Association of the United States Army
Voice for the Army—Support for the Soldier September 2015

The U.S. Army's Expeditionary Mission Command Capability

Winning in a Complex World

We must build a force that is agile, expeditionary, tailorable and prepared to meet the challenges of the global environment upon which our leaders are prepared to win. Ultimately battles are won on the ground in the crucible of ground combat. We must maintain the capacity and capability to win.

General Mark A. Milley, Chief of Staff, Army
to the Mission Command Center of Excellence Warfighting Conference,
15 September 2015, Fort Benning, Georgia

Introduction

Today's uncertain and dynamic security environment remains as volatile and unpredictable as ever, perhaps even more so. In fact, constant change now and in the foreseeable future is the norm. Once thought to be receding, the accelerating insecurity and instability across Europe, the Middle East, Africa and the Pacific, coupled with the continued threat to the homeland and the U.S. Army's ongoing operations in Afghanistan, remain significant concerns to America's security community. Potential adversaries continue to emphasize and pursue indirect and asymmetric techniques to negate the U.S. military's strengths and/or threaten America's vital interests. It is imperative that the Army maintain strategic and operational flexibility to deter and operate in multiple regions simultaneously—in all phases of military operations—to prevent conflicts, shape the security environment and win in support of U.S. policy objectives. To win, the Army must provide the joint force multiple options, integrate the efforts of multiple partners, operate across multiple domains and present adversaries with multiple dilemmas.

The Total Army—active, Guard and Reserve—is and will continue to be the backbone of the joint force, providing to each of the combatant commanders such fundamental capabilities as command and control, logistics, intelligence and communications support to set the theater, as well as providing ground combat forces, special operations forces and joint task force headquarters. Demand for Army capabilities and presence continues to increase across combatant commands in response to emerging contingencies. In its new operating concept—"Win in a Complex World"—the Army is developing forces that are expeditionary, tailorable, scalable and prepared to meet the challenges presented by this unprecedented, ever-changing security environment. The foundation of this new concept is the Army's ability to conduct joint combined-arms maneuver.

Imagine this scenario:

A division based in the United States is called upon to deploy with very little notice to a small-scale contingency operation in Africa, the region to which it is aligned. The operation entails foreign humanitarian assistance and disaster relief in a relatively austere portion of the continent threatened by instability. The division must establish a forward command post in the area of operations to support civilian efforts and to provide medical expertise, supplies and training, a robust mission command capability and logistics and engineering support. Once on the ground, the division will work with the U.S. Air Force and Marine Corps, the host nation's military and government, other foreign militaries providing assistance and various international nongovernmental organizations. Given the threat environment, the division will also need to obtain real-time intelligence and situational awareness and to maintain tight security for all of its and its partners' activities. That operational complexity and diversity are the new standard for U.S. Army engagements.

Source: Headquarters, Department of the Army

Expeditionary maneuver becomes the norm as most of the Army is based in the United States (e.g., there are only two brigade combat teams forward stationed). Strategic responsiveness—units ready to deploy, transition to operations rapidly, function over wide areas, import a smaller logistics footprint—is an imperative. Whether the primary mission is combat, humanitarian assistance, counterinsurgency or other, Soldiers and leaders need a robust and varied set of capabilities, especially mission command.

Expeditionary Mission Command and the Network

The keys to achieving these capabilities and characteristics are better command, control, communications and collaboration; on-demand access to and integration of intelligence and information from many sources (to produce thorough, actionable situational understanding); automatic interoperability and sharing with all approved mission partners; and a home-station working and training environment that mirrors what troops experience when deployed and allows split-base operations. Together, these essential elements of landpower form expeditionary mission command.

The core medium of expeditionary mission command is the network. The Army's current plan will create a robust, versatile network through redesign and modernization efforts. Stretching from Army installations, to training facilities around the world, to the operational theater and the Soldier on point, the envisioned network supplies the infrastructure, systems, applications and tools necessary for all Army activities (training, missions and daily business). The network reaches across the globe as a unified, protected and standards-based enterprise, with integrated cyber, electromagnetic and space capabilities. Its relative simplicity and intuitive quality minimize the cognitive and physical burdens on leaders and Soldiers and guarantee a common user experience across echelons, formations and operational phases.

From the mission command perspective, the network delivers converged voice, data, imagery and video by leveraging line-of-sight and beyond-line-of-sight means that are reliable, protected, layered, secure and defensible in cyberspace and the electronic warfare environment. It enables uninterrupted mission command from home station, while en route and immediately upon initial entry into the theater of operations (via satellite). The theater network then "thickens" over time through aerial and terrestrial capabilities.

