Torchbearer National Security Report

The U.S. Army's Information Revolution:

Delivering Information Dominance to the Warfighter

An AUSA Torchbearer Issue
August 2006

Preface

The National Defense Strategy identifies an array of traditional, irregular, catastrophic and disruptive challenges that pose threats to the [United States]. These threats are becoming increasingly complex. [The Army] no longer face[s] only conventional armies who operate within clearly established political boundaries. In addition, [the Army] will face enemies that employ irregular tactics, terror and asymmetric warfare. These enemies will be increasingly transnational and dispersed.

From the 2006 *U.S. Army Posture Statement*, 10 February 2006, p. 1; available at http://www.army.mil/aps/06/

This is an era of uncertainty, unpredictability, misinformation and misconceptions. Not only is the U.S. Army engaged in stability and counterinsurgency operations in Afghanistan and Iraq, it is also transforming into a modular, brigade-centric force to eliminate emerging threats to the American homeland and work with joint and coalition teams to mitigate military, political and economic threats to global security. Across the full spectrum of operations, from domestic disaster relief to counterinsurgency operations and future conventional conflicts, the Army can expect to remain fully engaged around the world for many years to come.

As the Army continues to provide combatant commanders a wide range of versatile and complementary capabilities, it fully realizes the importance of net-centric operations in the 21st century. Working alongside the other services, the Army is managing, maintaining and upgrading its own information systems while communicating information across the Defense community and other government agencies. As warfighting becomes increasingly network-centric, **the Army knows it must deliver information dominance to the warfighter.**

To do so, the Army has developed a bold plan to revolutionize its information technology and business practices. By developing a network called LandWarNet, part of the Defense Department's Global Information Grid (see pages 3–6), the Army is taking steps to ensure that the current and future forces will be able to operate in a joint network-centric information environment. Coupled with the eventual success of LandWarNet is a need to revitalize and upgrade the Army's existing information technology investments, including installation infrastructure, knowledge management systems and information assurance systems (see pages 7–12). Evolutionary change, such as using the Single Directorate of Information Management and IT Portfolio Management concepts (see pages 13–14), is leading to revolutionary outcomes. **All of these changes ensure that the Soldier—the centerpiece of the Army—will have strategic-, operational- and tactical-level superiority in all security environments.**

Ultimately, success in future Army operations will rest on decisions made now—especially decisions on resources. The matter of providing adequate resources for the current and future forces is not "either-or" but rather "both-and." For example, Future Combat Systems (FCS), the Army's main modernization program, comprises 18 manned and unmanned systems in support of the Soldier, **all connected by a robust, jointly interoperable information network.** FCS extends the information revolution, which has transformed air and naval warfare, to the realm of ground warfare. Even before the fielding of the first FCS-equipped brigade combat team (BCT), the FCS program will provide advanced technologies to be integrated, as they mature, into current formations in two-year increments called "spin-outs." These new capabilities will directly benefit all U.S. ground forces, including the U.S. Marine Corps and special operations forces (SOF) from all services.

This Torchbearer explores the Army's plan to revolutionize its information systems, infrastructure and processes. Each of the five issue papers that follow details a critical component of this plan to deliver information dominance to the warfighter.

Contents

All photos courtesy of HQ Department of the Army

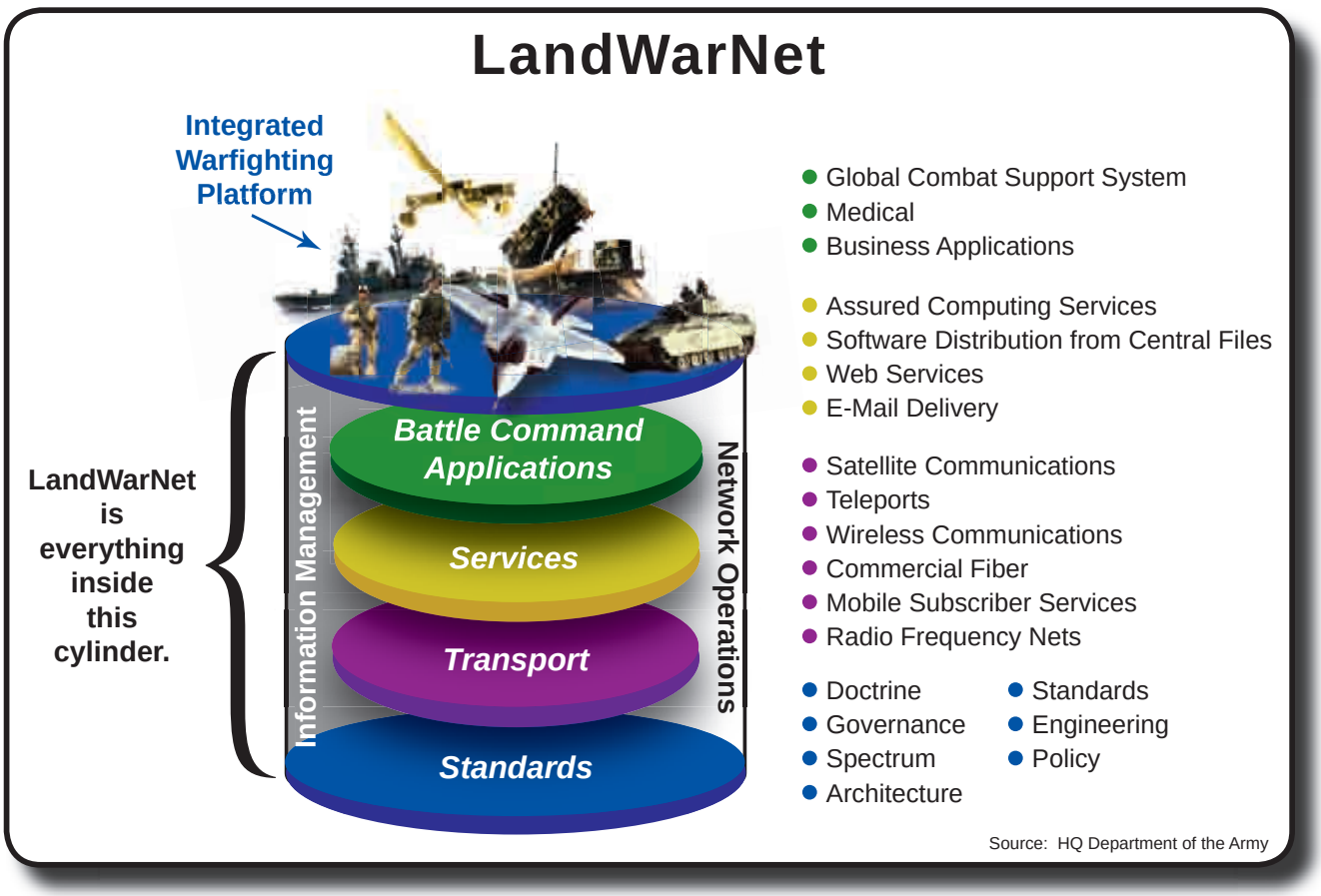
LandWarNet: *Connecting the Warfighter in the Current and Future Fights*

