Torchbearer
National Security Report

Modernizing LandWarNet: Empowering America's Army

An AUSA Torchbearer Issue
May 2012

30 May 2012

The Athenian Pheidippides' run through the Greek peninsula to warn of Persian invasion in 490 B.C. embodies a simple military truth: information is power. So too does George McClellan's strategic victory at Antietam in 1862, which rested on found orders detailing Robert E. Lee's movements. Armed with timely, accurate and relevant information, the Athenians and the Union Army were able to respond swiftly and effectively to win on the battlefield. More than 1,500 years after Pheidippides and 150 years after the Battle of Antietam, the U.S. Army is committed to constantly improving its access to information. The telegraph, radio and satellite may be many evolutionary steps beyond the lone message runner or horseback courier, but all share a single purpose—to connect warfighters together and enable decisive action.

The Army's number one modernization priority is the network and the information systems that link its forces around the world. The Army is upgrading its tactical network systems to provide on-the-move capability to maneuver forces and push access down to the lowest tactical level. It is also streamlining and consolidating garrison systems to improve security, efficiency and effectiveness. The endstate is a unified network that reaches from foxhole to home station and delivers to Soldiers the information and services they need, when and where they need them.

In this latest installment of AUSA's signature Torchbearer series, we examine the Army's LandWarNet modernization effort. A look at both the tactical and garrison elements of the network and how the enterprise is managed highlights the progress and remaining challenges to providing unrivaled battlefield connectivity. We hope you find this report a useful and informative resource and that you will continue to look to AUSA for insightful and credible analysis of contemporary national security issues.

GORDON R. SULLIVAN
General, USA Retired
President, AUSA

Contents

Executive Summary

The Army network must be dynamic to give Soldiers, civilians and partners information and services when and where needed. Investment must be steady and wisely applied, while maintaining a strong partnership with industry.

2012 Army Posture Statement

The United States Army is in a period of transition. As it moves out of Afghanistan, the Army is moving into a new era with different global challenges and priorities. The Army's ability to quickly and seamlessly transition between missions will be a requirement for success in an uncertain world. Underwriting that ability is the Army's information network. Connecting warfighters with the most accurate, relevant and up-to-date information is an imperative for unified land operations. As the Department of Defense's (DoD's) new strategic guidance highlights, forces must have reliable access to network capabilities to succeed in modern conflict. LandWarNet is the Army's enterprise-level network that will enable warfighters and leaders around the world to achieve information superiority.

The current Army network is fragmented into many smaller networks that have a variety of standards, systems and pathways. Moreover, the pace of technological advancement has outrun the Army's ability to procure information technology (IT) upgrades in a coherent manner; duplication, isolation and compatibility issues afflict users in every theater and echelon. LandWarNet addresses this complex problem through a single, standards-based network architecture. The Army's strategy for end-to-end network modernization has five high-level objectives: operationalize LandWarNet; dramatically improve cybersecurity posture; improve operational effectiveness while realizing efficiencies; enable joint interoperability and collaboration with mission partners; and recruit and retain an agile workforce to support an expeditionary Army.

The primary task for operationalizing LandWarNet is building the single, secure, standards-based environment. By focusing on standards and not hardware, the Army does not expend resources developing and maintaining proprietary standards that differ from system to system; this streamlines and accelerates acquisition. The standards-based environment also ties into DoD efforts to share IT resources and infrastructure to improve security and efficiency. The Army is also developing the means to let units use their mission command systems on home-station networks and connect to formerly separate tactical networks in combat theaters. Units will have the most current mission data and system updates before deploying—the essence of a single end-to-end network that enables a train-as-you-fight strategy.

The standards-based environment also reaches the tactical edge of the end-to-end network, where the Army is testing the Warfighter Information Network-Tactical (WIN-T) Increment 2 at its semi-annual exercise. WIN-T will provide battalions and above on-the-move network access to voice, video and data services provided by LandWarNet. The Joint Tactical Radio System program is being leveraged in conjunction with WIN-T to provide network access to companies and below.

Improving cybersecurity is an imperative for the Army; its network is under constant attack from capable, well-resourced groups. The Army has a number of security initiatives that are synchronized with interagency partners. Standardizing the network operations tools and accompanying procedures coupled with upgrading legacy software in the force will allow the Army to monitor and respond to attacks without fear of incompatibility. Introducing thin/zero clients—systems that export part or all of computer operations to a central server and instead handle just user input and display—will allow the Army to use cloud and centralized services that reduce the risk of compromise associated with a lost user-device. Enterprise directory and e-mail services establish a single network identity for a user, eliminating the multiple accounts that typically accompany a Soldier from station to station and theater to theater. In addition to increasing security, enterprise services improve access, add sharing opportunities and save resources through infrastructure consolidation. A robust, fully integrated network is




essential to security and efficiency and the ability to empower a smaller, yet more capable, expeditionary Army. LandWarNet is critical to maintaining the Army's technological edge. By modernizing, the Army will build an agile, responsive and affordable LandWarNet.

To facilitate the operational and cybersecurity initiatives, the Army is changing its business and acquisition processes to better harness the maturation of IT. By reforming process in governance, acquisition and architecture, the Army is improving the way it manages IT, ensuring visibility and accountability of purchases, procedures and policies. Implementing front-end standards for new purchases that demand integration into LandWarNet as a whole, versus a specific mission or location, supports the single network construct; shortening the life cycle of IT systems will increase the pace of upgrades and harness the latest evolutions in technology. The Army cannot supply the network the Soldier needs to retain a technological advantage without industry innovation and the support of DoD and Congress. Only through active, constructive partnerships will the Army provide the dynamic, robust network that is the backbone of the networked force and the information engine of the Army.