Mission command network capabilities, as envisioned, will link expeditionary forces to the analysis, tools and expertise they need, when they need them and regardless of whether the source is in theater or half a world away. All elements of the force—from dismounted Soldiers to higher-echelon command posts—can contribute and will have access to a consistent, coordinated and synchronized common operating picture (COP). That COP allows them to engage in real-time coordination and collaboration. Army forces—both in and outside of the theater—will continuously, via the network and its technology, gather, track and fuse intelligence, operational and logistical information to support strategic and tactical decisionmaking.

Challenges for Network Configuration

Expeditionary mission command presents multiple architectural and technological challenges for the network. That network must operate in the contested, congested and competitive media of cyberspace and the electromagnetic spectrum. Strategic lift constraints, the requirement for lighter, more mobile units and the physical limitations of the individual Soldier significantly impact the size, weight and power aspects of network components. Especially for early-entry forces, unique characteristics of airborne, air assault, airmobile and maritime means of insertion demand the network meet the requirements for man-portable and small-vehicle configurations. Moreover, the network must quickly become operational in theater and ready to rapidly integrate with available host-nation and partner communications infrastructures (if any exist).

The need for continuous availability in all circumstances adds another challenging dimension. For example, early-entry operations span multiple domains—land, air, space and cyber—and unfold rapidly. Friendly forces are extremely dispersed, with some portions still in transit, and they face human and materiel resource limits. Once on the ground, units must be able to move and communicate immediately and to expand operations as additional personnel arrive. Interaction and interoperability with joint forces to the lowest level are essential. And, at the forward edge of the network, the demand for relevant, timely information is especially intense.

While uninterrupted expeditionary mission command is the objective, the Army and its partners undoubtedly will encounter periods of limited, intermittent or no connectivity

to the network. To mitigate these circumstances, the network and mission command architecture must allow individuals and units to be disconnected yet continue operations, reconnect as soon as possible and then quickly and transparently resynchronize with the necessary data and services.

Capabilities

Major elements of expeditionary mission command—from the underlying global network architecture to the individual pieces of equipment in the hands of leaders and Soldiers—are beginning to take shape now. Requirements for global reach, high-volume usage, component interoperability and stringent security (for both the network itself and the data and services it provides) are driving multiple initiatives. To ensure that expeditionary mission command can begin while still at home station—and from a headquarters perspective remain there during distributed (split-base) operations—the Army is upgrading its installations' network infrastructure. Improvements include an exponential increase in capacity and a new virtual traffic management system, known as Multi-Protocol Label Switching, which maximizes available throughput. The high-bandwidth network allows voice, video and data (including imagery, sensory data, command and control, broadcasts and telemetry) to traverse the same "pipes" rather than riding separate networks. This convergence simplifies network operation and maintenance, facilitates better protection and cuts costs. During the past 18 months, the Army has modernized 11 installations—more than over the past decade combined—and is on track to sustain this pace.

The Army is also moving to an enterprise, cloud-based construct for management of data, applications and services. As part of the larger Federal Data Center Consolidation Initiative, the Army is centralizing its hosting environments. In concert with its published Cloud Strategy, instead of nearly 1,300 locally controlled facilities, the Army will tap into locations run by the Defense Information Systems Agency and will leverage commercial cloud providers that offer hosting services both on and off premises. (The Army will use its own locations when appropriate.) In tandem, unused and duplicative applications are being eliminated (more than 1,000 to date), which decreases the amount of server space needed. In addition, the Army is transitioning services such as e-mail, telephone, video-teleconferencing and other collaboration tools to an "enterprise-delivery" model.

Combined, these changes will reduce the Army's physical information technology footprint, lower operation and support costs and allow for reallocation of human resources. More important, they provide the path for the universal fast access to information and information technology (IT) capabilities that expeditionary mission command requires. The location of both the user and the data or application needed will not matter as long as he or she is connected to the network. Additionally, deploying units will become more agile as they eliminate servers, other IT equipment and support personnel from their logistics load.

Enterprise-level data management and provision of applications and services are important factors in tightening network and information security as well. For expeditionary mission command to work, the network must always be available and the information it transmits always trusted. Fewer data centers means fewer points of network entry for hackers. Patches and updates to software and firmware will be kept up to date across the force, reducing vulnerabilities. Centralized monitoring of network activity and viability will help prevent—and when it does occur, contain—insider and outsider threat activity.