A new era of information-intensive warfighting has led to the primacy of the Department of Defense's Global Information Grid (GIG) as an essential component of combat power and force protection. Today, the military requires an information capability that securely connects Soldiers (active Army, Army National Guard and Army Reserve) and systems to their support base, regardless of time or location.

LandWarNet is a jointly-inspired network vision that enables the warfighter's migration to the joint and interdependent future force. LandWarNet is the Army's portion of the GIG, networking the Army's active and reserve components to the GIG. A combination of infrastructure, applications and services, LandWarNet "moves information through a seamless network and enables the management of warfighting and business information."[1]

Current JNN Network Fills Some Needs

During Operations Enduring Freedom (OEF) and Iraqi Freedom (OIF), the Army's Cold War-era Mobile Subscriber Equipment (MSE) faced a number of shortcomings for the fast-paced battlefield of the 21st century. To meet connectivity demands during the initial fight, the Army purchased commercial satellite access and commercial off-the-shelf systems to satisfy substantial bandwidth demands. **The operational need for a dedicated joint network was born of this requirement for more bandwidth in a joint, geographically dispersed fight.**



[1] Office of the Chief Information Officer/G-6, "CIO/G-6 500 Day Plan" (5 October 2005), available online at http://www.army.mil/ciog6/news/500DayPlan.pdf.

To bring increased capabilities to units as quickly as possible, the Army has fielded a network of Joint Network Nodes (JNN), which consist of trailer-mounted *Ku*-band satellite terminals connected to local area network equipment. A component of the Army's LandWarNet, the JNN network provides Army units at the battalion level and above with beyond-line-of-sight interconnectivity to Army and joint forces. JNN also provides connectivity via the Defense Information Systems Network (DISN) to Network-Centric Enterprise Services such as messaging, voice, collaboration, information assurance and access to Army and DoD portals. Brigade combat teams (BCTs) equipped with JNN can deploy independently without additional communications assets from higher echelons, and they can connect directly to joint headquarters and access the DISN with their embedded communications. The JNN network also interoperates with both the older MSE network and the Army's newer Stryker BCT communications systems.

The disaster relief operations for Hurricanes Katrina and Rita demonstrated the JNN network's connectivity to civilian communications networks and to emergency operations centers. Because it uses commercial standards, including Internet Protocol (IP), the Army's communications equipment was interoperable with the severely damaged civilian network. Using JNN, the Army restored network function, either through the existing network or by alternate routing in areas where the civilian network had been destroyed. The Army also maintained emergency radio nets over two regions encompassing 13 states, assisting both military medical units and the American Red Cross with communications. A JNN at the Oakdale City Fire House in Jefferson Davis Parish, Louisiana, even linked up to a cellular telephone base station, allowing up to 300 cell phones to receive service in that area.

The JNN network also provides commercial satellite augmentation to Army military satellite communications and IP-based services such as voice-over-IP telephone service, e-mail, IP-based virtual private networks, and unclassified/classified Internet service at the battalion level and above, and secure digital telephone service at the brigade level and above. The Army has fielded this equipment to six divisions—3d Infantry, 101st Airborne (Air Assault), 10th Mountain, 4th Infantry, 1st Cavalry and 25th Infantry; fielding to the 82d Airborne Division is under way. The equipment has been in use in Iraq for almost two years, garnering much respect from the warfighters and communications personnel who use it.

Although the JNN network has helped Soldiers achieve critical battlefield successes, it has some limitations. Each node must be stationary and set up to be used—it is an at-the-halt capability only. Furthermore, if a hub for a field-deployed JNN network is taken out of service for any reason, a whole division may lose connectivity to LandWarNet. Thus, the JNN network now serves primarily as a *temporary* force multiplier while the Army develops the more capable Warfighter Information Network-Tactical (WIN-T) system.

On Demand and On the Move: Warfighter Information Network-Tactical

Warfighter Information Network-Tactical is the Army's emerging single integrated tactical communications network; it will provide increased network capacity, speed, security and seamless video, data, imagery and voice services that enable decisive combat actions. **WIN-T offers three critical improvements on the current JNN network**. First, WIN-T can function both at the halt and on the move, supplying the right information to commanders, staff, functional units and "capabilities-based formations"—the Army's mobile, agile, lethal, sustainable and deployable units. It also offers significantly improved network management capabilities, being optimized for offensive and joint operations to give combatant commanders the capability to direct multiple missions simultaneously. Finally, WIN-T is "self-healing," allowing a deployed network

to survive damage to individual nodes and hubs. WIN-T will establish an environment in which commanders at all levels have the ability to operate with virtual staffs and analytical centers at remote locations throughout the battlespace.

As a key communications system supporting the Army's current and future forces, WIN-T will meet the pressing need for efficient battlefield bandwidth utilization, optimal data throughput and on-the-move communications and critical information exchange. When completed, WIN-T will consist of a three-tier architecture—ground, airborne and space layers—**that enables constant connectivity among units in theater, while also providing reachback capability to sustaining base, joint, allied and coalition forces.** Corps, division, brigade and battalion units will be able to access the network *while mobile* via its robust networking, affording units the ability to share relevant information in all terrains and under all environmental conditions.