To improve the effectiveness of procuring critical capabilities, the Army has embraced the Network Integration Evaluation (NIE), a twice-yearly brigade combat team-led test that replicates the operational environment. Network technologies are tested for their utility and effectiveness, giving the Army the opportunity to quickly and thoroughly evaluate programs for purchase or cancellation. With network technology making a generational leap at least every 18 months, the Army can now keep pace by synchronizing with industry and leveraging its innovation, while adopting an incremental approach to modernization through capability set management. Capability sets are smaller purchases of tested systems that are then fielded to the part of the force in the train/reset phase of the deployment cycle. Overall, the NIE process removes the integration burden from deployed units and facilitates incremental upgrades of technology without having to replace an entire product across the force, which saves time and resources.

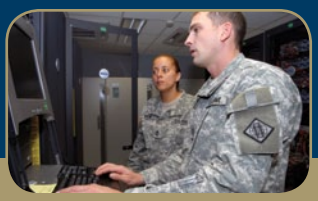
Since the Army's tactical forces operate with joint and multinational partners, LandWarNet is being designed to be interoperable and adaptable through the use of a common operating environment (COE) and Everything over Internet Protocol (EoIP) standards. Transitioning to the COE represents a significant cultural shift in the way the Army acquires and develops systems, providing a blueprint to guide the community on Army network and mission command capabilities. The COE, the set of standards to which all network systems must adhere, is based on open architecture that promotes commercial-off-the-shelf technologies wherever possible; EoIP describes a single method for transporting voice, video and data via nonproprietary Internet Protocol. Having the standards in advance will simplify the development and integration of systems and applications for joint partners and industry. Further, the Army will be better able to integrate commercially mature technologies and shorten development timelines for new capabilities.

Finally, LandWarNet is only as effective as the people who maintain it. The Army is working to rebalance its IT workforce to better meet the needs of an expeditionary force with sophisticated cybersecurity requirements. Overcoming challenges in professional development, retention, training and hiring will be critical to LandWarNet's success and endurance.

Linking the force through reliable, simple and effective network access is an imperative for the modern Army. LandWarNet will deliver the required capabilities only with constant support and investment. DoD and Congress must support network modernization through robust, timely and predictable funding, flexible acquisition and programming authorities and appropriate management reforms. The Army's industry partners must embrace the standards-based environment and develop enduring, efficient partnerships with research and development agencies to ensure wise use of limited resources.

The free flow of secure, accurate and timely information that is easily accessible to all warfighters is a nonnegotiable priority. The Army has a responsibility to answer the nation's call to conduct prompt and sustained combat operations on land; information superiority enables it to win decisively through precision, accuracy and speed. The network is the Army's information engine both for current operations and for transformation and transition.



Modernizing LandWarNet: Empowering America's Army

To be operationally effective, the LandWarNet must provide trusted access, assured connectivity, interoperability and collaboration with all required mission partners. Soldiers and leaders expect the network to be available wherever they are conducting the daily business of the Army, training, preparing for deployment, en route or deployed.

Lieutenant General Susan Lawrence,
U.S. Army Chief Information Officer/G-6, *Leader Blog*, 10 May 2012

Introduction

The United States Army is in a period of transition. As it shifts focus from extended operations in Afghanistan, the Army will enter into a new era with different global challenges and priorities. A variety of state and nonstate actors will employ hybrid techniques to challenge American presence, interests and effectiveness. As the nation's force of decisive action the Army will be intrinsically involved in a variety of worldwide missions designed to confront destabilizing forces. The Army's ability to quickly respond to any type of contingency is dependent upon its ability to generate, project, apply and sustain a trained, professional force.

Connecting all aspects of Army combat power are information and communications. The Department of Defense's current Strategic Guidance—"Sustaining U.S. Global Leadership: Priorities for 21st Century Defense"—explicitly highlights this fact: "Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space."[1] Timely, accurate and detailed information allows decisionmakers to employ the appropriate response to the full range of global events, from humanitarian crisis to combat. Further, information and the corresponding communications architecture provide formations the most relevant and up-to-date operational picture—regardless of location or position in the deployment cycle—and accelerate response time. Operational agility is an imperative for the Army of today and of 2020.

LandWarNet—the Army's enterprise-level network for delivering information to leaders and commanders conducting unified land operations—provides

that agility. It is the Army's top modernization priority. The network strategy builds on 10 years of expeditionary warfare experience and is currently addressing the force's tactical and operational requirements through a new acquisition process and the semi-annual Network Integration Evaluation (NIE) exercise. The Army is also modernizing the garrison elements of the network as part of the end-to-end vision that focuses on operational effectiveness, ease of use and cybersecurity. As the overall size of the Army decreases, the levels of technological integration and network connectivity must increase to provide warfighters the information superiority required by modern war.

Background

Fragmentation has affected both the Army's tactical and nontactical information networks; the networks are composed of different systems, standards and physical pathways. This fragmentation has roots in the significant advancement in network technology in the civilian sector, which has outpaced the Army's ability

[1] U.S. Department of Defense, "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," 3 January 2012, p. 5, http://www.defense.gov/news/Defense_Strategic_Guidance.pdf.




to procure upgrades. Additionally, the growth in information-sharing requirements, in both deployed and nondeployed locations, has created a range of separate, localized networks that address specific requirements but are isolated from other Army networks.

