The Mission Command Network Modernization Implementation Plan

Executive Summary
2 July 2018

Mission Command Network Integrated Planning Team

DISTRIBUTION RESTRICTION:
Approved For Public Release//Distribution Unlimited

This document is a product of the Mission Command Center of Excellence

Contents

Introduction

Mission Command (MC) is critical to develop commanders, staffs, and leaders with the right knowledge, skills, abilities, and other characteristics to practice the MC philosophy, effectively execute mission command warfighting function tasks, and organize the MC system.[1] The MC Network and the LandWarNet are the capabilities that enable commanders, leaders and Soldiers to exercise mission command (the philosophy) and integrate all warfighting functions and Unified Action enablers (the warfighting function) while providing a means for commanders to develop and maintain situational understanding, maneuver across domains and locations and conduct joint operations to accomplish the mission. It is an inherent component of the Joint Information Environment.[2] The MC Network is central to our ability to exercise mission command. Commanders, staffs, and leaders require a fully capable MC Network as part of the MC System. The Mission Command Network Modernization Implementation Plan (MCNIP) realizes the Mission Command Network Vision and Narrative through 2040, to support the Army Campaign Plan (ACP) that informs and influences the lines of effort for the Army Information Technology Network Strategy from a top down perspective and enables the Army Operating Concept (AOC). It further supports the Army Leader Development Strategy and Army Training Strategy by focusing on how the MC Network enables training, education, and experiences. The current set of Mission Command Network capabilities present challenges of complexity, completeness, vulnerability to emerging threats, affordability, and sustainability to current and future Army operations.

The Mission Command Network Modernization Implementation Plan reflects the Chief of Staff of the Army's (CSA) guidance to Army leaders to synchronize, develop, and deliver capabilities across doctrine, organizational structures, training, materiel, leadership and education, personnel, facilities and policy (DOTMLPF-P). It integrates and synchronizes the ends, ways, and means to enable mission command throughout the Army, utilizing the CSA's First Principles, Characteristics, and Requirements.

Framing The Plan

Operational Environment

To achieve the Army Vision and remain the world's most lethal land force, the Army must continually examine, understand and respond to the environment in which it operates. The Army will sustain a smaller force and will maintain asymmetric overmatch through innovation and the adoption of advanced technologies to enable mission command and the warfighter.

The Army will be largely CONUS-based with a smaller footprint of deployed forces; however, all forces will be prepared to respond globally to any threat. The Army will continue to fight jointly with a large and dynamic set of mission partners, and must operate seamlessly with other federal agencies, foreign government, non-government agencies, local organizations and non-combatants.

[1] The U. S. Army Functional Concept for Mission Command 2020-2040
[2] The Mission Command Network Vision & Narrative. 1 October 2015, p1.

U.S. adversaries will include state and non-state military, criminal and terrorist elements, all of whom present blended physical and cyber threats. Nontraditional combatants will continue to emerge as a result of threats from these adversaries as well as continued urbanization and the spread of advanced cyberspace and counter-cyberspace capabilities. The proliferation and availability of commercial technology may allow adversaries to obtain an operational advantage. Technology, including weapons of mass destruction, advanced sensors, augmented humans, autonomous processes and automated decision making, will permeate the battlefield. The speed at which data is disbursed will create an information-rich environment. However, information quality may be low and extraction of mission-relevant content may be challenging. Misinformation will be used as a weapon[3].

Given the current state of the Army's Mission Command Network Modernization, the Chief of Staff of the Army, General Milley, worked closely with several organizations to develop Mission, Principles, Characteristics, and Requirements of the network that will guide current and future modernization in which the tactical network will inform and drive the enterprise design.

The Problem

The CSA describes the state of the problem: "The current Network Modernization path will fall short of the survivability, effectiveness, interoperability and suitability operational Warfighter requirements for an expeditionary Army in all environments against all enemies." The Army's current network is too complex, fragile, and not sufficiently mobile. Additionally, it is not optimized for Joint, interagency and multination-partner collaboration, susceptible to jamming, vulnerable to cyber-attack, and does not meet size, weight and power needs for an agile ground force.

> "… the Army is woefully behind on modernization, and our soldiers are increasingly unprepared to confront the harsh realities of 21st century warfare. Analyses by the National Commission on the Future of the United States Army, the Office of the Secretary of Defense, and the Army itself have pointed to glaring capability gaps in mobility, lethality, and survivability. These problems will only get worse as adversaries such as Russia continue to modernize their forces. Put simply, our Army lacks both the adequate capacity and the key capabilities to win decisively."
>
> **Opening Statement of Hon. John McCain, U.S. Senator from Arizona, May 2017 Hearing to receive Testimony on the Posture of the Department of The Army In Review of the Defense Authorization Request for Fiscal Year 2018 and The Future Years Defense Program**

The Mission Command Network Vision and Narrative identifies the problem going forward as "how does the Army achieve expeditionary, uninterrupted mission command; a network that is intuitive, secured, standards-based, adapted to commander's requirements, and integrated into a common operating environment; network capabilities that are assured, interoperable, tailorable, collaborative, identity based, and accessible at the point of need in operations that includes the widest range of Unified Action Partners?"