Joint Regional Security Stacks (JRSS) are another key element of network defense. JRSS perform firewall functions, intrusion detection and prevention and virtual routing and forwarding. Separating server computing and traffic from end-user devices, they improve support to mobile users, a feature essential for expeditionary mission command. And, as the name implies, they are inherently joint, creating the unified security architecture necessary for mission partner interoperability.

The Army already has begun the migration to JRSS, in partnership with the Defense Information Systems Agency and the Air Force. Earlier this year, Joint Base San Antonio, Texas, became the first installation to operate under JRSS defense; implementation is ongoing at more than a dozen sites in the continental United States and overseas. In Korea, the Army is upgrading the network backbone and installing new hardware to set conditions for JRSS installation in 2017. The Army is also migrating the Army Corps of Engineers, Army National Guard and Army Reserve behind JRSS. Upon completion, this migration will put 60 percent of the total Army under JRSS—a major achievement across all components. Eventually, just two dozen JRSS sites will replace hundreds of legacy top-level architecture stacks worldwide.

The final key foundational component is the common operating environment (COE). The COE sets architectural standards for the network itself and everything that rides the network. It is composed of six computing environments (CEs): mobile handheld, mounted, command post, real time/safety critical, data center/cloud and sensor. With the COE's unified data framework, information will move seamlessly across the force. Adherence to the COE is also essential to creating the common user experience that forms the core of expeditionary mission command: the appearance and functionality of the mission command network should not change radically across echelons, formations or operational phases. Under the COE, within each computing environment, hardware and applications will have a common look and feel, and implementation of capabilities that cut across CEs, such as geospatial visualization, will become much easier.

On top of this robust IT base, the Army is layering new operating concepts and technologies specific to execution of expeditionary mission command. The first element is the Home-Station Mission Command Center (HSMCC). Composed of a suite of standardized capabilities at corps, division and select other headquarters, HSMCCs enable distributed mission command, as well as reach-back; commanders can forward-deploy the capabilities needed in theater while leaving those that can be provided remotely, such as planning, analysis and coordination functions, at home station. Deploying a tailored command post offers multiple advantages: it reduces the time and transport required to move into the area of operations, the logistics footprint needed to sustain the command post, the number of Soldiers in harm's way and the overarching cost of sustaining a headquarters. HSMCCs will also address reserve component statutory, regulatory and policy implications.

Paired with the Installation as a Docking Station concept (IaaDS), HSMCCs also will fix the gap between daily operations and deployed operations. Today, most of the mission command equipment Soldiers use in the field is kept packed away until they are called to a training exercise or a real-world mission. IaaDS is a standardized and streamlined connection process and environment that allows operating forces to employ their respective mission command systems on the installation communications infrastructure. While at home station, units will operate in the same manner as when they are deployed. Through daily use, Soldiers will seek to attain a high level of proficiency with their tactical mission command systems, and signal personnel will retain fluency in mission command system employment—making the overall force better prepared to operate in a tactical environment. In addition, mission command systems will be consistently updated with the latest software, ensuring that they are ready for immediate deployment.

The Army has begun implementing HSMCCs in a three-phased process. Survey teams are now assessing the "as is" capability state, against which the Army will set an interim technical baseline. Over the next year, the Army will conduct a technical refresh of headquarters' audio/visual equipment and ensure that they have the requisite network connectivity. By the end of 2016, the Army will have put in place a bridging strategy to incrementally improve and integrate additional required capabilities—such as common network management, cyber security and services—and supporting infrastructure enhancements.

Once a unit is called to deploy, it will tap en route mission command capabilities. While in the air, leaders will have real-time situational awareness and will be able to continue mission planning and synchronization with both the headquarters element at home station and any forces already on the ground. An interim capability that leverages special operations community technology became operational earlier

this year. The first five of 35 aircraft were equipped with Fixed Installation SATCOM Antennas and roll-on/roll-off baseband units. The remaining aircraft will be outfitted in Fiscal Years (FYs) 2016 and 2017. A full user assessment is expected in the third quarter of FY 2017 and a full materiel release is projected for the third quarter of FY 2018.

Early-entry forces have unique mission command needs. These units must be light, mobile, self-sufficient and appropriately sized for the mission and conditions. That translates to communications packages that are small, modular and able to connect to the global network immediately upon arrival. The Transportable Tactical Command Communications (T2C2) system will fill this role. T2C2 will provide satellite capability, via the Warfighter Information Network–Tactical, to small detachments and teams operating in remote locations without fixed network infrastructure. By allowing secure relay of classified and time-sensitive information, T2C2 will greatly improve situational awareness and unit effectiveness. The man-portable T2C2 Lite version will be carried by just one Soldier and can be on the air in less than ten minutes. The heavy version will offer a high-bandwidth tactical network extension to companies and small forward operating bases that are beyond their higher headquarters' line of sight. The Army expects to conduct an operational test in FY 2017 during Network Integration Evaluation (NIE) 17.2 and begin system fielding thereafter. In the interim, the Army is using Global Rapid Response Information Packages and Secure Internet Protocol Router/Nonsecure Internet Protocol Router (SIPR/NIPR) Access Point terminals as a nonstandard bridge capability.