At the tactical level, the Army has experienced drastic change in the past decade. Until 2003–2004, the Army tactical network was based on a system of line-of-sight towers and hardline telephone switches that brought voice and data capacity to the battalion level. After Operations Desert Shield/Desert Storm (1990–1991) and again after the invasion of Afghanistan in 2001, the Army recognized that the systems, purchased in the 1980s, were inadequate to support the geographic distribution and mobility of modern forces in unconventional conflicts. In 2002 the Army created Project Manager Warfighter Information Network–Tactical (WIN-T) to both incorporate past and begin new efforts at providing on-the-move, beyond-line-of-sight data capability to tactical units. After the invasion of Iraq in 2003, Army formations required still more data and voice capability, but WIN-T was just beginning as a program. Accordingly, the Army rapidly procured the Joint Network Node (JNN) system to give battalions and above the terrain-irrelevant capacity needed for counterinsurgency operations. JNN, a bridge between the legacy systems and WIN-T, provides at-the-halt capability for tactical formations. As operations in Afghanistan and Iraq continued, the Army leveraged non-program of record systems and other commercial solutions to provide network capability to companies and outposts in the battlespace. While effective, these systems have limited sustainability and require engineering efforts to integrate into existing networks.

While the Army focused on the tactical network, garrison networks were built, funded and provisioned locally, resulting in separate networks and infrastructure, serious overlap and redundancy. Added to these networks are those run by deployed units or in-theater commands. In-theater networks, both classified and unclassified, link deployed forces in a specific region but create another layer of network redundancy and fragmentation.

LandWarNet must support joint capability areas, warfighting, business and network functions by providing common information technology (IT) services and by hosting applications that move data across the globe. Modernizing LandWarNet will unify the disparate networks in a manner that emphasizes operational effectiveness and ease of use that spans the range of user possibilities—from frontline to home station. LandWarNet must meet its warfighter objectives and sharing requirements in a secure fashion that protects networks and Soldiers from cyber attack. A robust, fully integrated network is essential to security, efficiency and the ability to inform and connect a smaller yet more capable expeditionary Army. In coordination with the Department of Defense (DoD), the Army has developed an overall baseline strategy and is currently developing the Army LandWarNet Implementation Plan for Fiscal Year 2013 and beyond. Its strategy for end-to-end LandWarNet modernization includes five high-level objectives:

- operationalize LandWarNet;
- dramatically improve cybersecurity posture;
- improve operational effectiveness while realizing efficiencies;
- enable joint interoperability and collaboration with mission partners; and
- recruit and retain an agile workforce to support an expeditionary Army.

Operationalizing LandWarNet

The Army's primary task for operationalizing LandWarNet is to build a single, secure, standards-based network environment. The standards-based architecture is a significant shift for the Army, which has traditionally relied on platform-based acquisition

Big Game Changers

"End-to-End Information Environment"

Allied Mission Network

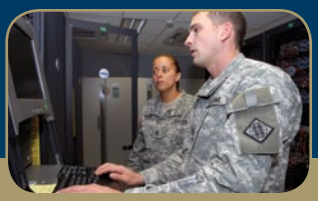
Common Operating Environment

Network Integration Evaluations

Network Capability Portfolio Reviews

Joint Information Environment



and fielding models. LandWarNet will focus on adhering to standards of transport, security and commonality and will be hardware neutral. As long as hardware platforms conform to the standards they will be allowed on the network, in much the same manner as different commercial cell phone models and brands are allowed to operate on a carrier's network. This standards-based environment will allow the Army to acquire hardware upgrades and improvements faster and without expending resources developing and maintaining proprietary network standards that differ from system to system.

Related to the standards-based architecture is the Army's support of DoD's Joint Information Environment (JIE). The JIE is a single, secure, reliable, effective and agile command, control, communications and computing enterprise for use by joint forces and mission partners across all operations, echelons and environments. The Army is supporting this effort and has aligned its top IT initiatives to support the JIE effort without being dependent on it.

The JIE framework focuses on improving network security and effectiveness while achieving efficiencies. It defines common DoD network standards, shared infrastructure and shared enterprise services. The shared IT infrastructure will operate uniformly regardless of service provider and/or function, using procedures developed at the enterprise level. The shared IT infrastructure includes a network that will be more defendable and navigable from garrison to the tactical edge. The Army and DoD are leveraging cloud technologies to enable the movement of mission command and business system data around the globe. JIE further enables DoD and the Army to optimize IT infrastructure by reducing the need for facilities, personnel and equipment. For example, a regional data center can support other joint posts, camps and stations in the region, resulting in cost savings. Army initiatives that directly support JIE include enterprise e-mail, thin/zero-client initiatives, data center consolidation, network security architecture, identity management and access control, and IT management reform.

Train As You Fight

LandWarNet must enable commanders and Soldiers to train as they fight and deploy to austere environments with little to no notice. To this end, the Army is instituting two key network capabilities: (1) operational network connectivity at home station and (2) Installation as a Docking Station (IAADS) linking homefront and battlefield technologies. These critical capabilities are essential to enabling units to train in real time as they will fight.

Institutionalizing coalition partnerships is a priority for the future force. Collaborative tools must be available before the start of any future operation. The Allied Mission Network (AMN) creates a common network from a collection of national and NATO networks that support operations in Afghanistan. The Army has established more than 40 locations in the continental United States that allow formations to communicate, collaborate and share real-time operations and intelligence information with multinational partners as they prepare, plan and execute deployment operations. A key element of AMN is connectivity at home station as early in the Army Force Generation cycle as possible to enhance pre-deployment training. The AMN is a model for future multinational network connection partnerships.

For home-station connectivity, the Army recently implemented IAADS capability at eight U.S. Army posts—Fort Hood, Texas; Fort Carson, Colorado; Fort Bragg, North Carolina; Fort Riley, Kansas; Fort Bliss, Texas; Fort Campbell, Kentucky; Fort Drum, New York; and Fort Stewart, Georgia—with more to follow by July 2012. This capability allows commanders and Soldiers access to the same mission command systems and software used on the battlefield, a critical element in the "train as you fight" model. IAADS provides consistent, streamlined and cost-effective mission command connectivity to garrisons with reduced requirements for costly satellite bandwidth typically needed to connect to combat theaters. The mission command systems provide command and control, distributed planning and situational awareness capabilities; using them at home ensures proficiency before deployment and updated situational awareness—the foundation of the fight-upon-arrival concept for deploying units. Home-station tactical and operational connectivity combined with initiatives such as the AMN have the potential to establish enduring multinational networks, independent of conflict. As the United States focuses more on partner building, multinational collaboration before operations begin must become the norm. LandWarNet can make this a reality.