[3] Shaping the Army Network: 2025-2040, (2016), pg. 9

In the spring of 2017, senior leaders from across the Army met with the CSA and developed the overarching guidance to inform the Mission Command Network Modernization. During this engagement, the CSA developed the First Principles, Characteristics, and Requirements for the network. The First Principles describe the "why" of modernization efforts, the Characteristics describe the attributes of the network that best suits the Army's mission and the Requirements show the minimum needs to support the Warfighter and develop an effective, technical network.

First Principles: The Army network must enable:

Conduct of War: Execution of expeditionary, world-wide, Unified Land Operations (ULO) to shape, prevent, and win as a part of Unified Action in all domains and all environments (Note 1/2/3/4)

Preparation for War: Execution of Title 10 responsibilities to man, train, and equip the force, and to build and sustain readiness.

Characteristics of the Network (Qualities and Attributes)

- Simple and Intuitive, single mission command suite (Single COP), installed, operated and maintained by Soldiers
- Available, Reliable and Resilient with the ability to operate in all operational environments against any enemy
- Expeditionary and Mobile, voice, data, and video on the move
- Standards-based, protected, and dynamic network that is upgradeable over time
- Enables the Warfighter to observe, orient, decide, and act faster than the enemy in the conduct of ULO (Note 4)
- Enables use of the network as a weapon system
- Enables leaders to lead and fight their formations from anywhere they choose

Warfighting Requirements

- Able to fight, shoot, move, communicate, protect, and sustain
- Reliably communicate anywhere, anytime, in all domains, in all environments, against any foe

Technical Network Requirements

- Must be capable of adequate secure communications, provides voice, data, video in all environments
- Capable of providing situational awareness down to Platoon level
- Device works anywhere in the world; installed, operated and maintained by Soldiers
- Standardized: Runs on a Common Operating Environment (COE), common graphics, applications, and integrated data
- Ensures continuous Joint interoperability enabling agile and adaptable operational flexibility
- i.e., Enables Rapid Task Organization and employment of joint capabilities
- Mitigates electronic signature
- Accessible to allies and coalition partners

Operational Requirements

The CSA's warfighting requirements are described at the highest level, and deserve amplification. In order to be "able to fight, shoot, move, communicate, protect, and sustain", and "reliably communicate anywhere, anytime, in all domains, in all environments, against any foe" an array of MC Network capabilities are needed.

A Table Top Exercise (TTX), executed by the Mission Command Center of Excellence (7-10 November 2016), analyzed network requirements within realistic scenarios against anticipated missions and threats in order to achieve mission success. The TTX vignettes and excursions spanned Forces Command (FORSCOM), Central Command (CENTCOM), European Command (EUCOM), and Pacific Command (PACOM),

addressing joint operational phases 0-3. As a result, the TTX identified the following five areas as key operational requirements for MC Network modernization: Converged Mission Command Network; Common Operating Environment; Network Augmentation and Extension; Deployable, Integrated and Mobile Command Post, Synthetic Training Environment

Operational Requirements:

- Converged Mission Command Network
- Common Operating Environment
- Network Augmentation and Extension
- Deployable, Integrated and Mobile Command Post
- Synthetic Training Environment

Converged Mission Command Network

The first operational requirement identified is *Converged Mission Command Network.* This enables the convergence of current, disparate networks into a single network that operates seamlessly worldwide in any environment. Areas of emphasis required to support the converged network include *integrated transport* which provides connectivity and network access for forces in an area of operation, especially command posts and mission command on the move (MCOTM), both tactical to strategic. To support integrated transport, a focus on c*yber and electronic warfare (EW) resiliency* in order to mitigate the enemy threat utilizing Cyber Electromagnetic Activity (CEMA) and EW tools. This will leverage Joint Regional Security Stack (JRSS) architecture creating security redundancy, standardizing security practices and reducing exposed cyber-attack surfaces in order to mitigate adversarial attack vectors.

Features that must apply to each modernization effort include *flexibility,* allowing the network *to* work in any environment; the provision of common user experience at home station, enroute, and in deployed conditions; and a *single identity* that provides person and non-person entities secure access to all authorized DoD resources, anywhere and at any time[4] (individuals and units). Additionally, *electromagnetic signature management* provides the capability to modify the signature of network components which facilitates the security of emissions, communications and operations.

This Operational Requirement has the following attributes:

- Access to any capabilities that enable multi-domain battle
- Open architecture for solutions tailored to mission and region
- Army Hybrid Data Center/Cloud enabled computer processing power, storage, marketplace, data and cross cutting capabilities, including enterprise-level authoritative data sources will support distributed Mission Command from any location and approved device
- Dynamic network reconfiguration to support command relationship and task organization changes
- End-to-end network operations
- Software-defined capabilities (automated, dynamic)

[4] Defense Information Systems Agency http://www.disa.mil/initiatives/identity-access-mgmt

- Multiple communication pathways which mitigate terrain, threat, and weather effects
- Leverages commercial network consistent with mission and risk
- Enables and integrates CEMA capabilities
- Meets Soldier responsiveness and 'quality of service' requirements
- Common form factors: able to modify platform radio/waveform capabilities based on mission (common form factors)
- Pooled capabilities – increase capability at desired time and place; Minimal "initializing" and "recovery" times
- Components meet size, weight, and power (SWaP) constraints
- Automated connections
- Standardizing security practices and reducing exposed cyber-attack surfaces to mitigate adversarial attack vectors
- Fault-tolerant Mission Command Systems (MCS) designed to accept and work through network degradation and disruption while maintaining network connectivity without mission suffering under bandwidth limiting conditions

Network Augmentation and Extension

The second operational requirement identified is *Network Augmentation and Extension* which are capabilities that thicken and extend the network to overcome space and terrestrial shortfalls.