As always, the command post (CP) is the centerpiece of the commander's ability to understand, visualize, describe, direct, lead and assess operations. To make the CP simpler, more mobile and more effective, the Army is consolidating computing hardware, adapting wireless technologies, converting systems into software applications and adding remote administration capabilities. The CP physical infrastructure (shelter, environmental control, power and work space) will vary according to echelon and whether it is

Army Command Post Wi-Fi demo in Hawaii supports expeditionary comms

By Amy Walker, Army.mil

SCHOFIELD BARRACKS, Hawaii (August 20, 2015) — Just like most American homes are shedding cables in favor of wireless technologies, the Army too is in the process of introducing Wi-Fi and 4G LTE to its command posts to improve the agility of its forces.

As part of the effort, the Army successfully demonstrated a National Security Agency (NSA)-accredited unclassified and classified Command Post (CP) Wi-Fi solution with a brigade command post recently, supported by Soldiers from the 25th Combat Aviation Brigade, 25th Infantry Division (ID), at Schofield Barracks, Hawaii.

"Network access is absolutely critical to expeditionary operations," said Lt. Col. Joe Pishock, 25th ID G6 (communications officer).

"Expeditionary communications [capabilities] that connect everyone to the network allow for the best and most rapid transition of forces into diverse environments."

Based in Hawaii, the 25th ID covers the entire Pacific area of responsibility and units are often restricted by the amount of equipment they can transport via ship or commercial air. Sometimes they have to establish headquarters and tactical operations centers (TOCs) in hardscape buildings and even hotel rooms, as well as traditional tents, Pishock said.

"The flexibility offered by going wireless reduces the equipment string while simultaneously increasing our ability to adapt to any location," Pishock said.

Wireless command posts not only shed cumbersome cabling, but network set up and tear down times could be cut significantly, increasing unit agility and reducing interruption of advanced situational awareness.

The Army's CP Wi-Fi demo in Hawaii was a risk reduction exercise to prepare for Network Integration Evaluation (NIE) 16.1 this fall, where the service plans to demonstrate both unclassified and classified CP Wi-Fi capability with a full brigade main command post. The Army successfully demonstrated "unclassified" CP Wi-Fi with a battalion-sized element during NIE 15.2 at Fort Bliss, Texas, in May.

"Unplugging the command post increases freedom of maneuver, to better fight the fight, or aid in disaster relief situations," said Lt. Col. Mark Henderson, product manager for Warfighter Information Network-Tactical (WIN-T) Increment 1, which manages the Army's CP Wi-Fi and 4G LTE capabilities. "Fewer cables enables speed of maneuver which allows Soldiers to remain fully engaged in the mission longer. This is a game changer!"

Without wireless capability, setting up a network in a brigade command post takes hours and requires 17 boxes of 1,000 feet of CAT 5 cable that weigh a total of 255 pounds. The cables have to be cut, laid out, configured and plugged in. Often a special protective flooring has to be laid to protect the cabling. By going wireless, network setup and teardown time may be reduced by hours. Additionally, units can turn on their Wi-Fi "hotspot" and instead of their network coming up last following command post setup, now it comes up first, significantly reducing network downtime for commanders and staff.

"Wi-Fi enables the Army's desire to be more expeditionary," said Andre Wiley, WIN-T Increment 1 project lead for Wi-Fi and 4G LTE. "It also provides more operational flexibility for the commander since he is no longer held hostage to set up and tear down times of equipment. He can move his command post when he needs to move it."

CP Wi-Fi reduces strategic lift, Soldier burden and also cuts down on troubleshooting time, since one of the most common network problems often stems from wiring issues. Additionally, Wi-Fi provides flexibility in how the command post is configured.

"As a signal officer with 20 years of service, I have never seen a TOC established the same way twice," Pishock said. "Not only does this save the labor of the communicators, but it allows commanders to tailor their mission command nodes to suit their personality."

People are sometimes confused between CP Wi-Fi and 4G LTE, but the difference is simple. CP Wi-Fi covers a limited footprint and is used inside the "skin" of the tent, while 4G LTE is used with smartphones to extend coverage to a larger area, like a base, Henderson said.