To make operating forces more effective and more responsive to joint mission needs around the world, the Army network will ensure global access and connectivity in all operational environments and throughout the Army Force Generation (ARFORGEN) cycle. Vital to that connectivity is improving home-station infrastructure to support mission command capabilities and extending those capabilities to deployed locations.

This "mission command system at home station" concept is known as Installation as a Docking Station (IAADS). IAADS allows units to use their tactical information systems on installation networks and to connect with networks in operational theaters. Having one continuous network from combat zone to home station will keep rotating units up to date with the latest operational information, thereby reducing the handover friction in theater. U.S. Army Forces Command and Network Enterprise Technology Command (NETCOM) have recently concluded a successful IAADS pilot program at Fort Carson, Colorado, and are expanding the program to more formations and installations.

Ultimately the garrison elements of the network exist to enable the tactical edge—the warfighters in combat. The WIN-T program was restructured in 2007 into four incremental phases. In response to operational needs, JNN was procured and folded into WIN-T Increment 1. By mid–2012 the Army will have completely fielded JNN to its formations and upgraded the original equipment to the most current configuration. At the same time, WIN-T Increment 2 is scheduled for initial operational testing at the Network Integration Evaluation—discussed in detail later on—and will provide on-the-move network access down to the company level. The Army is leveraging its Joint Tactical Radio System—a handheld and vehicular radio program—to extend WIN-T down to platoon level and below.

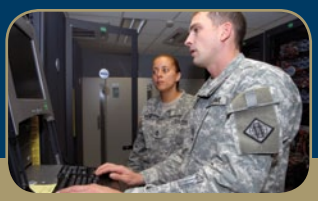
Improving Cybersecurity Posture

The Army's classified and unclassified networks face a growing threat from capable, well-financed and adaptable cyber adversaries—many with state backing. The Army is synchronizing its efforts to improve cyber defense capabilities and protect data, infrastructure and services from cyber attack, exploitation and manipulation. These cybersecurity efforts comprise a multilayered approach that partners with other agencies, such as the National Security Agency (NSA), United States Cyber Command (CYBERCOM), the Defense Information Systems Agency (DISA), Army Cyber Command (ARCYBER) and NETCOM. Several initiatives address the Army's requirements to quickly and effectively identify network intrusions and react accordingly.

The first step toward improving cybersecurity is standardizing the network operations tools used by network administrators. A force-wide standard suite of software and monitoring tools with compatibility across all systems and a corresponding set of tactics, techniques and procedures for their use are required for the Army to achieve effective visibility on the network's status, exert control over every device to take action against attack if required and protect the Army's people, technology and processes. Identifying and upgrading legacy software across the operational force and clearly defining command and control responsibilities with regard to network action are key components to implementing a standard toolkit and defragmenting the network.

Reducing the potential avenues for cyber attack is another development initiative. Migrating the Army to thin clients for its classified networks and zero clients for its unclassified networks is one aspect. A thin client uses the cloud computing concept to run part of an operating system and other applications at a central server while a user interacts with a device that connects to that server and displays the output. A zero client runs no operating system; instead, it controls server connection and display only. A thin/zero client provides the ability to secure one location and operating system, with no data storage capability at the user location, more effectively than various individual devices; also, the loss of a user-level device does not compromise data or access as thoroughly.



Cybersecurity Scenarios at Combat Training Centers

The Army is in the early stages of establishing a holistic cyber training strategy and doctrine to guide unit training and preparedness for cyber conflict. Army Cyber Command is leading this effort with cross-functional participation throughout the Army and is spearheading an initiative to institute non-kinetic warfare scenarios at the combat training centers to assess force readiness against cyber threats. In March 2012, the 1st Information Operations Command introduced cyberspace opposing forces for the first time at the National Training Center at Fort Irwin, California. The opposing forces provided commanders a sense of potential experiences in the cyber warfare domain. This informal pilot was limited in scope to ensure that operations were not significantly impacted, but still beneficial to the unit and to the Army. One event saw the opposing force enter into a unit's network, take control of its printers and then print messages highlighting the attack. Detection of the intrusion was not immediate, but the unit was ultimately able to scour the network logs, identify the point of entry and eventually mitigate the threat. This simple scenario reinforces the Army's need to expand cyber training beyond the current focus of computer network defense and information assurance tasks. As the Army develops its cyber doctrine, it is also working to develop the capability for units to conduct cyber training and non-kinetic scenarios at home stations. Critical to enabling home-station cyber training is the Army's Installation as a Docking Station initiative, which allows Soldiers to train on their battlefield systems in garrison. The Army's objective is to enable units to conduct cyber training at home station prior to rotating through the training centers and institute cyber scenarios and assessments as part of the pre-deployment readiness evaluations. The plan is to have two cyber scenarios per rotation, where leaders can be given immediate feedback and a composite annual report can be compiled for Army leaders to adjust future training programs. The Army is still working through the authorities, tactics, techniques and procedures to establish training center capabilities and is determined to aggressively advance home-station training capability as quickly as possible.

The Army has moved to DoD Enterprise Directory Service (EDS), a single point of management of network identities and access. Previously, a Soldier may have had multiple e-mail or network accounts depending on assignment and location. EDS eliminates both the requirement to establish new accounts and the risk and errors that accompany multiple accounts—a single user has a single network identity that travels with him. LandWarNet now allows a Soldier to transition seamlessly from assignment to assignment and, combined with thin/zero client systems, reduces the unit burden to maintain local-network access. Streamlining the access process will also make it easier to codify, teach and enforce information assurance rules and regulations across the force.

