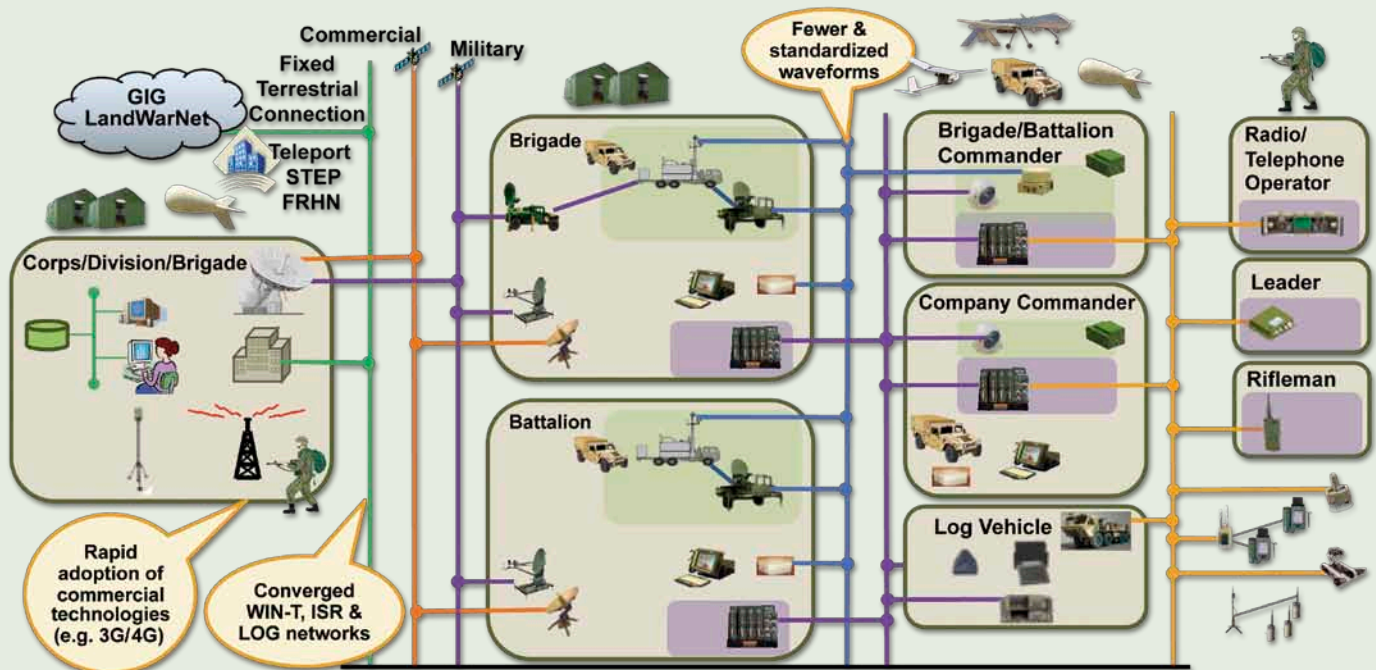
In 2011, the Army will take the next step in proving GNEC and LandWarNet capabilities and concepts in a live operational environment. For Operation Guardian Enable, a brigade combat team will train and prepare for its real deployment to Afghanistan using LandWarNet capabilities previously demonstrated in OPVAL II, mirroring exactly its expected theater activities, conditions and systems while still in CONUS. The objective is a seamless transition from home station to the area of operations and the Afghanistan Mission Network. Should Guardian Enable succeed, by 2012 all units will utilize these

new LandWarNet capabilities to get ready for deployment.

Work continues on the desired, or "to be", network architecture, as well. The shift to a converged, EoIP-based, vertically integrated infrastructure is well under way. By the end of this fiscal year, the Army expects to finish the geospatial information and information assurance portions of the architecture. Over the next two years, it will complete the Active Directory consolidation.

The Army is making a concerted effort to synchronize GNEC and LandWarNet implementation with the base closure and realignment process. A coordinated realignment of CONUS

"To Be" Network Architecture



ALL SYSTEMS RIDING A COMMON, INTEROPERABLE EoIP BACKBONE ESTABLISHING A 'PLUG & PLAY' ENVIRONMENT

network activities and functions from individual installations to the Army enterprise will minimize operational disruption and reduce cost.

The network, of course, is not static. The Army, therefore, will regularly conduct a holistic review of current network requirements — across the enterprise — to determine which remain valid, which require modification and what new requirements are emerging. Similarly, the Army will routinely examine and monitor enforcement of information-assurance policy, certification and accreditation standards, key technology-acquisition management, policies and procedures, and the layered defenses of the network.

Undoubtedly, warfighter capability or policy gaps will arise, and the Army will have to address some immediately. However, the need for expediency will not trump architectural

standards; alignment and integration with the end-state architecture is non-negotiable.

The Army expects the implementation of GNEC and the operationalizing of LandWarNet will bring significant financial benefit, reducing acquisition, administrative and maintenance costs and saving millions of dollars. In an environment of ever-tightening fiscal resources, this alone would be reason enough to pursue this course of action. But GNEC and LandWarNet also will vastly improve the agility, reliability and security of the network and Army data, and enhance interoperability with joint, coalition, interagency and inter-governmental/non-governmental partners and organizations. Ultimately, GNEC's transformation of LandWarNet will make the individual Soldier more powerful and effective, improving his or her overall situational awareness and thereby making the total force indomitable. ■



U.S.ARMY

**AMERICA'S ARMY:
THE STRENGTH OF THE NATION™**

Army Chief Information Officer/G-6
107 Army, Pentagon
Washington, DC 20310
CIOG6.Army.mil