Areas of emphasis needed to support this requirement include *improving a commander's ability to 'maneuver'* the network by providing additional communication pathways by increasing the bandwidth capacity and connectivity at the time and place of operation. Also included are *capabilities that facilitate operations* particularly ISR and long range precision fires. This operational requirement drives consideration of an objective that develops a range of terrestrial, aerial, and near-space capabilities to thicken and extend the network and include the following attributes:

- Terrestrial—mesh networks, robotic retransmission
- Aerial—aerostats, aircraft retransmission payloads
- Near-space—high altitude balloons, ionosphere (HF)
- Space—increase satellite capacity
- Maneuver in Spectrum, space segment, IP space, and Transport
- Redundant communication pathways in contested cyber/EW environments
- Additional bandwidth

Synthetic Training Environment

The third operational requirement is the Synthetic Training Environment (STE). STE is education and training delivered over the network to the point of need and will include Combat Training Centers (CTCs), Home Station Mission Command Centers (HSMCC) and the school houses. The STE will provide access to training support enablers and a repository of digitized learning content that portrays operational and mission variables in order to support on-demand training across the operational, institutional, and self-development training domains. This Operational Requirement will include the following attributes:

- Joint Combined Arms (an Army Operating Concept) and Multi-Domain Battle experience (a supporting concept) is accessible through STE across the three training domains.
- Knowledge at the point of need (education and training) and the ability to distribute training and education through cloud-based resources to individuals and their devices at the point of need in three training domains.

Common Operating Environment

The fourth operational requirement is a *Common Operating Environment* (COE) with emphasis on Unified Action Partner (UAP) interoperability. This is a fully integrated and interoperable environment (including cloud computing) that enables the joint operation in both the *Joint Information Environment* (JIE) and the *Mission Partner Environment* (MPE). This also applies to mission command applications in support of commanders and leaders across echelons, and enables all warfighting functions. Situational understanding for commanders and staff will be achieved through the common operation picture (COP) and enabled by a consolidation of applications and system interoperability while including CEMA and electromagnetic data. Episodic extension of MPE to the tactical network, tactical voice interoperability solutions and accessible situational understanding with UAPs will also occur in this requirement. This Operational Requirement will include the following attributes:

- Interoperable data, message, and waveforms
- Integrated with Joint C4ISR and strike capabilities
- Decision aids (knowledge management, big data analytics, and artificial intelligence)
- Data and database integration
- Sensors and applications that enable operations across domains
- Assigned personnel with appropriate CEMA expertise based on echelon, with linkages into the full cyber/EW enterprise

Deployable, Mobile, Agile, Integrated Command Posts

The fifth operational requirement identified is *Deployable, Mobile, Agile, and Integrated Command Posts (CPs).* This is an integrated CP design with inherent expeditionary communications package from Army Service Component Command (ASCC) to BN in support of immediate deployability/mobility. An Integrated design is tailored to echelon and formation and will features an expeditionary communications package. This package allows expeditionary maneuver by CP elements tailored for a wide range of operations from small unit early entry through full combat operations in support of a major campaign. This requirement meets the requirements for formation agility, mobility and protection. Modular and interchangeable components facilitate task reorganization and allows CPs to be employed in multiple locations with low profile signatures (cyber, electromagnetic, physical). This operational requirement will include the following attributes:

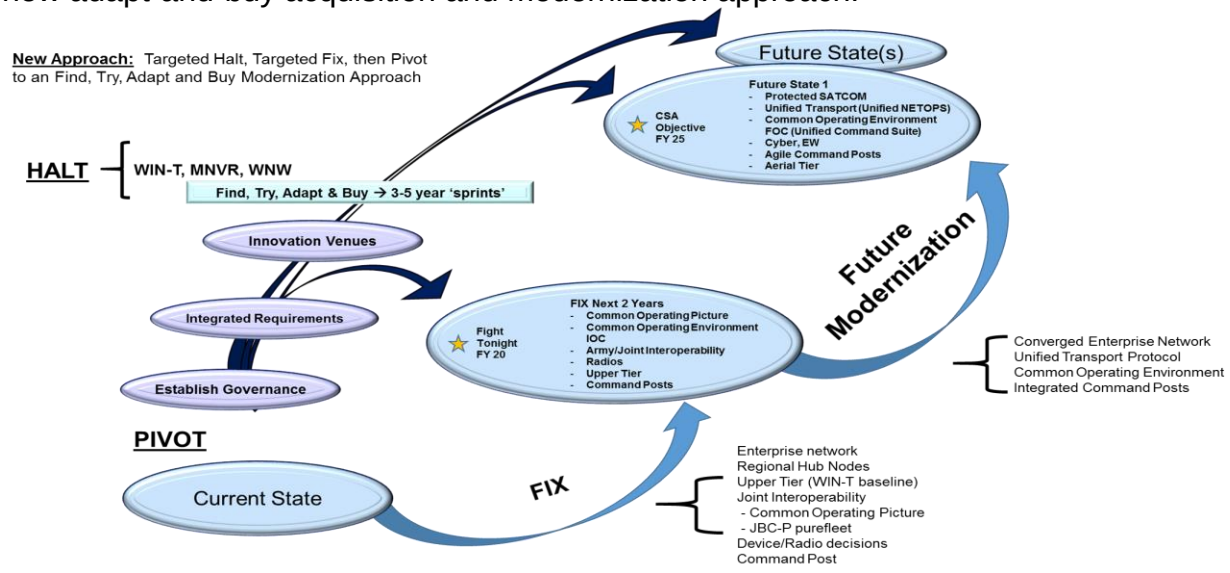
- Connected, resilient, and scalable
- Formation-appropriate survivability (physical protection)