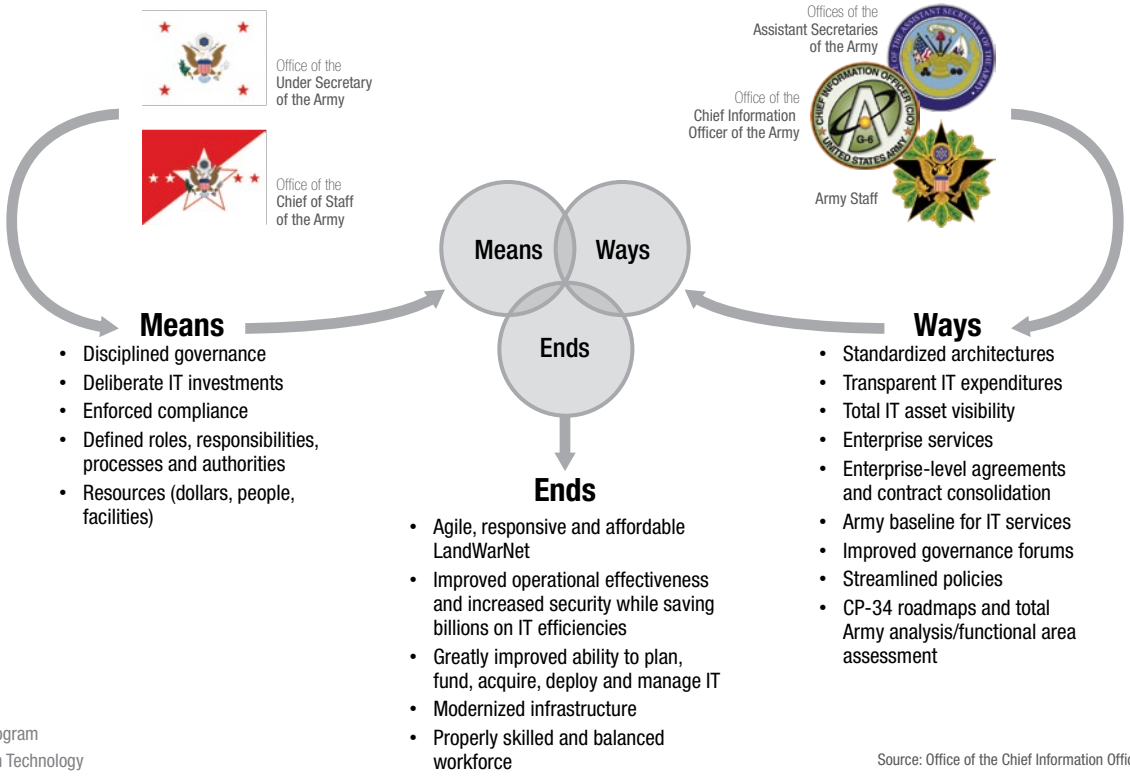
Related to EDS is DoD Enterprise E-mail. In 2010, the Army took initial steps toward consolidating IT capabilities by beginning the implementation of enterprise e-mail service provided by DISA. Enterprise E-mail frees the Army from the acquisition and operation of e-mail servers while receiving a single, integrated service in the DoD cloud. With congressional support, the Army expects consolidation of e-mail services by the second quarter of Fiscal Year 2013. The Joint Staff and National Security Agency are also migrating to DoD Enterprise E-mail. EDS is foundational to Enterprise E-mail through the creation of a single identity for each person/entity in the Army—in conformance with the DoD plan—and it enhances security, storage, address list and information-sharing capabilities. Enterprise E-mail is the first of a suite of enterprise services the Army will implement. Next it will migrate to Enterprise Collaboration Services (ECS), which will greatly improve the Army's ability to share and secure information across LandWarNet.

Improving Operational Effectiveness While Realizing Efficiencies

By adopting an enterprise approach, LandWarNet is providing more effective network services at lower cost than legacy architecture and processes; improving operational effectiveness and security while achieving efficiency is an Army priority. Efficiency is reflected in two broad categories: business process change and acquisition process change.

The way the Army operates and maintains its network is the focus of the Army Information Technology Management Reform Task Force. Business process reforms in governance, architecture and

Information Technology Management Reform Strategy



CP – Career Program
IT – Information Technology

Source: Office of the Chief Information Officer/G-6, U.S. Army

acquisition are setting the conditions for improved network performance.

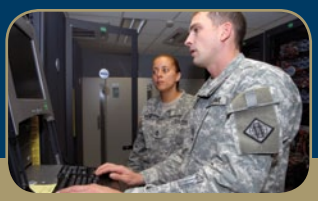
The Army's enterprise governance framework clearly identifies the roles and responsibilities within the Army and across DoD for developing and complying with IT policy and configuration standards. The proposed governance framework will guide IT policy and resource investment decisions in conjunction with the Army's network priorities—an approach that ensures visibility and accountability of IT expenditures throughout the Army. In the process, the Army will update and streamline outdated and redundant IT and governance policies, making them more accessible and understandable to administrators and users.

To complement the streamlined management effort, the Army is establishing an Army Enterprise Architecture (AEA) that synchs with DoD's JIE. The AEA establishes architectural rules and conditions on the front end of the requirements and acquisition processes—it includes all business and operational IT systems and the network infrastructure components required to enable them, from Army headquarters to the foxhole. New systems and platforms must be integrated into LandWarNet as a whole, not just connected to a small branch or specific location within the network (the root cause of network fragmentation and vulnerabilities).