Satellites: A Combat Multiplier

As military satellites mature, the Army is turning to them for greater control and lower operation and maintenance costs than are available with civilian satellites.

As the battlefield area and distances among warfighting units continue to grow, more satellite capability is required. Planning for near- and far-term satellite communications (SATCOM) capabilities is paramount to successful Army operations. Future military SATCOM systems such as the Wideband Gapfiller Satellite (WGS) and Transformational Satellite (TSAT) are critical.

WGS satellites will provide greatly increased capability over the current Defense Satellite Communications System (DSCS) satellites—one WGS satellite provides approximately eight times the throughput capacity of one DSCS satellite. WGS satellites are also capable of supporting some satellite communications on the move. The Army anticipates the successful first launch of the WGS in Fiscal Year 2007.

TSAT, the next-generation communication satellite, will network in space, providing unprecedented continuous protected high bandwidth to highly mobile forces that routinely operate at beyond-line-of-sight distances

from one another. TSAT is vital to ensuring joint battle command capabilities for the future force. The first launch is expected in FY 2014.

Training the Net-Centric Warfighter: LandWarNet University

Signal officers are no longer the only Soldiers who need to understand the network. Commanders at all levels must be able to control their sections of the network and know LandWarNet as well as they do any other battle system under their command. Through LandWarNet University (LWN-U), leaders will learn LandWarNet's operational and strategic focus, gain an understanding of its complexity, and develop the ability to employ LandWarNet in support of the warfighter. These competencies and skills will be essential when the Army transitions to WIN-T.

LWN-U makes training and education available through the network to support Soldiers and leaders around the clock throughout all phases of the Army Force Generation Model.[2] The transformation of the University of Information Technology's web portal into the LandWarNet-electronic University (LWN-eU) is the first step in expanding LandWarNet to provide lifelong learning to all its users. Training will occur in the classroom and on the battlefield by integrating training among multiple enabling organizations, with LWN-U providing training support to the warfighter through on-site resident training, mobile training teams and distance learning. Soldiers can now access LWN-eU via Army Knowledge Online.

[2] For more about Army Transformation and Army Force Generation, see AUSA's Torchbearer National Security Report "2006 and Beyond: What the U.S. Army is Doing" (March 2006), available online at http://www.ausa.org/PDFdocs/TBSecRpt/TBear_March_06_optimized.pdf.

FCS Network: Key to Future Combat Systems

The Future Combat Systems (FCS), the Army's modernization program for the operating force, consists of a family of manned and unmanned systems, to include the Soldier, connected by a common network. This networking of systems will provide Soldiers and leaders with leading-edge technologies and capabilities and allow them to dominate complex environments. **The network is the backbone and key to the success of FCS.**

The FCS network allows the FCS family of systems to operate as a cohesive "system of systems." As the key to the Army's transformation, the network enables the Army to employ revolutionary operational and organizational concepts. The network enables Soldiers and leaders to sense, comprehend, shape and dominate the future battlefield at unprecedented levels.

The FCS network comprises four main building blocks: System-of-Systems Common Operating Environment (SOSCOE); Battle Command (BC) software; Communications and Computers (CC) systems; and Intelligence, Surveillance and Reconnaissance (ISR) systems. These four building blocks are interconnected, enabling BCTs to see first, understand first, act first and finish decisively or reengage.[3]

System-of-Systems Common Operating Environment. Central to FCS network implementation is the System-of-Systems Common Operating Environment, which supports multiple mission-critical applications independently and simultaneously. SOSCOE acts as a standardized suite of configurable software modules, allowing any specific application to incorporate only those components needed for a given operation. Because the SOSCOE architecture uses commercial off-the-shelf hardware and a Joint Tactical Architecture-Army-compliant operating environment, its architecture is cost-effective—**it does not require expensive, dedicated software development, nor does it result in a single-function, "stovepipe" system.**[4] The SOSCOE framework is also versatile, allowing the Army to use its own message format within FCS to communicate with joint and allied forces in real time, near-real time, and non-real time.

Battle Command Software. Battle Command software applications include mission planning and preparation, situational understanding, battle command and mission execution. The BC software's combined capabilities will enable full interaction among FCS-equipped units. The BC capabilities will be common to, and tightly integrated into, FCS, and will share a common framework to achieve integrated and interoperable systems without hardware, software or information "stovepipes."

Communications and Computers Systems. The FCS Communications and Computers network includes several systems, such as the Joint Tactical Radio System, that network with WIN-T and satellite communications systems. The CC network employs all available resources to provide a robust, survivable and reliable communications network that seamlessly integrates ground, near-ground, airborne and spaceborne assets for constant connectivity and layered redundancy.

Intelligence, Surveillance and Reconnaissance Systems. A distributed and networked array of intelligence, surveillance and reconnaissance sensors provides FCS with the ability to see the enemy first. The ISR assets within the Modular Force—as well as those external to the Modular Force and at higher command levels—will provide timely and accurate situational awareness, enhance survivability by avoiding enemy fire, enable precision networked fires and maintain contact throughout engagement.

LandWarNet, the Army's portion of the Global Information Grid, provides robust networking capabilities to Soldiers and leaders in the current fight and will allow Future Combat Systems to function as a cohesive "system of systems."

---

[3] For more about the Army's development of FCS-enabled BCTs, see AUSA's Torchbearer National Security Report "Accelerating Momentum: The Stryker Brigade Combat Team as a Learning Organization" (June 2006), available online at http://www.ausa.org/webpub/deptilw.nsf/byid/JSUR-6QLHTM.

[4] "Stovepipe" refers to the use of a system, component or software package for one vertically aligned task, instead of a system that can be integrated horizontally. An example would be a command-and-control system that allows Army units in the field to communicate with one another but not with other services.