- Container, tent-based, and on-platform capabilities that can enable rapid set-up and tear-down
- Deployable, common equipment that scales based on echelon/mission and provides the basic services of voice, data and position available on mobile devices and access to network that enables full motion video and collaboration
- Minimize 'recovery' time to re-establish MC systems and network;
- Main CP is mobile when required
- Tactical Command Post (TAC): mobile, low profile signature
- Mobile Command Group (small, air/vehicle based Mission Command on the Move, TAC reach back)
- Able to modify the physical signature of CP elements, incorporating platform and CP integrated camouflage design
- Mission Command nodes incorporated with Component Command (CCMD) and Joint CCMD further described as Joint Force Air Component Commander (JFACC) and Joint Force Maritime Component Commander (JFMCC) (e.g. Digital Liaison Detachments).

CSA's Implementation Guidance

The Chief of Staff of the Army's guidance to Army leaders is to move away from the current network modernization path which falls short of the operational Warfighter requirements of survivability, effectiveness, interoperability and suitability for an expeditionary Army in all environments against all enemies. Based on the CSA's guidance, the Army must now pivot from its current state to a new network modernization approach.

The new course of action (shown below) depicts the Army's targeted halt, fix and pivot to an adapt and buy modernization approach. Near-term fixes focus on readiness in order to fight tonight and buys down risk on fixable components of the network. This ensures we can support the most pressing OPLANs, while simultaneously pivoting to a new adapt-and-buy acquisition and modernization approach.



This new approach provides greater predictability for our forces and better facilitates collaboration with industry. This approach begins in FY 18, occurs in 3-5 year sprints and reaches incremental future states as indicated in the Strategy Framework. The initial Halt, Fix and Adapt and Buy actions to support the Framework will occur utilizing the following timeline:

- Targeted Halt (Near-Term FY 18-20): Halt all programs that are not needed for the future state, or do not meet operational requirements for today.
- Targeted Fix (Near-Term FY 18-20): Fix those programs necessary for acceptable Army baseline, Joint interoperability and to buy down risk against a peer adversary. This includes fixing individual systems and the tactical network as a whole.
- Pivot to Find, Try, Adapt and Buy (Near-term FY18-20): Utilizing a Find and Try method allows continuous evaluation of available, commercial solutions for military application using operational units to test potential technologies in the field. The Army will then 'adapt and buy' the best-tested solution to meet unique military challenges, and modify its tactics, techniques and procedures to enable it to best leverage new and existing technologies.

This approach requires a complete review and update of our governance processes, from how we draft requirements, to the acquisition process, to how we fiscally manage this portfolio, and how we better hold ourselves and industry accountable to deliver the requirements our Soldiers deserve and need. It also affords the Army an opportunity to pivot to an Adapt-and-Buy acquisition process partnering with industry utilizing the following solutions:

- **Find existing and emerging solutions versus develop solutions**: Given the rate of industry R&D and the rate of change in technology, it is futile for the Army to spend millions of dollars on "development". It is our belief that the most effective and efficient path forward is to "find" available solutions that meet our needs, rapidly "adapt" those solutions with funding dedicated to integration and a more rapid test and evaluation process – this puts relevant capabilities in the hands of Soldiers faster.
- **Team Approach**: We will stand up a military-industry Cross-Functional Teams (CFTs) comprised of operators, a contracting team, legal, human engineers and design experts. They will narrow an existing capability gap by developing capability documents, informed in appropriate cases by experimentation and technical demonstrations, and rapidly transition leader-approved capability requirements to the Army Acquisition System[5]. The future network must be built from the Soldier's experience, not by engineers. The hub of these efforts will be with operational units so innovation and improvements are made more rapidly. These CFTs will address network disconnects and misalignments by horizontally and vertically integrating requirements. Concurrently, they will seek available solutions for experimentation, demonstration and evaluation by Soldiers and leaders in the field.
- **Soldier-Centric Design:** Fundamentally we need to change how we design every aspect of our network so we take into account the one constant – our Soldier. This is no different than in the commercial sector, which is designed around consumers. We

[5] Army Directive 2017-24 (Cross-Functional Team Pilot In Support of Materiel Development)

will adapt leading design-theory fundamentals that turn upside down the current government acquisition process. Innovation around and with Soldiers is key.