For its business processes, the Army is revising and streamlining acquisition, contracting and information-assurance certification processes. The intent is to reduce the time required to test and certify new devices to keep pace with rapid technological advances within the IT industry. The Army plans to shorten product life cycles and use incremental fielding to ensure that the most current, capable devices—for example, smartphones and tablets—are integrated into the network. The COE architecture for LandWarNet ensures that all products, regardless of vendor or developer, can be evaluated and certified with these new processes, thus saving time and resources. **The acquisition objective is rapid insertion of validated developing technologies into the Army's ongoing modernization of LandWarNet.**

Finally, the Army is consolidating its data centers—large rooms or buildings that house data-related



servers, storage media or computers—to reduce operating expenses and improve efficiency. Army data center consolidation began in 2011 and is currently reducing the Army's data center inventory worldwide, improving security of Army information assets and providing managed information services at the enterprise level. By consolidating servers and using common client servers for all applications, the Army will reduce the administrative and logistical burden. An Army application rationalization program accompanies the data center consolidation. The program, which began in early 2012, requires the Army to review all applications and evaluate the redundancy, obsolescence, cost-effectiveness, complexity and interoperability of its software applications with the goal of consolidating and reducing both the number of applications Army-wide and the number of data centers and repositories.

For modernizing the tactical edge of LandWarNet, the Army has embraced an agile acquisition process that uses the Network Integration Evaluation and capability set management to more effectively procure rapidly evolving network-related systems. This method ensures technological maturity and network compatibility in ways that did not always exist in the past. With network technology making a generational leap at least every 18 months, the Army can keep pace only by synchronizing with industry and leveraging its innovation while simultaneously adopting an incremental approach to modernization.

The NIE is a twice-yearly exercise conducted at White Sands, New Mexico, by a brigade combat team (BCT) from nearby Fort Bliss, Texas, with the purpose of evaluating new technologies in an austere and

Network Integration Evaluations (NIEs) – Streamlining Acquisition

The Army has fundamentally changed the way it develops, evaluates, tests and delivers networked capability to its operating forces. NIEs conducted by the Brigade Modernization Command at Fort Bliss, Texas/White Sands Missile Range, New Mexico, bring the operational test, acquisition and requirements communities together in a realistic operational environment to leverage industry innovation and eliminate network integration burdens on deployed forces. The convergence of Soldiers, materiel developers and engineers provides more useable test data and direct user feedback about systems. The NIE is based on incremental modernization that allows the Army to buy fewer capabilities but more often—referred to as capability set management.

The President's 2013 budget request identified $214 million to support the System of Systems Integration Directorate and conduct NIEs. The benefits of the NIE far exceed testing and evaluation costs. So far, lessons learned from the NIEs have helped the Army avoid approximately $6 billion in planned spending and reallocate resources to other priorities—all while providing more capability, sooner, to its operational formations. Major program savings identified by NIEs so far include:

- Network Integration Kit termination–$60.8 million
- Early Infantry Brigade Combat Team termination/capability set implementation–$4.0 billion
- Ground Mobile Radio restructure–$609 million
- Nett Warrior restructure–$822 million
- Mounted Soldier System termination–$445 million

Consolidating testing at NIEs has yielded more than $7 million in savings from reduced test costs.

The Army has also procured systems as a result of the NIE process. After NIE 11.2 the Army awarded a contract worth $66 million for vehicle-mounted data radios as part of Capability Set 13 for fielding to up to eight brigade combat teams. As a direct result of NIE 12.1, the Army is in current source selection for a single-channel vehicle-mounted radio capable of importing the Soldier Radio Waveform. This will be a competitive procurement with a summer 2012 target date of contract award for up to 5,000 radios to support concurrent Capability Set 13 fielding efforts. Further, this contract action was rapidly instituted just months after the close of NIE 12.1.

The NIE allows for integration of systems prior to deployment while providing an avenue for industry to bring in mature capabilities for evaluation. The Army is committed to this method. Monolithic programs of record will be phased out as the Army advances an incremental, capability set-based acquisition model. This aligns with the recommendations of the 2010 Army Acquisition Review, "Army Strong: Equipped, Trained and Ready." NIEs help the Army leverage industry advancements and provide its formations the most up-to-date network capabilities required by an agile, versatile, expeditionary and technologically enabled force.

realistic environment.[2] The NIE is meant to remove the integration burden of new technology from combat commanders and place it on the test BCT; this allows the Army to properly assess systems for effectiveness and network compatibility before purchasing in mass and sending the systems to combat theaters. Additionally, it brings together industry engineers and Soldiers, ensuring accurate, timely feedback on performance and change requirements. An ongoing major NIE initiative in the tactical portion of LandWarNet is performance testing of new Internet Protocol radios that extend network access and services to mobile platforms and dismounted Soldiers. The scope of Army NIEs will evolve as the Army eliminates the operating- and generating-force distinctions from LandWarNet. The NIE also identifies underperforming programs and reduces acquisition risk. The next NIE is scheduled for fall 2012.

The Army's acquisition of capability sets ties directly into the NIE process. Rather than commit funding and resources to a whole-force buy, capability set management lets the Army buy, test and field (as warranted) NIE-vetted systems in smaller increments. The Army aligns programs (funding, timelines and integration) through capability set management so that operational units receive an integrated network capability set during their reset or training phase of the ARFORGEN cycle. Through capability sets, the Army procures only what is needed by units entering reset or training—this helps keep pace with technology while allowing for better resourcing and incremental modernization. Approximately every two years the Army will implement the next iteration of a given capability set, which will reflect any changes or advances in technology realized since the last set.