Information Technology on Installations:

Modernizing Home-Station Support to the Warfighter

The Army's ultimate vision for its information technology (IT) architecture is the integration of Army installations—its "flagships of readiness"—into the Defense Department's Global Information Grid (GIG), providing essential home-station support to the warfighter in the field. As installations modernize their IT infrastructure, they gain access to a fully-integrated, interoperable and efficiently networked information system. Moreover, Soldiers from deployed or off-installation locations will have remote access to storage and computing services. In this way, information producers and information consumers will have seamless connectivity to satisfy command-and-control, collaboration, coordination and information-processing needs regardless of location, allowing the full integration of operations around the globe.

The Army is realizing this vision through the systematic modernization of information technologies—computing, communications, network infrastructure and enterprise-level systems management—to support users and organizations on Army installations.

Installation Information Infrastructure Modernization

The Installation Information Infrastructure Modernization Program (I3MP) establishes, extends and refreshes the connections and technologies that make up the installation information networks for the Army. Enabling net-centric operations on an installation, I3MP installs the hardware, software and fiber-optic and wireless information transport systems necessary to ensure that the installation has the most efficient, interoperable and commercially upgradeable technology available. I3MP continually upgrades the physical connectivity and bandwidth capacity of Army installation networks, enabling the information infrastructure to sustain net-centric operations.

At its inception in 1996, I3MP focused on providing all Army installations worldwide with the minimum network connectivity, information assurance and computing capabilities required for operating on the GIG. However, as a result of emerging mission requirements along with Army Transformation, Base Realignment and Closure (BRAC) and the Integrated Global Presence and Basing Strategy (IGPBS), the program was restructured in Fiscal Year 2005 to focus directly on those installations housing and supporting modular units, their training and support activities, and any gaps between these current Army networks and the DoD GIG. The I3MP is fielding this modernized network infrastructure to 23 installations identified as Force Generation Platforms.

Continuous Access for the Warfighter

Modernization of the Army's information infrastructure is a key part of ensuring that Soldiers have continuous access to critical information across all phases of deployment. To streamline the Army's IT networking operations, new area processing centers will host services for the entire array of combat support functions, including

transportation, logistics, maintenance, military personnel readiness and many other functions. In addition to providing enhanced access by placing more information and services "in the network," the consolidation of IT investments and resources, currently scattered across individual installations, will reduce operating costs and enhance the Army's ability to secure its networks.

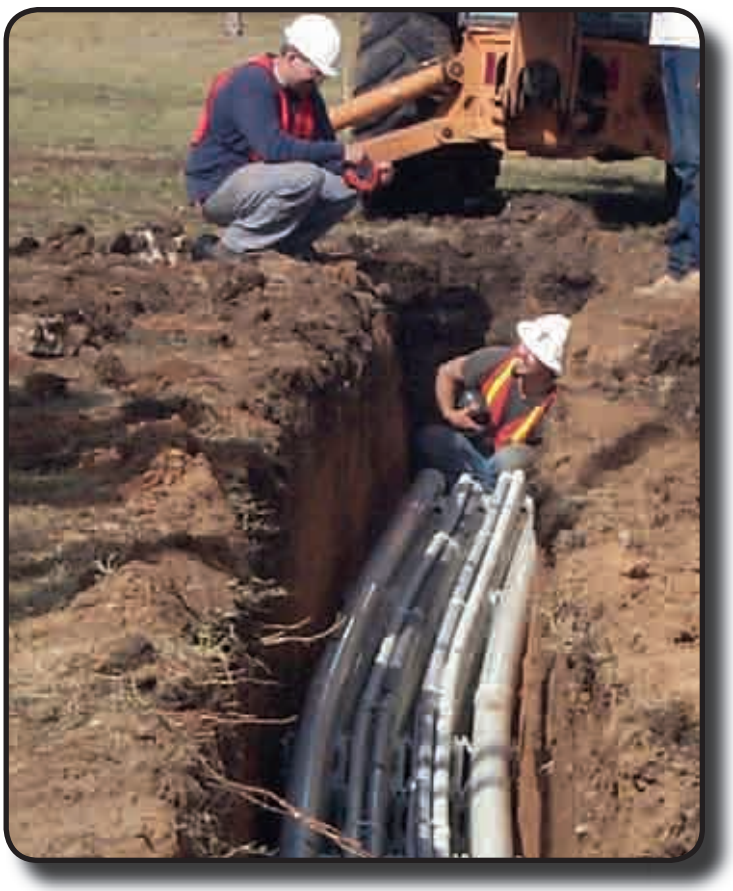
At the same time, modernization of the Army's information infrastructure will allow Soldiers in garrison to train, prepare and deploy in the same IT environment they will encounter when fully deployed. With garrison IT services available over the Secret Internet Protocol Router Network (SIPRNET) at the battalion level and above, the Soldier will be able to access the same IT resources at home station as when deployed.

Emerging Technologies

The Army is continually evaluating and adopting emerging technologies for integration into its IT architecture. The Joint Network Nodes (JNN) network uses commercial off-the-shelf solutions to lower the total cost of ownership (TCO) of Army IT investments, to achieve operational efficiencies and to improve the security of its networks. As new technologies become available, the Army conducts research, development, testing and evaluation on these technologies for the Warfighter Information Network-Tactical (WIN-T) system. The organic union of existing JNN equipment with new WIN-T-enabled devices will offer the Army a more robust and cost-effective way of delivering information to the warfighter.

Where practical, the Army is adopting "thin client" architectures, which transfer applications, data storage and IT management from the desktop computer to a centralized server, allowing applications and data to be centrally installed, configured, managed and distributed at the enterprise level. This architecture results in added efficiencies, increased security and lower TCO. Users access these systems from a simple terminal consisting of little more than a keyboard, mouse and monitor; there is no data storage at the terminal, meaning sensitive information cannot be removed and malicious programs cannot be introduced. Additionally, because thin clients have fewer components than personal computers (PCs)—there is no hard drive, motherboard or microprocessor—thin clients can outlast the traditional three-to-five-year life cycle replacement of PCs.

Voice over Internet Protocol (VoIP) is another emerging technology that the Army is already using. In the past, telephone service has been provided by separate networks (e.g., the Defense Switched Network, or DSN). By placing voice communications on the existing data network, the Army gains a much simpler and more scalable voice capability that is cheaper to operate and maintain. The JNN network now carries VoIP alongside DSN and other legacy networks, realizing the full potential of networked communications by combining voice with data and video to create an "everything over IP" (EoIP) network.