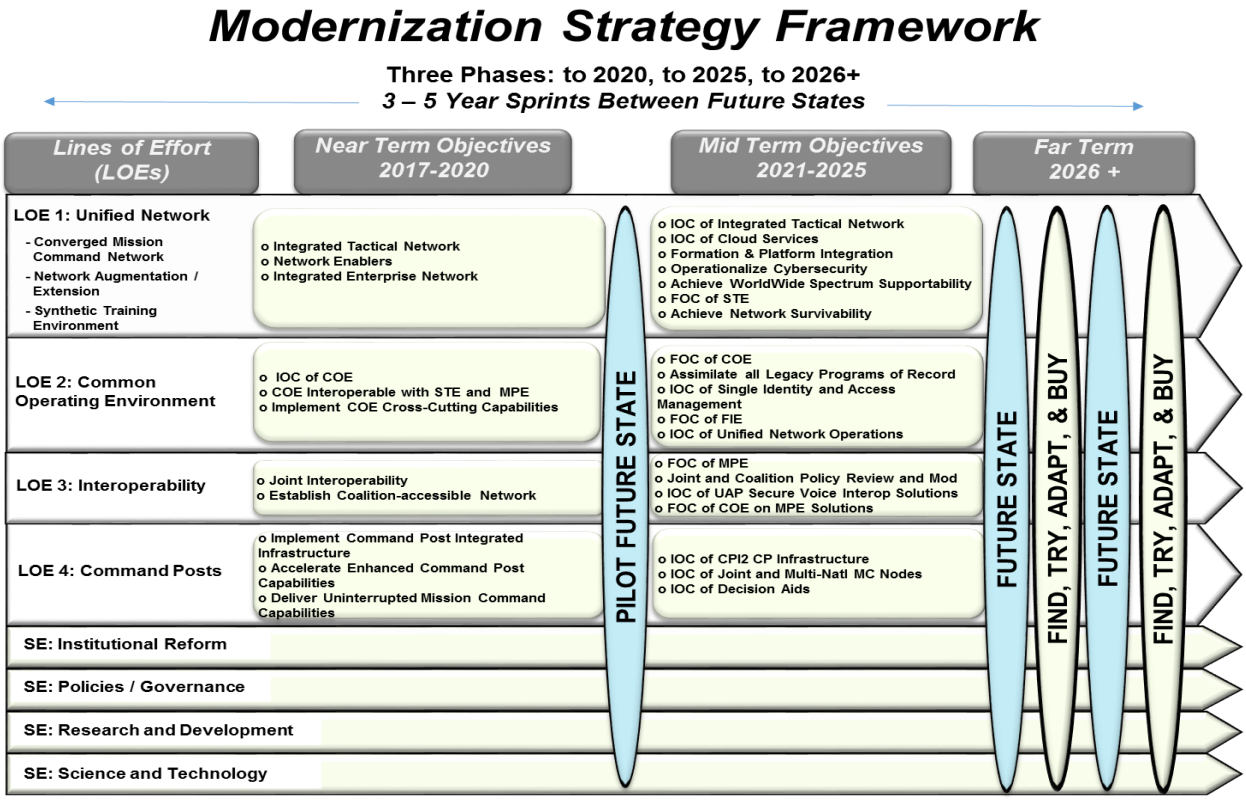
The Strategy

The Mission Statement

The Army's mission statement for the Implementation Plan is "The Army will field a network that is easy to use, works in all environments, in order to prepare for war, and to fight and win wars."

Strategy Framework

The Strategy has four modernization lines of effort (LOE), oriented on operational requirements and will occur over three phases: near (to 2020), mid (to 2025), and far (2030 and beyond). These near-, mid- and far-term objectives will support objectives that will be achieved in the Pilot Future State 2020, Future State 2025 and Future State 2030 and beyond. Each of these Future States will be reached in 3-5 year sprints as advances in technology emerge.



Lines of Effort and Future Network States

The Strategy enables operational requirements through the LOEs and future states of the network as discussed above. The following sections will take a closer look at the LOEs and how each supports the network future states. The chart below indicates Objectives in Pilot Future State 2020, Future State 2025 and Future State 2030:

	Objectives Pilot Future State 2020	Objectives Future State 1 (2025)	Characteristics of Future State 2 (2030)
LOE 1	o Integrated Tactical Network o Network Enablers o Integrated Enterprise Network	o IOC of Integrated Tactical Network o IOC of Cloud Services o Formation & Platform Integration o Operationalize Cybersecurity o Achieve WorldWide Spectrum Supportability o FOC of STE o Achieve Network Survivability	o Internet of 'battle things' o Mesh network o Intuitive and seamlessly integrated (aided by AI and advanced interfaces) o Persistent cross domain operations o Balanced access vs. protection * Characteristics will inform Future State 2 objectives as technology advances and previous Future State objectives are achieved
LOE 2	o IOC of COE o COE Interoperable with STE and MPE o Implement COE Cross-Cutting Capabilities	o FOC of COE o Assimilate all Legacy Programs of Record o IOC of Single Identity and Access Management o FOC of FIE o IOC of Unified Network Operations	
LOE 3	o Joint Interoperability o Establish Coalition-accessible Network	o FOC of MPE o Joint and Coalition Policy Review and Mod o IOC of UAP Secure Voice Interop Solutions o FOC of COE on MPE Solutions	
LOE 4	o Implement Command Post Integrated Infrastructure o Accelerate Enhanced Command Post Capabilities o Deliver Uninterrupted Mission Command Capabilities	o IOC of CPI2 CP Infrastructure o IOC of Joint and Multi-Natl MC Nodes o IOC of Decision Aids	

Line of Effort 1: Unified Network

The CSA's intent for the network is met by establishing a converged Mission Command Network that operates seamlessly worldwide in any environment. This effort has three components: Integrated Tactical Network, Integrated Enterprise Network and Unified Network Enabling Capabilities. It includes the development of a standards-based network architecture that unifies enterprise and deployed network capabilities and features a unified transport layer, network operations and other enabling functions that allows integration of disparate networks. The Army desires the network to provide resiliency through path diversity and dynamic routing to ensure tactical units can communicate in hostile environments. It fully incorporates cyber and electronic warfare capabilities that support the employment of the network as a weapon system.