The Army took advantage of the secure Wi-Fi demonstration in Hawaii to test 4G LTE capability with Nett Warrior, a handheld smartphone-like device usually used in combination with software-defined Rifleman Radios. Using the 4G LTE network instead of radio networks for transport provides higher bandwidth to support the exchange of larger files like video or real-time maps.

CP Wireless can be applied to U.S. and coalition battlefield operations, homeland defense, disaster relief missions and humanitarian aid.

The Wi-Fi capability was already used during support to the Ebola outbreak in West Africa. Once fielded with CP Wireless, when the National Guard rolls in to an incident site with its new Disaster Incident Response Emergency Communications Terminal (DIRECT) system, it can immediately provide 4G LTE/Wi-Fi capability to first responders and nongovernmental agencies as part of its commercial disaster support package.

"The average American takes Wi-Fi and 4G for granted these days, but on the battlefield or in disaster relief efforts, these secure capabilities will actually improve the speed and situational awareness of operations, potentially saving lives," Henderson said. "Staying continually connected is at the core of information dominance and represents the future of how we will fight and win."

operating from home station, while en route or in deployed conditions. Interface media, such as mobile devices, laptop computers, displays and video-teleconferencing, will be COE-compliant and capable of use across any of the three environments. Integration into formation-appropriate CP vehicles of systems such as servers, routers, voice and data radios will further increase mobility and agility, especially for the commander on the move. This will also reduce clutter, the demand for cooling and setup and teardown times. Additionally, under the Command Post Computing Environment, the Army is converging operations, intelligence and network-based transport server architectures onto a single Tactical Server Infrastructure (TSI). TSI, which is undergoing developmental testing and will debut at NIE 16.2, will replace separate server stacks in the command post, reducing the burden on Soldiers and making fielding, training and sustainment easier and more efficient.

As the Army empowers its own Soldiers and leaders, its network and mission command capability must also enable the collaboration and information sharing among U.S. and international partners that are the hallmark of modern humanitarian, combat, stability and support and training operations. The Army and the Department of Defense (DoD) envision a federation of networks and systems—known as the Mission Partner Environment and including transport, applications, policy and a concept of operations—that will integrate combatant commands and nations to produce unity of effort. At the field level, the Mission Partner Environment will provide commanders efficient, responsive IT systems that support sharing operational and intelligence information within multiple communities of interest.

The first piece of the Mission Partner Environment is under construction now through Central Command's Data Center Virtualization (DCV) Pilot. This effort is creating an on-demand data center that can provide IT services for enduring and episodic communities of interest (COIs) with little to no additional computing resources. COIs within the DCV share physical hardware resources but are logically and securely separated. The same COI may be replicated on different virtualized data centers in different locations. As the pilot matures, it will include transaction-based services, such as directory, access control, e-mail with attachments, web/portal, file sharing, office automation, printing and chat; session-based services, such as chat, voice, video-teleconferencing and full-motion video; and function-based services, such as geo-situational awareness and a COP.

The Way Ahead

Expeditionary mission command is fluid: leaders' and Soldiers' needs, the threat environment and national security objectives all will evolve. The Army, therefore, will continuously refine expeditionary mission command capabilities, tactics, techniques and procedures. Beginning in FY 2017, the Army will conduct one NIE and one Army Warfighting Assessment (AWA) annually. The AWA enables the holistic modernization strategy called Force 2025 and Beyond and will further enhance Army interoperability and expeditionary mission command capabilities.[1]

For the Army to achieve and maintain expeditionary mission command superiority, certain conditions, both within and beyond its control, must be met. As it does today, the Army will continue to include its expeditionary mission command portfolio within DoD's Joint Information Environment; this remains an Army priority. Interoperability and efficiency (both functional and fiscal) are central to mission success. Moreover, in addition to working with the other services and allies, the Army needs industry and academia's unique perspectives and potential solution sets regarding architecture, infrastructure, technology and processes. They are key for the Total Army—active, Guard and Reserve—to retain technological overmatch against current and future adversaries.

Putting the best expeditionary mission command capabilities in the hands of Soldiers and partners requires timely and predictable investment: significant funding for basic science and technology; more advanced research and development; acquisition; and sustainment. Failure to invest now in expeditionary mission command and the network increases the risk of sending Soldiers into harm's way without the tools and capabilities they need to win in a complex world.

[1] Association of the United States Army, Torchbearer Issue Paper, "Force 2025 and Beyond: The Army's Holistic Modernization Strategy," January 2015, http://www.ausa.org/publications/ilw/DigitalPublications/Documents/tbip-st/index.html.