The Army's efforts to upgrade its information infrastructure are making it possible for Soldiers and leaders to stay connected to their sustaining base through all phases of deployment. Emerging technologies enhance the power of that infrastructure while reducing its cost.

Army Knowledge Management:
Serving the Warfighter Worldwide

Army Knowledge Management (AKM) allows Soldiers to use information to their advantage, exploit this information against the enemy and make critical information available to fellow Soldiers in theater and to those preparing to deploy. AKM also enables the Army's generating force to provide the highest-quality acquisition, financial, personnel, logistics and installations support.

AKM creates a clear process for finding, selecting, organizing, improving and sharing information for optimal mission results. It is integral to the Army Modular Force initiative, which involves the total redesign of the operational Army from its division-based structure to a structure built around brigade combat teams.[1] AKM also supports the portfolio management of IT systems. This initiative is eliminating redundant and inefficient "stovepipe" systems and data, integrating networks and improving the security of the Army's knowledge sources. The two main components of AKM are Army Knowledge Online and the Battle Command Knowledge System.

Army Knowledge Online

Soldiers and leaders expect and demand knowledge *now*—not next week, next month or next year. To find that knowledge, they turn to Army Knowledge Online (AKO). **AKO, the Army's Enterprise Portal, serves as the single entry point into official Army knowledge systems and services**. Because AKO is a secure environment, available around the clock worldwide, it provides a reachback capability previously unavailable to the Army. AKO is constantly evolving to meet the knowledge management (KM) demands of the warfighter and sustaining base. AKO also plays a critical morale-building support role in Family Readiness Groups—it allows families to remain in contact with their deployed servicemembers. AKO currently has a user population in excess of 1.8 million, including Soldiers (active Army, Army National Guard and Army Reserve), Department of the Army civilians, family members, retirees and contractor personnel. When Soldiers have questions, they can find the answers in AKO.

AKO provides enterprise-level services (user authentication, global e-mail, web-based collaboration, file storage, instant messenger, etc.) that the Army leverages to streamline business processes, reducing redundancy and eliminating "stovepipe" applications. AKO e-mail also provides every Soldier with one e-mail address for life.

The Army is working to place an "AKO Forward" capability within Southwest Asia and elsewhere. This will extend AKO access to Soldiers in theater, serving as a forward continuity-of-operations capability in the event of network disruptions and reducing the IT hardware/software requirements to be taken into and out of theater. The system should be operational by the end of 2006.

The Defense Information Systems Agency has selected AKO to provide its portal capability under the Net-Centric Enterprise Services program. This will extend AKO across the Department of Defense (DoD) to create Defense Knowledge Online (DKO), providing all DoD personnel with information technology tools including search, discovery, collaboration and information assurance.

Battle Command Knowledge System

The Battle Command Knowledge System (BCKS) is the Army Knowledge Management program focused on the Soldier in combat. BCKS improves the Soldier's ability to exchange timely, relevant information and expertise. This, in turn, increases the speed and quality of decisionmaking,

[1] For more information about the Army's transition to the brigade combat team concept, see AUSA's Torchbearer National Security Reports "The U.S. Army: A Modular Force for the 21st Century" (March 2005), available online at http://www.ausa.org/pdfdocs/TB_Modularity.pdf; and "2006 and Beyond: What the U.S. Army is Doing" (March 2006), available online at http://www.ausa.org/pdfdocs/TBSecRpt/TBear_March_06_optimized.pdf).

leader development, training and education; it also enhances both the lessons-learned process and doctrine development.[2] Specifically, BCKS works to:

- facilitate professional discussions through online collaboration forums;
- foster leader development through professional forums, online teaming and collaborative decision games;
- enhance professional education and lifelong learning by connecting institutional schools/centers with operational units;
- familiarize and train personnel by allowing virtual "right-seat rides"[3] between deployed units and those preparing to deploy; and
- establish a method of discussion related to Soldiers' observations, lessons and doctrine development.

BCKS provides the Army a cadre of knowledge managers and the web-based capabilities necessary to transfer knowledge from those who have it to those who need it. A growing voluntary group of more than 90,000 Soldiers uses BCKS to share and preserve information through an expanding system of Army, DoD, and joint, interagency, intergovernmental and multinational (JIIM) information repositories.

BCKS comprises a growing system of networks connecting the operating and generating forces for rapid knowledge transfer to the warfighter. BCKS is supporting the implementation of knowledge management in units undergoing the Army Force Generation (ARFORGEN) process, particularly as they prepare to deploy. The three main components of BCKS are:

- **Leader Network** (the most mature component of BCKS): Peer-to-peer professional forums that support horizontal teaming and leader development and enable linkage between the institutional/operational Army and the active and reserve components.
- **Unit Network**: Unit-based, vertical and hierarchical structured professional forums that support vertical teaming, virtual right-seat rides and high-performing teams, assisting military units in development of unit-specific portals to enhance their abilities to share knowledge and conduct discussions on unique subjects and missions.
- **Warrior Knowledge Base**: A web-based repository system of data, information, references and knowledge needed by BCKS users, focused on achieving information accessibility and interoperability across the Army.

In response to Soldiers' demand for knowledge, the Army has initiated a BCKS franchise concept that recommends standards, hardware, software and metrics, and provides access to a cadre of community coordinators experienced in managing knowledge networks. Warfighters themselves have also developed an array of KM tools and forums.

To capitalize on this wealth of knowledge and experience, the Army has created an initiative called **"Knowledge Management to the Edge." The goals are to deliver a common tactical KM capability to the warfighter, implement tactical KM configuration management and continually improve and evolve AKO capabilities to support tactical KM requirements.** In another initiative called "Best of Breed," unit-developed knowledge tools will be evaluated at the Central Technical Support Facility, Fort Hood, Texas, to establish an Army Warfighter Enterprise standard. The Army is selecting, integrating and packaging for the tactical environment a standardized Army Best of Breed KM/collaboration solution. The goal is to mitigate the proliferation of unit-purchased, nonstandard KM/collaboration tools and applications across the Army and to reduce the total cost of ownership. An Army G-3/5/7 (Strategy, Plans, Policy and Joint/International Affairs) initiative is also underway to merge the KM capabilities of BCKS into Army Battle Command Systems.