This LOE addresses current issues such as fragmented organizational and functional networks, cyber vulnerabilities, complexity, fragility, and lack of interoperability with joint and coalition mission partners. This will require the creation of a standards-based network architecture that effectively integrates enterprise and deployed network capabilities across domains and environments, and features a unified transport layer that permits "plug and play" for specific network capabilities. LOE 1 addresses the following operational requirements: Converged Mission Command Network, Network Augmentation / Extension, and Synthetic Training Environment.

A vital support element to achieve key actions in LOE 1 are the APNT, Network, and Synthetic Training Environment (STE) Cross Functional Teams (CFTs). These CFTs will be leveraged to innovate and inform requirements and solutions. Key actions in the near-term include 'secure but unclassified' network, air-ground integration, and next generation tactical radios. In the near term, key objectives include (1) a standardized WIN-T baseline, (2) the standards-based network architecture described above, (3)

initial network, provisioning, and transport convergence, (4) joint & coalition gateways, and (5) adaptation of available, interoperable radios. These actions help create the first 'future state' of the network.

In the mid-term, key actions are: (1) completion of network, provisioning, and transport convergence; (2) incorporating cyber and electronic warfare capabilities; (3) dynamic spectrum allocation; and (4) and dynamic network adaptation. Key Research & Development (R&D) and Science & Technology (S&T) efforts for successive 'future states' include Lite Sabre, improved waveforms, and network augmentation/extension capabilities.

Line of Effort 2: Common Operating Environment (COE)

The CSA's intent for the network is to have a Common Operating Environment (COE) with an approved set of standards and technologies that enables a unified set of mission command applications and allows warfighters to adapt and configure the network as conditions change. COE is fundamentally designed as part of the Joint Information Environment (JIE).

This LOE provides solutions for current issues with stove-piped mission command systems that function well individually, but do not integrate easily with each other nor does it provide an accurate common operating picture. It will also support collaboration using a common picture with joint and coalition mission partners. This LOE delivers an integrated body of requirements that meet operational needs. The decisive action within this LOE is fielding of the initial version of COE in FY19.

This LOE leverages the APNT, Network, and Synthetic Training Environment (STE) Cross Functional Teams to innovate and inform requirements and solutions. Key CFT-supported actions in the near-term is bridging solutions for a joint common operational picture focused on software baseline reduction, JBC-P pure fleeting (with an initial operational capability in FY19), and data center/cloud migration.
Key mid-term objectives are instituting COE across the Army, maturing COE with additional capabilities, and transitioning legacy mission command systems to COE-based applications. R&D and S&T initiatives that help create successive 'future states' include automated planning and high-tempo data-driven decision tools. Operational Requirements met in LOE 2 are Common Operating Environment and Interoperability.

Line of Effort 3: Interoperability

The CSA's intent for the network is to create joint interoperability and coalition accessibility through a network that enables appropriate collaboration with all unified action partners. This is in alignment with DOD JIE and the Mission Partner Environment (MPE) efforts and is achieved through the development of an architecture and mission command systems that are rapidly adaptable to common operational standards. Interoperability is the ability to routinely act together coherently, effectively, and efficiently in order to achieve tactical, operational and strategic objectives.

Going forward, the Army will procure solutions that will incorporate the ability to leverage common commercial standards and/or widely recognized military interoperability standards.

In the near-term, this LOE focuses on the development of a "secure but unclassified" network, and interoperable gateways and radios in order to achieve initial operating capability (IOC) for the MPE. Key mid-term objectives include: MPE full operating capability (FOC); a deployed Army solution to extend episodic MPEs into the tactical network; and implementing solutions to UAP information exchange gaps (data, message and waveform Interoperability).

Long-term key actions are R&D and S&T initiatives that focus on interoperability in the areas of communication, information systems and information management; intelligence, surveillance and reconnaissance (ISR); intelligence fusion; digital fires; and sustainment. Similar to LOE 2, this effort establishes an interoperable network environment and addresses the operational requirements of Common Operating Environment & Interoperability.

Line of Effort 4: Command Posts

The CSA's intent for the network is to implement capabilities that enable the Army to employ command posts across the operational spectrum, from early entry to major combat operations, and that resolve current issues with set-up and tear-down, survivability, mobility, suitability and footprint. This LOE will focus on developing and obtaining approval of requirements for integrated command posts, then delivering these integrated command post designs to Army units. LOE 4 addresses the operational requirement of Deployable, Integrated, and Mobile Command Post and integrates Knowledge Management.

Key near-term objectives are the delivery of containers and vans to high priority units in FY 18, reprioritization of interim CP enhancements to Brigade Combat Teams (e.g. secure Wi-Fi), and improved platform integration. Key mid-term objectives include the delivery of CP Directed Requirement capabilities, and the development and delivery of Integrated CP Designs that provide agility, mobility, and protection. Key R&D and S&T initiatives include signature management and advanced mobility solutions for CPs. The Network CFT efforts will inform these future requirements.