To ensure the NIE and acquisition process is being used appropriately, the Army has instituted a network Capability Portfolio Review (CPR).[3] The CPR is designed to facilitate better understanding of the requirements that drive IT investment and procurement. It also ensures funds are programmed, budgeted and executed against validated requirements that consider cost- and risk-informed alternatives. This approach helps the Army evaluate and adjust current and planned network capabilities by considering factors such as combatant command operational needs, lessons learned, emerging technologies and affordability. CPRs help eliminate duplicative IT acquisition efforts, optimize return on investment and ensure that the Army is getting the capabilities it needs most when it needs them.

Enabling Joint Interoperability and Collaboration with Mission Partners

The Army operates as part of a joint force that conducts unified land operations worldwide and uses technology to augment its core strengths. It is coordinating with DoD, the other services and mission partners on network technical architecture, data standards and IT procurement to ensure that each technology and process is synchronized across all communities. **LandWarNet must not only be accessible and effective within the Army but also able to accept and integrate systems and software from joint partners as well.** To achieve this, LandWarNet is built on the two principles of a common operating environment and Everything over Internet Protocol.

In 2011 the Army instituted the COE, a centrally approved set of computing technologies and standards that will enable rapid development of secure and interoperable applications and to which the network itself and all applications and systems riding the network must adhere. The COE addresses the specifics of the standards-based network model and defines minimum configurations for the Army's computing environments, from the enterprise server to mobile small handheld devices. Transitioning to the COE represents a significant cultural shift in the way the Army acquires and develops systems. The plan is designed to tell industry upfront and with certainty the parameters within which Army applications and foundational software must fit. The Army is changing the culture of how it builds systems, how its programs look at themselves

[2] For more information on the Network Integration Evaluation, see AUSA's Defense Report "Network Integration Evaluations: Developing Technologies with the Army's Industry Partners," October 2011, http://www.ausa.org/publications/ilw/Documents/DR%2011-3_web%20(2).pdf.

[3] For more information on the Capability Portfolio Reviews, see AUSA's Defense Report "Capability Portfolio Reviews," September 2010, http://www.ausa.org/publications/ilw/Documents/DR%2010-3%20CPR%20v2%20web.pdf.

respective to other programs, how requirements and funding are done and how it puts in place a blueprint to guide the community on where it is going with regard to network and mission command capabilities. COE is based on open architecture that promotes commercial-off-the-shelf (COTS) technologies whenever possible. Alignment with the COE is mandatory for new systems and capabilities; the Army is bringing existing systems into compliance as well.

To solidify the underlying framework established by the COE, the Army also standardized to a single mode of information transmission, regardless of format or delivery means. Whether simple text, voice, video or any other format, the network will move all data via a nonproprietary Internet Protocol. The COE and EoIP will enable quicker development and fielding of secure, interoperable applications and systems that satisfy today's operational requirements. Industry will know in advance the standards it must meet, cutting response time and lowering costs. Because the COE aligns with commercial standards, the Army will be able to use more COTS and near-COTS technology. Enforcing compliance with the COE will ensure interoperability among all Army systems, improve the network's defense posture and simplify training and sustainment. The COE and EoIP will simplify and accelerate integration of new capabilities with existing systems and software, including those of joint and multinational partners.

Recruiting and Retaining an Agile Workforce to Support an Expeditionary Army

Fundamentally the Army is people. LandWarNet is only as effective as the dedicated professionals who maintain it. To ensure that LandWarNet can support the entire Army requires people at every echelon who are trained and qualified to engineer, install, operate, maintain and defend the network. The Army is rebalancing and redesigning the IT workforce, developing effectively organized and better-trained personnel to operate and defend LandWarNet.

Part of the personnel challenge is evolving the professional development path that addresses the quickly changing and overlapping requirements of IT management and cybersecurity. Building the appropriate, flexible and current skill sets required for network

operations is time intensive. Recruiting and retention of skilled cyber operators will require proper career incentives. The Army is championing federal hiring reform to create the next-generation approach for recruiting, building and maintaining the information workforce. Effort will be required to expand the available pool of potential workforce members, reach that pool with appropriate career progression and reduce the barriers to entry into the Army's force structure.

What is Needed

Linking the force together around the world through reliable, simple and effective network access is imperative. The information requirements of complex unified land operations are significant; LandWarNet will meet those requirements, but the Army needs continued support for its vision.

A strict adherence to the COE architecture for acquisition is needed to establish interoperability and prevent the fragmentation of the network, making it accessible to warfighters regardless of location or station. Further, incremental modernization and shortened life cycles are necessary for the Army to keep pace with industry development and ensure that Soldiers retain the technological advantage. Close partnerships among the Army, DoD and industry combined with the efficient use of research and development resources are needed to streamline the procurement process and advance cost-effective, achievable, relevant programs. Leveraging COTS or near-COTS technology must continue to be a priority for information technology modernization and building the predictable common operating environment.

DoD and the Army need to invest in the network workforce of the future. Reaching out to civilian educational institutions and developing internship/training opportunities are part of building the force. An additional part is changing the Army's practices to make it more accessible to a larger pool of potential cyberspace experts while still maintaining the appropriate security conditions. The Army then must adequately train and professionally develop its workforce while offering competitive incentives for long-term service.

What Must Be Done

As the Army reduces its overall size, it will have to: better integrate information across the force; improve network access to enable collaboration and response; and retain its technological advantage. To that end, the Army must continue its efforts to rapidly acquire new technologies that adhere to a common standard, recruit, develop and retain its network force and build enduring partnerships with the commercial sector to fuel innovation. Beyond the Army, the **Department of Defense must:**

- approve and fund the Army portion of the Joint Information Environment initiative and follow-on architecture and capabilities (AUSA Resolutions 12-7 and 12-18);
- approve and endorse IT management reform proposals (AUSA Resolution 12-18);
- fully fund LandWarNet capabilities, especially for posts, camps and stations (AUSA Resolution 12-7);
- fully fund the Army WIN-T and tactical radio programs to extend network access to warfighters on the move (AUSA Resolution 12-16); and
- continue to resource and support the Network Integration Evaluation process (AUSA Resolutions 12-10 and 12-16).