Army Knowledge Online and the Battle Command Knowledge System, the twin pillars of the Army's worldwide knowledge management system, ensure that Soldiers and leaders can learn, communicate and collaborate with one another anywhere in the world.

[2] For an example of information exchange already in use in the field, see AUSA's Torchbearer National Security Report "Accelerating Momentum: The Stryker Brigade Combat Team as a Learning Organization" (June 2006), available online at http://www.ausa.org/webpub/deptilw.nsf/byid/JSUR-6QLHTM.

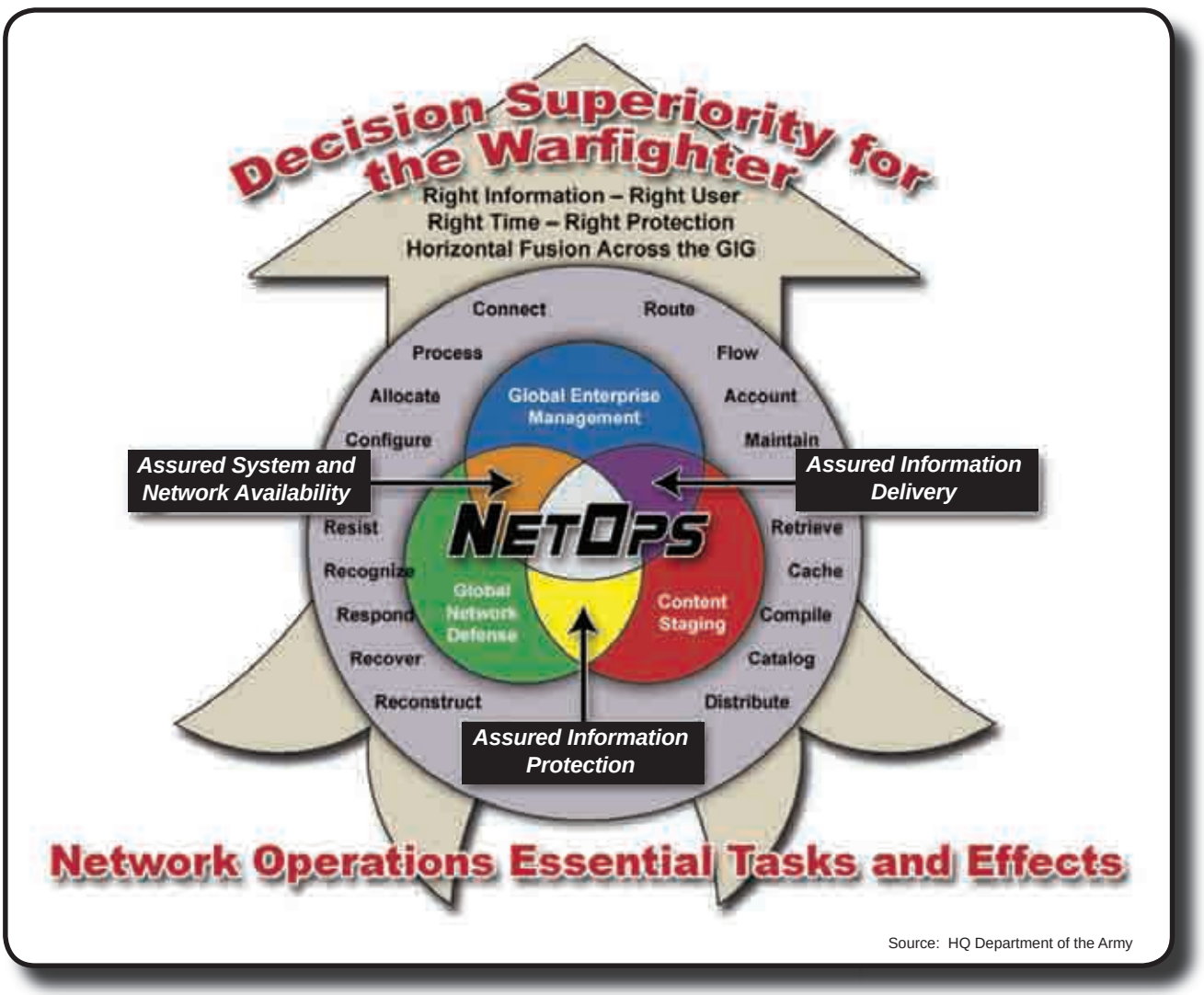
[3] It is standard Army practice for outgoing personnel to provide continuity on duties and lessons learned for incoming personnel. This continuity is commonly known as a "right-seat ride," after the orientation ride that new vehicle crew members are given.

Information Assurance:

Defending and Securing Army Networks and Systems

Information Assurance (IA) is the cornerstone of the strategy for ensuring information dominance in a net-centric warfare environment. IA safeguards the capacity of LandWarNet to provide reliable communications for a global force, securing the Army's warfighting capabilities across the full spectrum of conflict.

IA is significantly enhanced by several programs. These programs are incorporated throughout the life cycle for developing and sustaining all Army networks, systems, architectures, tools and software for the strategic, operational and tactical environments. The most important of these—the IA Policy and Compliance Program—is a proactive defense-in-depth strategy using risk management principles to defend against external threats (rogue nations, criminal elements and hackers) and internal threats (inadequately trained personnel and unauthorized software) to the Army's information systems, networks and data. The program develops, promulgates and enforces IA policies, processes, best practices and compliance to include the Federal Information Security Management Act (FISMA), Army certification and accreditation, "networthiness," and cryptographic and key management modernization programs.



Source: HQ Department of the Army

Information Assurance

IA Tools

To ensure that tools and products used with Army information systems and assets are invulnerable to attack, the Army has established baseline requirements for the commercial, industry, acquisition, integrator and testing communities. Vetting tools, products and manufacturers through a structured process allows Army suppliers, acquisition decisionmakers and equipment integrators to harmonize IA requirements for design, development, selection and deployment of "Best of Breed" technology that minimizes risks and threats and conforms to federal government and Department of Defense (DoD) standards.