Conclusion

The Mission Command Network Modernization Strategy and Implementation Plan supports the Army Mission Command Strategy by fulfilling the ideas and design principles outlined in the Mission Command Network Vision and Narrative. It integrates and synchronizes the ends, ways, and means to enable mission command throughout the Army and in collaboration with joint and multinational partners. The Strategy also integrates the outcomes of the Operational Requirements Table Top Exercise (November 2016) and the five operational requirements established therein: Converged Mission Command Network; Common Operating Environment; Network Augmentation

and Extension; Deployable, Integrated, Mobile Command Post; and Synthetic Training Environment. Each are aligned to the Implementation Plans' four lines of effort and will be evaluated and assessed over near-, mid- and far-terms in order to achieve Future States. The Strategy achieves unity of effort to develop and deliver capabilities across all DOTMLPF-P domains.

Appendices

1. Abbreviations, Acronyms, And Initialisms
2. Definitions

Appendix 1: Abbreviations, Acronyms, And Initialisms

ASCC	army service component command
BYOD	bring your own device
COMSEC	communications security
CONOPS	concept of operations
CP	command post
DIL	disrupted, intermittent, limited
EMS	electromagnetic spectrum
ICD	initial capabilities document
JTF	joint task force
JFLCC	joint force land component commander
MC	mission command
MC Network	mission command network
MC System	mission command system
OPSEC	operational security
PED	processing, exploitation, and dissemination
RAF	regionally aligned forces
STE	synthetic training environment
SWaP	size, weight, and power
TTP	tactics, techniques, and procedures
UAS	unmanned aircraft system

2: Definitions

Accessible - Easy to approach, reach, enter, speak with, or use.

Adaptive - Adjust or modify to changing requirements or conditions.

Assured - Guaranteed; sure; certain; secure.

Bandwidth-tolerant Applications and Resilient Communications - Communications must be able to adjust dynamically to restrictions in bandwidth availability, communication protocols and architecture limitations. Data mapping must be able to function no matter how much or little bandwidth is available and with appropriate server and physical infrastructure considerations.

CP Infrastructure - The physical infrastructure of CPs, with emphasis on deployability and tactical mobility.

Collaborative - Sharing information, knowledge, perceptions, ideas, and concepts regardless of physical location.

Cyber Electronic Warfare capability integration - Resilient against peer, near peer, and non-state actors situational awareness for commanders & staff part of includes sensors and applications that enable operations across domains. Operational Utility and Adaptability through Simplified and Protected Network to achieve a more robust satellite communications network in a contested environment.

Decision Aids - Provide decision aids (e.g. knowledge management, big data analytics, artificial intelligence) to commanders, leaders, and soldiers.

Distributed - Accessible at all geographic locations, garrison or deployed.

Deployable - Movement of forces and sustainment resources from their original locations to a specific operational area.

Early Entry CP Capability - Establish tailorable mission command package capable of home station reach-back, liaison, and controlling operations until TAC CP IOC.

Enroute Mission Command Capability - Able to execute distributed uninterrupted Mission Command across multiple locations with continuity of purpose in spite of discrete breaks in communications.

Enterprise Services to the Tactical Edge - Soldiers are able to access core enterprise information services (Unified Capabilities) in both garrison and the tactical environments with a common experience (relative to equipment constraints).

Expeditionary - The ability to deploy task-organized forces on short notice to austere locations, capable of conducting operations immediately upon arrival.

Expeditionary communications - Provide an ‘Expeditionary Communications Package’ with deployable, common equipment, which scales based on echelon/mission, and provides basic services (voice, data, PLI, FMV, collaboration) upon arrival.

Expeditionary Maneuver - The rapid deployment of task-organized combined arms forces able to transition quickly and conduct operations of sufficient scale and ample duration to achieve strategic objectives.

Federated Integration Environment - A collaborative COE development environment that links capability developers, material developers, training developers, TCMS, and evaluators/testers.

Global Enterprise Network - Warfighter's use of LANDWARNET is more secure with the cyber attack surface reduced from over 1000 disparate network ingress points to less than 50. Provides timely information to Network Defenders so responsive actions can be taken when an anomaly is detected. Achieves a standard cybersecurity architecture.

Home Station Mission Command Center Capability - A standardized Home Station Mission Command Center Capability (HSMCC) that permits the execution of distributed mission command with the Main CP operating primarily from home station (Active and Reserve).

Identity-based - Capable of assigning an identity to individual nodes; facilitates mission command and security.

Improved Education and Training Strategies - Mission Command Learning (training and education) strategies & plans are adapted for a modernized network, learning environment, and other human dimension initiatives. Leaders and Soldiers are trained and educated on how to leverage these new capabilities in order to enable expeditionary/uninterrupted mission command and employ new operational and institutional capabilities.

Improved Network Capacity - Increased capacity at home stations and between installations to support commander's training and operational needs.

Installation as a Docking Station (IaaDS) - Units operate and maintain their organic tactical systems on Installation Campus Area Networks to maximize system readiness, unit digital training capabilities, and both unit system maintainer and end user tactical system proficiency.