Congress and the administration must:

- ensure that IT funding for modernizing DoD networks is a priority (AUSA Resolution 12-14);
- support Army network modernization—to improve governance and visibility of IT spending—and implement IT acquisition reform (AUSA Resolution 12-18);
- consider the size of each service's network when allocating resources for network operations and security;
- allow reprogramming of IT budgets/appropriations to save money and increase the Army's effectiveness and efficiencies (AUSA Resolution 12-18); and
- provide adequate funding for network modernization and IT management reform (AUSA Resolutions 12-7 and 12-18).

Industry partners must:

- meet the technical requirements outlined in the Army's common operating environment architecture at affordable costs; and
- partner with DoD and Army research and development agencies so precious research and development dollars are leveraged efficiently (AUSA Resolution 12-18).

The Army is the nation's force of decisive action. The force's ability to prevent, shape and win is tied to its ability to understand and respond to the global environment. The free flow of secure, accurate and timely information that is easily accessible to all warfighters is a nonnegotiable priority. The Army's LandWarNet will deliver streamlined network capability to support unified land operations in any theater or location. By focusing on a standards-based operating environment and acquisition model that emphasizes mature technology and enterprise services, the Army is adding capability and lowering costs. The NIE process is ensuring that warfighters receive tested, relevant equipment with the lowest possible integration burden. Pushing the network down to the tactical edge and giving Soldiers on-the-move network access through WIN-T remains an Army priority. The Army of 2020 must be able to quickly and flexibly respond to global contingencies and totally dominate any battlefield upon which it finds itself. Information must flow quickly between tactical, operational and strategic command levels to enable appropriate action and support. The Army's responsibility is to answer the nation's call to conduct prompt and sustained combat operations on land; information superiority enables it to win decisively through precision, accuracy and speed. The network is the Army's information engine both for current operations and for transformation and transition.

Torchbearer Message

As stated in the Department of Defense's current strategic guidance—"Sustaining U.S. Global Leadership: Priorities for 21st Century Defense"—"modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space." The Army, as the nation's force of decisive action, requires accurate, timely and relevant information delivered in a prompt and accessible manner. To that end, the Army is modernizing LandWarNet, the force-wide network designed to support unified land operations through seamless access across echelons.

LandWarNet must be managed like a weapon system, with the same discipline and rigor applied to other Army weapon systems. With effective governance and aggressive change implementation, the Army will overcome the challenges and inefficiencies that have hampered its cyber operations and investments in the past. Balanced, end-to-end modernization enables more effective application of resources—technology, personnel, funding and time.

End-to-end modernization consists of upgrading and merging existing tactical and garrison networks into a single, standards-based environment. Operational data will be available to forces around the world, regardless of location or placement in the deployment cycle. This ensures that Army users have the very latest relevant data and that deployed forces have assured access. Switching to more centrally managed and cloud-based services increases security from cyber attacks, eases network identity management and streamlines access for users. Adhering to a standards-based architecture makes it easier for the Army to leverage commercially available, mature technologies that are manufacturer neutral.

The Army is also testing the next increment of the Warfighter Information Network–Tactical (WIN-T). WIN-T will provide on-the-move network access to voice, video and data services for battalions and above. The Army is using its individual and vehicular radio procurement programs to extend access to companies and below. Both programs are being evaluated in a comprehensive, realistic test environment.

The Network Integration Evaluation (NIE), a twice-yearly exercise, tests potential new acquisitions in a realistic operational environment to determine technological maturity, utility and compatibility with the LandWarNet standards. The NIE brings the operational test, acquisition and requirements communities together to leverage industry innovation and eliminate network integration burdens on deployed forces. The convergence of Soldiers, materiel developers and engineers provides more useable test data and direct user feedback about systems, making the process more responsive to operational input and reducing costs. An outgrowth of the NIE is the acquisition strategy of capability sets. Capability sets are purchases of a new network-related system in small batches—enough to outfit the fraction of the force in the train/reset phase of the deployment cycle. Buying in smaller sets allows a unit to train on the system fully before deploying with it. Capability sets also allow the Army to introduce upgrades as they occur, without the need to replace a previous version in every formation at the same time. The NIE and capability set management are addressing the rapid development cycle of information technologies; the Army has the ability to quickly evaluate and procure network-ready systems or terminate underperforming programs. So far, the NIE has helped the Army avoid approximately $6 billion in planned spending and reallocate resources to other priorities—all while providing more capability, sooner, to its operational formations.

Finally, the Army is moving toward enterprise-level services and consolidation to improve functionality, security and efficiency. Enterprise E-mail and collaboration programs are streamlining network access for all Army users and better connecting the force. Data center consolidation reduces the logistical footprint of network infrastructure and associated costs. All these measures will enable the Army to save $1.5 billion annually starting in 2015.

For LandWarNet modernization to succeed, the Department of Defense and Congress must support the Army's ongoing efforts. Constant support, timely and predicable funding, flexible acquisition and programming authorities and appropriate management reforms are essential for LandWarNet to deliver the required capabilities for future forces. The Army must keep pace with global innovation through enduring partnerships with industry. The Army must have information superiority.

The foundation of the modernized network is a joint, secure and common architecture that will provide information from the cloud to enable leaders, units and the institutional Army to function more effectively. The Army will extend this critical capability to its installations around the world. This capability will increase force effectiveness, facilitate transition for units and individuals from one phase of the Army Force Generation cycle to another and greatly improve network security.

2012 Army Posture Statement







Institute of Land Warfare
Association of the United States Army

2425 Wilson Boulevard, Arlington, Virginia 22201-3385
800-336-4570 www.ausa.org