Securing the Networks

In 2001, the Army began using the Common Access Card (CAC) and Public Key Infrastructure (PKI) with digital signature and encryption capability to reduce vulnerabilities to its networks and protect against insider threats. The Army continues to incorporate technical solutions to ensure identity and system authentication and verification.

Two key IA programs significantly enhance the security of Army networks and systems: 1) implementation of two-factor authentication, and 2) mitigation of threats to networks through the Information Assurance Vulnerability Management Program.

CAC Cryptographic Logon (CCL) is the Army's smart-card logon for LandWarNet users. It relies on two-factor authentication—a CAC with PKI certificates (something one has) and a personal identification number (something one knows)—to provide logical access to an information system. CCL is more secure than the common user name/password single-factor authentication and cannot be readily compromised by keystroke loggers and similar attacks used today. Phase I of CCL, launched in October 2005, implements the 2004 Department of Homeland Security Presidential Directive 12, which requires a common credential for gaining physical and logical access to federal facilities and information systems. The CAC also serves as the DoD Personal Identity Verification token.

The Army is leading the way in its efforts to enhance CAC's smart-card capability with contactless technology such as Radio Frequency Identification technology to interact with Physical Access Control Systems throughout the federal government. In the near future, the smart-card token will be the only credential used for accessing government computers and facilities.

IA Training

The Army IA Training and Certification Program develops, trains and certifies the Army IA, security and IT workforce. The program employs the best of commercial and DoD training methods to facilitate classroom and on-demand training for Soldiers and civilians.

As the Army embraces innovation and improvements, its IA training and certification program adapts quickly to fill emerging requirements for training on the latest technologies. Over the years, the program has matured and now includes accurate tracking and reporting of training and certification of the IA workforce, with the ability to report the metrics, outcomes and results in various publications including FISMA, personnel records and military service records.

U.S. Army Information Assurance programs are critical for safeguarding the capacity of LandWarNet to provide reliable communications for a global force.

Association of the United States Army

Voice for the Army – Support for the Soldier August 2006

Army Information Business Transformation:

Streamlining Organizations and Investments

Information systems infrastructure expanded rapidly in the 1990s as the Army realized the benefits of information technology. In a rush to get IT capabilities into the force, both individual unit commanders and installation Directors of Information Management (DOIMs) built networks and common-user services to serve the warfighter and support organizations. The Army is now looking at hundreds of IT systems and software packages that have been developed over time by these entities; the goal is to identify and reduce by 80 percent redundant and stovepiped IT investments by 2007.

As the Army transforms its information systems, it is streamlining information management processes. To ensure Army transformation proceeds efficiently and cost-effectively, it is imperative that IT investments support the Army's goals, ensure an efficient delivery of capabilities and maximize return on investment. Two programs form the foundation of this streamlining process: reorganization of IT capabilities under a single DOIM at each installation and consolidation of all IT investments into a portfolio management system.

Single DOIM: Key to One Army Network

The DOIM provides all organizations on the installation with common-user services such as telephone and e-mail services, file and web-server administration, and office automation support. Although tenant organizations may opt to provide their own mission-unique services, the DOIM retains ultimate authority to validate all purchases of IT resources on the installation to ensure compliance with Army enterprise standards and local architecture.

In 2002, the Army Chief of Staff directed the move to one Army information network to permit Army leaders to access the information they need at any time from anywhere in the world. Facilitating this move is the implementation of the Single DOIM. Currently, some organizations still provide a portion of their own common-user services through service centers outside the installation DOIM. The intent of the installation Single DOIM initiative is to realign these services and the associated resources under the installation DOIM, thus complying with Army guidance and applying the principles of Lean Six Sigma[1] by increasing efficiency ("lean") while improving quality and effectiveness ("six sigma"). Specific advantages include:

- consolidation of support infrastructure and streamlined delivery of services, which will optimize usage of IT resources, including both equipment and personnel;
- consolidation and centralization of servers, which will improve server oversight for compliance-monitoring, thus improving overall computer network defense on the installation; and
- increased efficiency obtained by realigning services under the installation DOIM, which will allow organizations to focus more on their core missions.

Business Transformation Supports the Soldier

[1] For more information, see Mike George, Dave Rowlands and Bill Kastle, *What Is Lean Six Sigma?* (New York: McGraw-Hill, 2004).

All of these advantages serve to conserve resources, eliminate waste and ensure that the Army has more resources available for the most critical warfighting tasks.

Future realignment will consolidate the delivery of some services within regional Army area processing centers. This will further enhance the benefits of Single DOIM by consolidating computing and support services, currently scattered across numerous Army installations, into a few select locations.

In December 2005, Headquarters, Department of the Army instructed all Army organizations to begin immediately implementing the Single DOIM concept, with completion by October 2007. There are four phases of implementation: Planning, Design, Transition and Integration. Most DOIMs are currently in either the Planning or Design phase. Approximately 20 percent are at or near completion.

As the Single DOIM concept moves forward, the Army is also assessing the number of personnel required to "right-size"—that is, effectively and efficiently structure—the DOIM, thereby eliminating the need perceived by some organizations to maintain their own common-user IT services. The Installation Management Agency has engaged the Army Manpower Analysis Agency and functional experts to develop a DOIM staffing model that will be released for implementation upon completion of field validation and final approval by Headquarters, Department of the Army.

IT Portfolio Management: Tracking Investments in Warfighting Capabilities

The Clinger-Cohen Act of 1996, in conjunction with DoD and Office of Management and Budget directives, created the basis for Army IT Portfolio Management (PfM). Through IT PfM, the Army is consolidating all IT investments, systems and initiatives into a single repository, categorizing these assets by capability into portfolios and determining if duplicate capabilities exist. Ongoing technical testing at the Central Technical Support Facility at Fort Hood, Texas, is now assessing the impact of these efforts on the tactical network and making further recommendations to effectively support the warfighter.