Institutional Training Domain - Institutional training domain includes Army centers/schools that provide initial training and subsequent functional and professional military education for Soldiers, military leaders, and Army Civilians.

Integrated - The process of linking together different computing systems, software applications, business processes, and functionally to act as a coordinated whole.

Integrated CP Designs that provide agility, mobility, protection - Meet formation agility, mobility and protection requirements, and minimize 'recovery' time to re-establish MC systems and network. It also ensures these integrated designs feature low-profile signatures, with additional signature management capabilities.

Integrated Family of Requirements - The maintenance of an integrated family of requirements for the Mission Command Network)Requirements are governed by the Mission Command Requirements Governance Team).

Interoperability – 1. The ability to operate in synergy in the execution of assigned tasks (JP 3-0). 2. The condition achieved when information or services can be exchanged directly and satisfactorily between them and/or their users (JP 6-0).

Intuitive - Understandable to the intended user with a reasonable amount of training.

Knowledge Management Capabilities - Provide decision aids (knowledge management, big data analytics, artificial intelligence) to commanders, leaders, and soldiers.

Main CP Capability - Develop deployable and scalable mission command nodes (Corps/Division) that conducts mission command from home station and/or deployed locations; capable of supporting forward deployed mission command nodes with global reach. Develop agile and scalable (BCT/BN) mission command nodes integrated as a platform.

Mobile Command Group Capability - Develop nodes able to conduct mission command and maintain situational awareness while away from the command post and moving on the ground and in the air.

Network Augmentation and Extension - Overcoming terrestrial and space communication shortfalls.

Network Modernization - Corps and divisions are able to effectively execute mission command from home station for a broad array of missions, including garrison operations, split-based operations, regionally aligned force (RAF), homeland defense, military support to civil authorities, and other operations. Preventing unauthorized interceptors from accessing telecommunications in an intelligible form while still delivering content to intended recipients. Transportation systems and insure safe travel. Transfer or title or disposal of system not supporting the modernization of the network (COMSEC, TRANSEC, divestiture).

Network supports UTR, AGO, network join, rejoin, traverse. “flexible task organization” - A set of integrated capabilities fielded BDE and below empowering units to be able to plan, establish, and sustain all of their communications systems impacted by the new task organization, meeting the following conditions: (1) all changes can be conducted within the timelines allotted during the planning phase of the mission (i.e. 1/3 planning, 2/3 execution rule), (2) the unit can provide all required voice and data services required to support the mission to the extent possible based on the C4ISR systems they have available, (3) the unit can execute the UTR without support from FSEs.

Operational Training Domain - Operational domain encompasses training activities that unit leaders schedule, and individuals, units and organizations undertake. These activities include: progressive training conducted at home station, regional collective training capability, regional training centers, and mobilization centers.

Proliferation of Capabilities Across the Force - Timely increase of capabilities across all echelons.

Reach - Collaboration, information sharing, and capability integration with any organization and/or individuals, regardless of location, echelon, or affiliation.

Resilient - We value the network’s ability to (1) enable distributed, uninterrupted mission command; (2) function in spite of cyber electromagnetic threats; and (3) maintain functionality in spite of the loss of key nodes and pathways through PACE.

Secure / Secured - Assured confidentiality and integrity of data.

Self-development Training Domain - 1.Structured self-development. Learning that continues throughout a career and that is closely linked to and synchronized with

classroom and on-the-job learning. 2. Guided self-development. Recommended but optional learning that will help keep personnel prepared for changing technical, functional, and leadership responsibilities throughout their career. 3. Personal self-development. Self-initiated learning where the individual defines the objective, pace and process, such as: pursuing college education, advanced degree programs, and so forth.

Signature Management - Provide capabilities that conceal or minimize the physical, cyber, and electronic signature of CPs.

Simplicity - We value the ability to (1) leverage network capabilities in intense, time-constrained situations placing significant cognitive and physical demands on leaders and soldiers; and (2) provide for a common user experience across echelons, formations, and phases of the operation

Single Identity - For individuals and units.

Standard-based - Built on a common technical foundation; enables interoperability.

Synthetic Training Environment - Realistic training and education at home station, off-site, and deployed is fully enabled with installation and infrastructure network capacity and connectivity. Training resources are delivered to the point of need via the AEN to enable collective and individual training and education within and across all three training domains (Operational, Institutional, and Self-Development).

TAC CP Capability - Develop agile/expeditionary/scalable mission command node (BN through Corps) that can deploy rapidly and conduct mission command; includes at-the-halt and on-the-move capability.

Tailorable - Adjustable to different missions, conditions, and task organization in a reasonable period of time.

Transport Convergence - The merging of command and control, intelligence, logistics and medical systems onto a common network architecture.

Unified Mission Command Platform (CP CE, Mounted CE, & Mobile CE consolidation) - Consolidate the existing CP, mounted, and mobile hand/held computing environments into a single unified mission command platform that functions across all three conditions.

Unified NETOPS & Software Defined Networks - A suite that will allow the soldier/operators at the BDE to plan, configure, initialize, monitor and manage the network. NetOps tools will have a common set of integrated capabilities and are adaptable by echelon, reduce duplicate functions and produce a repeatable process to reduce operator and maintainer workload, and increase operator efficiency.

Uninterrupted - Having an arrangement of capabilities that supports continuity in purpose in spite of discrete breaks in service or priority; continuous.