The Army's IT PfM process includes overseeing all IT capabilities, programs, initiatives, requirements, funding and systems necessary to support joint interoperability, broken down into Mission Areas and Domains. Mission Areas are the areas of responsibility with functions and processes that contribute to mission accomplishment. The Mission Areas may be further divided into Domains, or areas of common operational and functional requirements. For example, the Warfighter Mission Area comprises the Battlespace Awareness, Force Application, Protection, Focused Logistics, and Battlespace Communications Systems Domains. To identify and reduce redundant and stovepiped IT investments, the Army is implementing quarterly enterprise-wide portfolio reviews of IT investments with participation from Mission Areas and Domains.[2]

The official repository for all Army IT assets is the Army Portfolio Management System (APMS). APMS supports the alignment of IT initiatives to Mission Areas/Domains and captures the capabilities the initiative provides the Army enterprise. Ultimately, APMS will allow the Army to manage a vast amount of information using a centralized, accountable system. Different commands, and different levels of command, will have systems that "talk" to one another, significantly enhancing the sharing of knowledge, best practices and lessons learned both in training and on the battlefield. The Army will also be able to shed unneeded systems and ensure that everyone trains on a single network, thus minimizing the amount of retraining needed when transitioning to a new post, while also reducing costs arising from maintaining different systems. In short, **IT PfM is the backbone of the Army's Information Revolution, ensuring that new systems meet the Army's transformational needs efficiently and cost-effectively.**

The Army is applying the concept of business transformation to streamline its information management processes, providing Soldiers and leaders a centralized, accountable, worldwide-accessible knowledge-sharing system.

[2] The Mission Area/Domain structure was established by the Secretary of the Army and the Army Chief of Staff in "Army Knowledge Management (AKM) Guidance Memorandum—Capabilities-Based Information Technology (IT) Portfolio Governance," 20 July 2005, available online at http://www.army.mil/ciog6/references/policy/docs/EIEMA.pdf.

Torchbearer Message

From the military point of view, a network-centric-capable force is one that is robustly networked . . . fully interoperable and shares information and collaborates by means of a communications and information infrastructure that is global.

Secretary of the Army Francis J. Harvey, Welcome Ceremony, Fort Myer, Virginia, 6 December 2004

U.S. Soldiers in Iraq, Afghanistan and elsewhere have both tactical and strategic advantages due to new network-centric information systems and organizations. The United States remains the most formidable military power in the world in large part because the Army continues to **revolutionize** its digital capabilities through innovation, collaboration and joint/coalition teaming. **These advances help ensure that the Soldier—the centerpiece of the Army—has the very best tools for accomplishing missions at home and abroad.**

The 2006 Quadrennial Defense Review emphasized five main areas under "Information": information assurance, information sharing, data strategy, common enterprise services and infrastructure/transport. By concentrating on these critical areas, the Army will have greater success in bringing LandWarNet—the Army's portion of the Department of Defense's Global Information Grid (GIG)—to the Soldier and the fight. LandWarNet is a jointly-inspired vision that networks the Army's active and reserve components to the GIG.

To bring increased capabilities to units as quickly as possible, the Army has fielded a network of Joint Network Nodes (JNN), which consist of trailer-mounted *Ku*-band satellite terminals connected to local area network equipment. A component of the Army's LandWarNet, the JNN network provides Army units at the battalion level and above with beyond-line-of-sight interconnectivity to Army and joint forces. JNN has answered the immediate need for increased bandwidth in the Global War on Terrorism and in domestic hurricane relief efforts.

The next step is to deliver a network that operates on the move with the Soldier. Soldiers and leaders must be ready to maneuver assets throughout the battlespace—land, sea, air, outer space and cyberspace—in real time, and they must exploit IT capabilities through the full spectrum of operations, from domestic disaster relief to counterinsurgency operations in Iraq and Afghanistan and future conventional conflicts. **To succeed, Soldiers and leaders must have a full suite of network capabilities, whether in garrison, en route to destination or deployed.** The Army's future network, which includes the Warfighter Information Network-Tactical (WIN-T) and the Joint Tactical Radio System (JTRS), will provide Soldiers and leaders a network that can automatically adapt and move with them on the battlefield worldwide as they fight with Future Combat Systems (FCS), the Army's primary modernization program and its most critical investment.

As the battlefield area and distances among warfighting units continue to grow, more satellite capability is required. Planning for near- and far-term satellite communications (SATCOM) capabilities and systems such as the Wideband Gapfiller Satellite (WGS) and the Transformational Satellite (TSAT) is paramount to successful Army operations. LandWarNet relies on cost-saving military satellite systems; when one of these systems is delayed, a critical LandWarNet link is delayed and must be replaced by costly civilian satellites.

The Army's activities in developing LandWarNet, modernizing installation IT systems, improving knowledge management, expanding network security capacity and transforming its business practices by streamlining organizations and investments are vital to creating a network that serves as a force multiplier for the current force and forms the critical component of FCS. By equipping the Soldier with robust networking capabilities, the United States will ensure that the Army's Modular Force, with its evolution into the future force, remains the preeminent landpower on Earth.

The Army must have the research, testing and procurement funds to pursue these new technologies so they can be inserted into current forces. An Army engaged in a global war must be able to deliver to its Soldiers and leaders the latest critical information technologies as soon as they are available.

Potential enemies are not standing still; it is therefore imperative that the Army move forward farther and faster than any adversary it may face. For the Army to do so, Congress and DoD must do their part and, in a timely manner, fully fund the Army's plan to deliver information dominance to the warfighter and the Army business leaders who support them.

We are a nation at war. It's our job to help make sure these soldiers get back safely. . . . It's not about the weapons system; it's about information. [Warfighters] need to get the information they need at the time and place they need it.

Lieutenant General Charles E. Croom, Jr., USAF, Director, Defense Information Systems Agency, quoted in Carol Horen, "Team Partnerships to Support the Warfighter," *The Grid*, vol.5, no. 3, July 2006, p. 4, online at http://disa.dtic.mil/grid/pdf/thegrid_web_july2006.pdf

Institute of Land Warfare
Association of the United States Army
2425 Wilson Boulevard, Arlington, Virginia 22201-3385
800-336-4570 www.ausa.org